

106

# FINANCIAL PRIVACY

---

Y 4.B 22/1:106-32

Financial Privacy, Serial No. 106-32, Vol. 20, No. 1, 1999  
106-1 Hearings,

## HEARINGS

BEFORE THE

SUBCOMMITTEE ON  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
OF THE

COMMITTEE ON BANKING AND  
FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

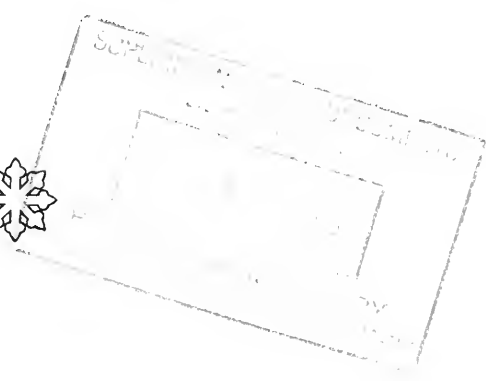
ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

\_\_\_\_\_  
JULY 20, 21, 1999  
\_\_\_\_\_

Printed for the use of the Committee on Banking and Financial Services

**Serial No. 106-32**





# FINANCIAL PRIVACY

---

---

**HEARINGS**  
BEFORE THE  
SUBCOMMITTEE ON  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
OF THE  
COMMITTEE ON BANKING AND  
FINANCIAL SERVICES  
U.S. HOUSE OF REPRESENTATIVES  
ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

---

JULY 20, 21, 1999

---

Printed for the use of the Committee on Banking and Financial Services

**Serial No. 106-32**



U.S. GOVERNMENT PRINTING OFFICE

58-308 CC

WASHINGTON : 2000

---

For sale by the U.S. Government Printing Office  
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402  
ISBN 0-16-060190-8

HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES

JAMES A. LEACH, Iowa, *Chairman*  
BILL McCOLLUM, Florida, *Vice Chairman*

MARGE ROUKEMA, New Jersey	JOHN J. LAFALCE, New York
DOUG K. BEREUTER, Nebraska	BRUCE F. VENTO, Minnesota
RICHARD H. BAKER, Louisiana	BARNEY FRANK, Massachusetts
RICK LAZIO, New York	PAUL E. KANJORSKI, Pennsylvania
SPENCER BACHUS III, Alabama	MAXINE WATERS, California
MICHAEL N. CASTLE, Delaware	CAROLYN B. MALONEY, New York
PETER T. KING, New York	LUIS V. GUTIERREZ, Illinois
TOM CAMPBELL, California	NYDIA M. VELAZQUEZ, New York
EDWARD R. ROYCE, California	MELVIN L. WATT, North Carolina
FRANK D. LUCAS, Oklahoma	GARY L. ACKERMAN, New York
JACK METCALF, Washington	KEN BENTSEN, Texas
ROBERT W. NEY, Ohio	JAMES H. MALONEY, Connecticut
BOB BARR, Georgia	DARLENE HOOLEY, Oregon
SUE W. KELLY, New York	JULIA M. CARSON, Indiana
RON PAUL, Texas	ROBERT A. WEYGAND, Rhode Island
DAVE WELDON, Florida	BRAD SHERMAN, California
JIM RYUN, Kansas	MAX SANDLIN, Texas
MERRILL COOK, Utah	GREGORY W. MEEKS, New York
BOB RILEY, Alabama	BARBARA LEE, California
RICK HILL, Montana	VIRGIL H. GOODE JR., Virginia
STEVEN C. LATOURETTE, Ohio	FRANK R. MASCARA, Pennsylvania
DONALD A. MANZULLO, Illinois	JAY INSLEE, Washington
WALTER B. JONES JR., North Carolina	JANICE D. SCHAKOWSKY, Illinois
PAUL RYAN, Wisconsin	DENNIS MOORE, Kansas
DOUG OSE, California	CHARLES A. GONZALEZ, Texas
JOHN E. SWEENEY, New York	STEPHANIE TUBBS JONES, Ohio
JUDY BIGGERT, Illinois	MICHAEL E. CAPUANO, Massachusetts
LEE TERRY, Nebraska	
MARK GREEN, Wisconsin	BERNARD SANDERS, Vermont
PATRICK J. TOOMEY, Pennsylvania	

---

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

MARGE ROUKEMA, New Jersey, *Chairwoman*  
BILL McCOLLUM, Florida, *Vice Chairman*

DOUG K. BEREUTER, Nebraska	BRUCE F. VENTO, Minnesota
MICHAEL N. CASTLE, Delaware	CAROLYN B. MALONEY, New York
TOM CAMPBELL, California	MELVIN L. WATT, North Carolina
EDWARD R. ROYCE, California	GARY L. ACKERMAN, New York
JACK METCALF, Washington	KEN BENTSEN, Texas
BOB BARR, Georgia	BRAD SHERMAN, California
SUE W. KELLY, New York	MAX SANDLIN, Texas
DAVE WELDON, Florida	GREGORY W. MEEKS, New York
JIM RYUN, Kansas	LUIS V. GUTIERREZ, Illinois
MERRILL COOK, Utah	FRANK R. MASCARA, Pennsylvania
BOB RILEY, Alabama	JAY INSLEE, Washington
RICK HILL, Montana	DENNIS MOORE, Kansas
STEVEN C. LATOURETTE, Ohio	CHARLES A. GONZALEZ, Texas

# CONTENTS

	Page
Hearings held on:	
July 20, 1999 .....	1
July 21, 1999 .....	59
Appendixes:	
July 20, 1999 .....	113
July 21, 1999 .....	358

## WITNESSES

TUESDAY, JULY 20, 1999

Barsness, Robert N., Chairman and President, Prior Lake State Bank, Prior Lake, MN, on behalf of the Independent Community Bankers of America ....	27
Barton, Richard A., Senior Vice President for Congressional Relations, The Direct Marketing Association, Washington, DC .....	33
Brice, Jack, member, AARP's Board of Directors, Decatur, GA .....	48
Cate, Fred H., Professor of Law, Harry T. Ice Faculty Fellow; Director of the Information Law and Commerce Institute, Indiana University School of Law, Bloomington, IN .....	16
Clayton, Gary E., President and CEO, The Privacy Council, Dallas, TX .....	14
Connelly, D. Barry, President, Associated Credit Bureaus, Inc., Washington DC .....	34
Culnan, Dr. Mary J., Professor, The McDonough School of Business, Georgetown University, Washington, DC .....	12
Davis, Robert R., Director of Government Relations, America's Community Bankers, Washington, DC .....	29
Kloiber, Michael D., President and CEO, Tinker Federal Credit Union, on behalf of The National Association of Federal Credit Unions and the Credit Union National Association .....	31
Litan, Robert E., Vice President and Director, Economic Studies Program, The Brookings Institution, and Co-director, AEI-Brookings Joint Center for Regulatory Studies, Washington, DC .....	11
Mierzwinski, Edmund, Consumer Program Director, U.S. PIRG, on behalf of the Consumer Federation of America, Consumers Union and U.S. PIRG ..	45
Rotenberg, Marc, Director, Electronic Privacy Information Center, Washington, DC .....	46

## APPENDIX

Prepared statements:	
Roukema, Hon. Marge .....	114
Vento, Hon. Bruce .....	116
Barsness, Robert N. ....	213
Barton, Richard A. ....	261
Brice, Jack .....	315
Cate, Fred H. ....	173
Clayton, Gary E. ....	164
Connelly, D. Barry .....	278
Culnan, Dr. Mary J. ....	147
Davis, Robert R. ....	231
Kloiber, Michael D. ....	244
Litan, Robert E. ....	125
Mierzwinski, Edmund .....	283
Rotenberg, Marc .....	294

## ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Vento, Hon. Bruce:	
Written questions submitted to Robert Barsness .....	119
Written questions submitted to Richard Barton .....	120
Written questions submitted to Fred Cate .....	121
Written questions submitted to Barry Connelly .....	122
Written questions submitted to Edmund Mierzwinski .....	123
Written questions submitted to Marc Rotenberg .....	124
Barton, Richard A.:	
"Marketing Online, Privacy Principles and Guidance" .....	267
Written response to questions from Hon. Bruce Vento .....	277
Cate, Fred H.:	
"The Public Record: Information Privacy and Access, a New Framework for Finding the Balance" .....	181
Clayton, Gary E.:	
Written response to questions from Hon. Bruce Vento .....	170
Culnan, Dr. Mary J.:	
American Express brochure .....	162
Written response to questions from Hon. Bruce Vento .....	158
Davis, Robert R.:	
Written response to questions from Hon. Bruce Vento .....	241
Kloiber, Michael D.:	
Written response to questions from Hon. Bruce Vento .....	259
Litan, Robert E.:	
The Regulatory Right-to-Know Act and the Congressional Office of Regulatory Analysis Act, April, 1999 .....	128
Written response to questions from Hon. Bruce Vento .....	145
Credit Union National Association, Inc., policy statement .....	331
CUNA Mutual Group, policy statement .....	336
Electronic Financial Services Council, policy statement .....	341
National Council of Investigation and Security Services, policy statement .....	347

## WITNESSES

WEDNESDAY, JULY 21, 1999

Becker, Brandon, Partner, Wilmer, Cutler & Pickering, on behalf of the Securities Industry Association .....	91
Fink, Matthew P., President, Investment Company Institute .....	95
Fischer, L. Richard, Partner, Morrison & Foerster, on behalf of the American Bankers Association, Consumer Bankers Association, The Financial Services Roundtable, and Visa U.S.A. ....	89
Gensler, Hon. Gary, Under Secretary for Domestic Finance, Department of the Treasury .....	65
Gramlich, Hon. Edward M., Member, Board of Governors, Federal Reserve System .....	67
Harding, Richard K., M.D., Vice Chairman, Clinical Affairs, Professor of Neuropsychiatry and Pediatrics, University of South Carolina, on behalf of the American Psychiatric Association .....	99
Hawke, Hon. John D. Jr., Comptroller, Office of the Comptroller of the Currency .....	69
Meyer, Roberta B., Senior Counsel, American Council of Life Insurance .....	93
Nazareth, Hon. Annette L., Director, Division of Market Regulation, Securities and Exchange Commission .....	72
Palmisano, Donald J., M.D., J.D., Board of Trustees, American Medical Association .....	97
Pitofsky, Hon. Robert, Chairman, Federal Trade Commission .....	70
Reider, Hon. George M. Jr., Commissioner of Insurance, State of Connecticut, on behalf of the National Association of Insurance Commissioners .....	73

APPENDIX

Page

Prepared statements:

Roukema, Hon. Marge .....	359
Becker, Brandon .....	493
Fink, Matthew P. ....	520
Fischer, L. Richard (with attachments) .....	474
Gensler, Hon. Gary .....	365
Gramlich, Hon. Edward M. ....	382
Harding, Richard K., M.D. ....	534
Hawke, Hon. John D. Jr. (with attachments) .....	394
Meyer, Roberta B. ....	505
Nazareth, Hon. Annette L. (with attachments) .....	443
Palmisano, Donald J., M.D., J.D. ....	524
Pitofsky, Hon. Robert (with attachments) .....	425
Reider, Hon. George M. Jr. ....	465

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Vento, Hon. Bruce F.:	
Consumer Coalition for Health Privacy, policy letter .....	363
Written questions for Richard L. Fisher .....	360
Gensler, Hon. Gary:	
Written response to questions from Hon. Bruce Vento .....	376
Gramlich, Hon. Edward M.:	
Written response to questions from Hon. Marge Roukema .....	392
Written response to questions from Hon. Bruce Vento .....	389
Hawke, Hon. John D. Jr.:	
Written response to questions from Hon. Bruce Vento .....	421
Pitofsky, Hon. Robert:	
Written response to questions from Hon. Bruce Vento .....	440
American Insurance Association, policy statement .....	539
MasterCard International, policy statement .....	546





# FINANCIAL PRIVACY

---

TUESDAY, JULY 20, 1999

U.S. HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS  
AND CONSUMER CREDIT,  
COMMITTEE ON BANKING AND FINANCIAL SERVICES,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:00 a.m., in room 2128, Rayburn House Office Building, Hon. Marge Roukema, [chairwoman of the subcommittee], presiding.

Present: Chairwoman Roukema; Representatives Royce, Leach [ex officio], Vento, Bentsen, Sherman, Moore, Gonzalez, Schakowsky, and LaFalce.

Also Present: Representative Lucas of Oklahoma.

Chairwoman ROUKEMA. We have a well scheduled, long, intensive hearing today, so we will get started.

We fully expect that there will be more Members arriving, although I am sorry they are not here at this moment. But we need to start this hearing. Let me assure all the witnesses that Mr. Vento and I and others will be listening very intently to everything.

Let me set the scene for this hearing today. I think it is an extremely important hearing. It is the first of two hearings on financial and medical privacy for this week. I fully expect that we will have several more hearings, as the privacy issue is both compelling and complicated. I don't think I have to go into a lot of detail about why the question of privacy is important. It touches all of our lives, and all the issues relating to them—financial, medical, or otherwise. Privacy is all-encompassing and involves literally, as I have said, every aspect of our lives.

During the consideration of H.R. 10, I worked with my colleagues Mr. Vento, Ms. Pryce, Mr. Oxley, Mr. LaFalce and Mr. Frost on an amendment to enhance H.R. 10 with what we considered to be workable privacy protections. In the end, the House approved that amendment by a vote of 427-to-1. The privacy provisions require banks, securities firms, and insurance companies to disclose their privacy policies and provide consumers with the ability to "opt-out" of sharing their non-public personal information with non-affiliated third parties. In addition, the privacy provisions in H.R. 10 prohibit financial institutions from sharing customer account numbers for the purpose of third-party marketing.

The question, of course, arises: Does this address all of the concerns relating to privacy? And it is quite obvious that it does not. In fact, Congressman Inslee—and I would hope that he would be

here shortly—offered an amendment during the Banking Committee markup of H.R. 10 which was much broader than the language contained in H.R. 10 as it passed the House. I would like to remind everyone that I supported that Inslee amendment at the time.

However, I do feel that first a comprehensive, rational discussion must be engaged in before we proceed further with issues relating to privacy. Such discussions and debates are necessary to ensure that any new legislation does not create unintended consequences, such as inhibiting an institution's daily operational needs, which is frequently cited as a concern by the industry.

Our hearings this week largely will focus on privacy as it relates to the financial services industry. Our financial services industry is growing rapidly. Services are being offered in many different ways, including over the Internet, which raises a host of privacy issues that this subcommittee, I believe, is compelled to address. The hearings this week are intended to be only the beginning of a series of hearings in order to give due attention and hopefully proper legislation in the future on this issue of privacy.

The debate has raised many questions regarding the extent to which we as consumers can trust that our financial, medical and other personal information is maintained in a confidential manner. A breakdown in that trust would result in severe consequences for the business world and for our economy. I think the business world and the financial services industry must understand that there is the danger of consumer backlash here. Consumers want to know who is collecting their information, what kind of information is being collected, and who has access to that information. For example, consumers may not object if their information is being shared so they can be offered a product or a service, but consumers do want to know under what circumstances such information is being shared. That raises the disclosure question: What is the definition of disclosure?

Further, consumers want to know how they can maintain a reasonable degree of control over who collects their personal information. And that, of course, leads to the sharing of information with third-party question and the question of information-sharing with affiliates. The industry has expressed significant concerns about new legislation that would have, as I stated, "unintended consequences" on their business operations. This is the time for industry to be precise as to what they expect the unintended consequences of limiting information-sharing with third parties to have on their business operations.

Rather than general rhetoric, I hope that we can be quite precise. I am sure those on the panels today and tomorrow will do that. The industry received a wake-up call last month when the Minnesota attorney general filed suit against U.S. BanCorp for practices related to sharing customer account information with third parties. The information was used for the purpose of marketing non-financial products and services, such as marketing of low-cost medical and dental plans that could be paid for by automatic debits from consumers checking accounts or automatic charges to their credit cards. Once aware of the practice, consumers expressed outrage. In a clear demonstration of market discipline, many institutions reacted to the U.S. BanCorp announcement by revamping their pri-

vacancy policies and committing to not engage in such third-party information-sharing practices. The U.S. BanCorp episode has become Exhibit A in this wider debate.

Along with financial privacy issues, the subcommittee will receive information on medical privacy. Concerns have been expressed by many groups that H.R. 10's medical privacy provisions will undermine the more comprehensive medical privacy initiatives currently being pursued on both sides of the Capitol. Many of these medical groups have suggested that medical privacy provisions be stripped from the bill. I personally do not understand the logic of this suggestion and believe it would be irresponsible for H.R. 10 to be enacted without fundamental privacy medical protections for consumers.

Now, let me emphasize that H.R. 10 is only a foundation. It is a beginning. It is more than a first step. It forms a foundation. I, too, favor more comprehensive privacy legislation. However, stripping H.R. 10 of medical privacy provisions in hopes that separate, more comprehensive legislation will be enacted is, I believe, most unwise. We shall hear from those medical groups tomorrow, groups with whom I have worked closely over the years on numerous issues relating to health concerns. I do not understand the logic of their position on this, but we will question them on that tomorrow.

Over the course of these two days we will hear witnesses from a wide range of perspectives, including Government, academia, consumer advocacy and industry. The witnesses will provide the information as I have outlined on all aspects of the privacy issue. We will examine what Federal and State laws already cover financial privacy and their protections. Furthermore, our witnesses will offer their expert opinions on how both consumers and businesses are affected by some of the privacy approaches currently contemplated by Congress.

I look forward to their testimony. I have every intention of using this hearing as the beginning of a more comprehensive review of laws and legislation that relates to all aspects of financial privacy as well as those that relate to medical privacy.

With that, I would like to recognize our Ranking Member who has played a very vital leadership role on the privacy issues, Congressman Vento.

[The prepared statement of Hon. Marge Roukema can be found on page 114 in the appendix.

Mr. VENTO. Thank you, Madam Chairwoman, for chairing the hearing. We have a significant group of witnesses who will explore the full range of privacy issues in our economy. Privacy is on the minds of consumers as they see the technological advances eroding barriers, linking data and shrinking the world and sharing their personal profiles with others. In many respects I think that they believe that the ability to maintain their privacy is greatly eroded.

In many respects, these two days of hearings are a continuation of our look at consumer financial privacy which began in September of 1997. We took that look with a slight focus on the impact of the Internet on consumer privacy as well. We also touched on many of the same issues we will have before us today: the adequacy of the Fair Credit Reporting Act, data security and identity

theft and information-sharing for marketing of products and services.

What may be different is that in these post-H.R. 10, post-“know your customer” days, we have finally become a very sensitized Congress and perhaps the public. With every day it becomes more clear that the American economy is running on data: personal data, consumer data. We collect, share and peddle profiles and preferences of people to run companies and enforce laws and sell products. But what voice and choice does any consumer have over their own personal and public data? What is the right balance of free flow of information versus privacy protection? Should the only choice a consumer has be that he or she not do business with a company or group of companies because he or she doesn't like their privacy policies?

Public concerns about personal information privacy, of course, as I stated, are growing. Each week there are new reports of stolen identities and credit cards, selling of financial data, “cookies” on the Internet sites, false IRS reports, hijacked ATM cards and numbers. Bad actors are still stealing mail to divert your account statements. Companies are using old-fashioned directories based on where you live in deciding whether to interrupt your dinner with a phone call. Grocery stores are compiling your complete eating habits just because you sought to save a few bucks by using a card. Charitable groups are sharing or selling lists of their contributors. States are selling driver's license numbers which often include your Social Security number. And the litany goes on and on throughout our lives.

No matter what we do or do not do here, the modern consumer must be vigilant about the information that is out there about themselves. We are in essence surrounded by unwanted junk mail, Internet spam, catalogs, and all sorts of material and telephone calls coming to us and, of course, knowing personal data about us that we would choose not to share.

With regard to financial privacy, that is, of course, of paramount importance. I think that the expectation of the public has always been that financial institutions, the entities with which we transact, have a higher obligation and usually one which they have met that standard.

Madam Chairwoman, I think that we have a very good work product which has passed the House of Representatives as an amendment that we worked out to H.R. 10 early this month. This product affords consumers new important safeguards for their financial privacy, putting banks, credit unions, securities firms and insurance firms at the forefront of most other U.S. sectors regarding privacy.

As passed, this measure provides strong provisions of law to respect and provide for consumer privacy with a privacy policy that meets Federal standards to protect the security and confidentiality of consumers and consumers' financial and personal information.

H.R. 10 prohibits the sharing of account numbers for the purpose of third-party marketing. This protection applies to all consumers and requires no action on their part. Consumers can opt-out, of course, of sharing information with third parties in a workable fashion that protects consumers' privacy while allowing the proc-

essing of services they request and that are required by virtue of the regulatory and accounting standards of any financial entity.

Importantly, regulatory enforcement authority is provided to the specific regulators of each type of financial institution to safeguard and to implement this policy.

This measure, H.R. 10, specifically prohibits the repackaging of consumer information. Data cannot be resold or shared by third parties or repackaged to avoid privacy protections. Consumers must be notified of the financial institution's policy at the time that they open an account and at least annually thereafter. Certainly these are major steps forward. These commonsense and workable provisions were added to the substantial provisions already included in H.R. 10 that prohibit obtaining consumer information through false pretenses and disclosing a consumer's health and medical information.

But, because there are those who would have liked to have gone further, some who wanted to eliminate provisions like the medical privacy protections in the bill, and because the issue of financial privacy is certainly larger than the financial institution marketplace, larger than H.R. 10 and financial modernization, I am hopeful that with these hearings we can begin to look at the big picture and then to act appropriately on the totality of privacy policy matters.

This Congress needs to step up to the plate and provide the legal framework for protecting consumer privacy. While it is appropriate to ensure that adequate policy safeguards are in place to protect consumer privacy in our changing financial marketplace, we need to look at all of the economic sectors—retail sales, commercial corporations, the Government at all levels—to understand how they all utilize information and private information about the individual.

As many of my colleagues are aware, I have worked on consumer rights and privacy. I have worked to protect consumer privacy through laws like Truth in Lending, the Fair Credit Reporting Act and the Electronic Funds Transfer Act. I also introduced one of the first proposals to protect the consumers' privacy on the Internet, the Consumer Internet Privacy Protection Act.

During the Banking Committee markup, I introduced an amendment that would have provided an annual opt-out on affiliate-sharing and beyond. I withdrew the amendment when I realized it was unworkable and there was much more that needed to be shaped in terms of financial privacy and policy issues.

What is clear is that a law that requires consumer action is appropriate. A third party and affiliate opt-out is hardly the first and last word in consumer rights. The fact is that the number of consumers that have such a right today under the Fair Credit Reporting Act or under various institutional policies. Even with that authority, only a small fraction of individuals exercise that option. Consumer choice may give us a warm feeling about what is appropriate, but what does it really accomplish? What is the bottom line? Does it really provide choice if a fraction of 1 percent responds to opt-out?

The bottom line must be the enforcement of the law. I note that we will have a witness from the Federal Trade Commission. Their

testimony at the Commerce Committee last week promoting continued self-regulation for Internet privacy protection underscores for me the deficiency of some of the proposals for H.R. 10 which superimposed the Federal Trade Commission as a privacy regulator. That approach would have given enforcement authority to the FTC as opposed to the appropriate functional regulator for each financial institution. I do not think we should turn over such an important enforcement authority to a non-financial institutions regulator. Indeed, the functional regulators today show every sign of eagerness and awareness and the will to make financial privacy law work.

Madam Chairwoman, I would entreat my colleagues and other witnesses that as we go forward, to first look to the breadth of the personal privacy issues in our economy. Financial privacy is important; however, privacy concerns are not limited to banks, securities firms, and insurance companies.

Second, look to the basics for consumers and business. People want to know what information is being collected, and how and why. People want to know how the data about them is being protected. People want to know how to correct false information. People want to know how the laws are enforced. Business wants a fair opportunity to provide options and to use information to better serve their consumers. Business wants a level playing field across economic sectors. Business wants to develop the means to keep data confidential and accurate. There has to be a way to bring both sides together that does not violate the privacy of individuals or jeopardize the flow of a smooth functioning economy.

Madam Chairwoman, we have a big task ahead of us. I think we have taken a positive step in terms of H.R. 10. I hope to preserve most of the provisions in conference.

I look forward to working with you, Madam Chairwoman, and I yield back the balance of my time.

[The prepared statement of Hon. Bruce Vento can be found on page 116 in the appendix.]

Chairwoman ROUKEMA. I thank the Ranking Member. That was a comprehensive analysis of what we have been addressing.

Now the Ranking Member of the full committee, Mr. LaFalce, do you have an opening statement, sir?

Mr. LAFALCE. I will be very brief, Madam Chairwoman. I certainly appreciate the opportunity to join with the subcommittee today, and I commend you for holding this hearing with so many panels over a number of days.

Issues of financial privacy have moved to the forefront of the debate over the financial modernization bill and moved to the forefront of the debate with respect to financial policy issues generally. Consumers have become increasingly concerned. Consumers have a right to expect that their private financial records will in fact remain private and confidential. And they have what has proven to be legitimate concerns regarding possible misuse of their private financial and personal information.

A number of Members of this subcommittee, Mrs. Roukema, Mr. Vento in particular, have authored privacy proposals to address these concerns, and a number of them were included by the subcommittee in the Financial Modernization Bill. Most especially the

amendment that was offered during floor debate that was adopted with almost unanimous House vote.

The amendment that so many of us worked on provides consumers with financial privacy protections that go far beyond anything in current law and well beyond the privacy protections available to consumers elsewhere in the economy. But the Senate version contains minimal privacy protections. We may, therefore, in conference with the Senate, face efforts to weaken what we think is absolutely essential. The financial privacy protections that we currently have, the House version of H.R. 10, that we may find difficulty in enhancing these protections, because a good many number of Members would like to enhance these protections, whether in conference or through other legislation under consideration.

So this makes the hearing today not only timely, but extremely important, Madam Chairwoman. But it is also important that we remember that the financial privacy issues joined in H.R. 10 are but a subset of privacy policy issues. It is not only financial institutions that are in a position to misuse private consumer information, there are a wide variety of commercial and high-technology companies, credit bureaus, marketing organizations, that have and use similar opportunities. Electronic commerce, on-line banking, the Internet, all bring tremendous benefits; but they also pose enormous challenges for those of us who would protect consumer privacy.

I hope that these hearings will provide us the opportunity to see the privacy within financial services within context so that we might be able to begin exploration of a broader array of privacy issues.

In addition, I think that recent discussions that I have had show there is some confusion regarding the privacy protections presently available in current law, whether it is under a statute such as the Federal Right to Financial Privacy Act of 1978, the Privacy Act of 1974, the Fair Credit Reporting Act, or various State laws. So I hope that the various panels that we have today and tomorrow will address some of these issues and clarify them in the course of the testimony. And I join you in welcoming the witnesses, Madam Chairwoman. Thank you very much.

Chairwoman ROUKEMA. Are there other opening statements, please?

Mr. Moore.

Mr. MOORE. I would like to thank you for holding these important hearings today and tomorrow. We have several different panels so I will try to be brief. These hearings could not be more timely, given the floor debate on the privacy provisions that could have been contained in H.R. 10. The debate three weeks ago in Congress highlighted the concerns we have about privacy in every aspect of our lives from the annoying phone calls, to the horror stories of entire lives being disrupted and destroyed from the wrongful dissemination of private information. These issues of privacy should be at the top of our legislative agendas.

We have great economic expansion and growth. Much of our recent success has been driven by our robust information economy and unprecedented technological advances in which consumers benefit from broad new sets of choices, efficiencies and quality services.

But the expansion of our technology sector and the consumer benefits that have come as a result of more and better services come at a cost to personal privacy.

You mentioned, Madam Chairwoman, the lopsided 427-to-1 vote on Representative Oxley's amendment which limits the ability of financial institutions to provide confidential information to unaffiliated third parties. By doing that, this Congress stated its clear intention to require our financial institutions to respect the privacy of their customers. These limitations on the use of personal information, though, should not be exclusively required of our financial institutions and this industry should not be singled out to bear the entire burden of congressional regulation over matters that aim to protect personal privacy. Many of our concerns are derived from our better and more efficient use of technology and increased access to information.

If we want to protect privacy, and I strongly believe that we should, we should do so comprehensively, as you have indicated, Madam Chairwoman, and not just impose a new burden on one industry that many of us voted just three weeks ago to modernize. We must not only act comprehensively, but we must act judiciously in our approach to these matters of personal privacy, particularly financial privacy. We must seek a balance between the ability of financial institutions to conduct their business under the new framework of H.R. 10 and the individual consumer's right to privacy. That Congress should also examine these important matters of personal privacy across all sectors of industry and commerce. While I understand that this subcommittee's consideration of this issue is primarily limited to the financial services sector, I want to again thank you, Madam Chairwoman, for your leadership in moving forward with these important hearings.

I hope that our colleagues presiding over other industry sectors will follow your lead and begin to comprehensively examine this privacy issue. I also appreciate your statements about the concern that a lot of Americans have about medical privacy. Again, thank you very much.

Chairwoman ROUKEMA. Thank you, Mr. Moore.

Are there other opening statements?

Mr. Inslee of Washington.

Mr. INSLEE. Thank you for your leadership, Madam Chairwoman, on this issue. First off, I want to tell you I have been in public life for ten years and I don't think that I have had an issue that has blossomed so rapidly and caught the outrage of the American public so much.

We started this debate on H.R. 10 a couple of months ago and I don't think that any of us understood the depth of the abuse of people's privacy, number one, and the people's outrage that that is going on. Because of that, I think it is important in these hearings today and tomorrow that we realize our discussion here and on the floor to H.R. 10 is not the end and it is even the beginning of the end, it is maybe the end of beginning of the U.S. Congress dealing with privacy issues, and I think that should be true in H.R. 10 as well, because I don't believe our work is completed on privacy issues in H.R. 10. And we are going to be talking to the conferees in the hopes that they can go further, and that is because we be-



lieve that there is unfinished business, unfinished in the sense of being able to guarantee consumers' privacy, at the same time allowing financial institutions to enjoy the benefits of consolidation that H.R. 10 will allow.

What I am hoping, and the second point that I want to make is that I hope that the folks who are going to testify in the next couple of days can answer this question. How can we give consumers what they are entitled to, which is the right to have banking information used for banking purposes and banking purposes alone if that is what they desire? How can we make sure that consumers have that right, while at the same time allowing financial institutions the use of that information to prevent fraud and the like that might be necessitated in certain instances?

The reason that I ask you to help us in that regard is because when I was trying to draft legislation, I tried to accommodate financial institutions. They said "We have to send the checks out to be printed, so you can't prohibit us from doing that," so we did an exception to that. They said "We have to have a situation if there is fraud, you have to give us the ability to share information," so we wrote an exception to do that.

We have to know how to draft legislation that will accommodate consumers' rights to use banking information for banking purposes and banking purposes only, not marketing purposes. Now, I heard many folks say "That is impossible. Can't be done." Well, in honor of today, July 20, let me refer to thirty years ago when we put a man on the Moon and, in a statement that has been used a lot in the last three decades, if we can put a man on the Moon, the U.S. Congress ought to be able to draft legislation that makes sure that consumers can use banking information for banking purposes exclusively.

And I am going to ask you to help us and not give us the response that people did not give President Kennedy, saying "It just can't be done, Mr. President." This can be done, and I hope that you will help us find a way to do it, to guarantee consumer privacy and allow the banks to move forward. Thank you.

Chairwoman ROUKEMA. Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Madam Chairwoman. I join my colleagues in commending you for the leadership role you have taken in this issue. I am going to be very brief.

The potential for this issue to derail passage of H.R. 10 financial modernization is very real, and that is where we are going to be focusing our attention. As Congressman Inslee has pointed out, this may be the launching pad to issues in other arenas. We ask for your expert help with this matter.

I look at the privacy issue like this: Technology is expanding. I guess it is really the backdrop. It has expanded, and it is forever changing the financial landscape. Our biggest challenge will be how we operate out there in the commercial world and how we determine what are reasonable and practicable expectations of privacy in today's society with the emerging technology.

I truly believe that you have anticipated this, and that will be the basis as we proceed to take into account technological advancement and what it has done to commercial enterprise and basic be-

havior and how such changes impact society's expectations of privacy.

I will use a quick example in the law, in that I was a judge and a lawyer for many years. At one time, consumers could expect their phone calls to be private. However, with introduction of cell phones, do you still have the practical and reasonable expectations of privacy if you are using it when you get on a subway? Of course not. You can expand this idea to financial privacy, and that is what we will deal with here today.

Thank you, Madam Chairwoman, and I look forward to the testimony today.

Chairwoman ROUKEMA. Thank you.

Now we must get on to this hearing, which I am afraid is going to be quite long. We were ambitious in setting up three panels. Let me just outline the procedures under the rules of the subcommittee, and particularly today with the extended number of panels and panelists that we have. First, I do want you to cooperate with the five-minute rule if you can. The light in front of you will tell you how to proceed; green to start, the yellow warning sign and then the red light when you should finish. If you can, please abbreviate your remarks. All of your written testimony will be submitted for the official record of this hearing. Again, we will do everything that we can to comply with the five-minute rule. I will also suggest to our subcommittee Members that we also comply with the five-minute rule.

Second, Members will have—especially since the time is limited—the ability to submit written questions to the witnesses for the further explanation of the issues. Those written questions will be submitted to the witnesses.

Third, the hearing record will be open for the usual period of time for the submission of additional information, and that goes for all of the panelists. In this regard, I have already received written submissions from several groups, including the Electronic Financial Services Council, the American Insurance Association, and the National Council of Investigation and Security Services, Inc., and I would ask unanimous consent for their written testimony to be submitted for the record. And it is so moved.

[The information referred to can be found on page 341 in the appendix.]

Now, the first panel of witnesses, we have academics as well as experts on privacy and known authorities in their particular fields. The first witness is Dr. Robert Litan, the Vice President and Director of Economic Studies at the Brookings Institution. He is the co-director of the new AEI-Brookings Joint Center on Regulatory Studies and co-editor of the Brookings-Wharton paper on financial services. I do thank you, Dr. Litan, for adjusting your travel schedule and being here today, and of course your written testimony will be submitted for the record.

Secondly, we have Professor Mary Culnan, from the McDonough School of Business at Georgetown University. She is a known authority in this area who has conducted various privacy studies, including one on Internet privacy policies that was conducted in the spring of this year.

Our third witness is Mr. Gary Clayton, who is the President of the Privacy Council and also Vice President and General Counsel and Senior Privacy Analyst for Stone Investments of Dallas, Texas.

And the fourth witness is Professor Fred Cate from Indiana University School of Law. He is the Director of Information Law and Commerce Institute at the School of Law at the University of Indiana.

Thank you all for being here, and without further delay we will have Dr. Litan.

**STATEMENT OF ROBERT E. LITAN, DIRECTOR OF ECONOMIC STUDY, BROOKINGS INSTITUTION**

Mr. LITAN. Thank you very much, Madam Chairwoman. Thank you for inviting me to appear here today. I apologize for not having written testimony, because the dog ate it.

No, that is not the reason. My extensive travels have prevented me from writing prepared testimony, but I will submit something after the hearing. Actually, these opening statements were so good that I am going to skip over the detailed notes that I prepared last night and get right to the heart of the matter.

I recently prepared a paper which I think your committee staff has called "Balancing Costs and Benefits of New Privacy Mandates" that I did for the AEI-Brookings Joint Center for Regulatory Studies, and I am going to summarize some of those points which are relevant to your inquiry today.

[The paper referred to can be found on page 128 in the appendix.]

First, policymakers, including Congress, should be cautious about legislating in this area because of rapid technological change.

Second, Congress should not hesitate to legislate where there is evidence of market failure as long as the steps that it takes do not create unintended side effects that are worse than the disease. I think the opening statements have eloquently demonstrated that there is a market failure here and that something needs to be done.

The third point, and this is the most important, and something that I learned from Fred Cate in a book he wrote for Brookings several years ago, is that United States law has never made privacy an absolute right, as it more or less is in Europe. Instead, we have balanced the benefits of privacy protection against the costs of providing it and have selectively legislated.

There are other things that we worry about. We want to catch crooks. We have a guarantee of free speech. We want to prevent fraud and so forth. I would encourage the Congress to continue this balancing approach. Indeed, I believe that H.R. 10 reflects this approach and I applaud Congress for moving cautiously in this area.

H.R. 10 implicitly recognizes that there are benefits to the sharing of information that have been referred to. We want to reduce the cost of credit. We want to prevent fraud. We want to have third-party processing in many cases. The heart of the privacy-related complaints really center around the sharing of information for marketing purposes. That is the problem.

H.R. 10 addresses this problem by providing a notice and opt-out requirement that extends only to third parties, but not to affiliates.

The financial industry is strongly opposed to extending this provision to affiliates. I think this opposition is shortsighted.

One of the things that make financial institutions, and especially banks, unique is that consumers have a strong degree of trust in them. You abuse that trust, you lose the business. Now some say "Let the market take care of this. If banks want to abuse it, that is their problem, not the industry's problem." I beg to differ. The problem in this area is that as more and more stories appear about banks abusing information, consumers can sour on the whole industry, so there are what economists call negative externalities associated with the abuse of information.

So I think it is in the interest of the banking industry to have the privacy provisions extended to affiliates. In fact, I think it would save them money. When you are doing direct marketing, the last thing you want to do is send out a bunch of calls and mail to people who are never going to respond. Why not save yourself some money up front by at least having those people who don't want to hear from you identify themselves? We have heard that this is a relatively small fraction of the population anyhow. Banks would save money if they knew ahead of time that certain people in their database they should not approach. Indeed, those people are likely to be offended when the bank bothers them.

In fact, I have come around to the view that I think a notice and opt-out ought to be mandatory for all businesses doing interstate commerce, not just on the Internet where it has come up most often; but why make a distinction between business on the Net and off the Net? For all interstate commerce, why not a minimum notice and opt-out requirement? Same argument. It is in people's interest, it enhances trust. We had a \$50 credit limit on credit cards many years ago that basically allowed that industry to take off. I think enacting something like a minimum notice and opt-out will do the same thing for Net commerce—enhance its growth.

I also think a broad notice and opt-out may help solve this dispute that we have with the EU over privacy. I think if we told the EU, this is what we are doing, we have a minimum cross-the-board rule, although it is not the same as yours, at least we are paying attention to the issue. I think we would have the moral leverage to finally get this argument resolved.

So I would encourage Congress as it goes forward in the negotiations on H.R. 10 to have a stiff back on this issue. Thank you very much.

[The prepared statement of Robert E. Litan can be found on page 125 in the appendix.]

Chairwoman ROUKEMA. Thank you.  
Dr. Culnan.

**STATEMENT OF DR. MARY J. CULNAN, PROFESSOR, THE  
McDONOUGH SCHOOL OF BUSINESS, GEORGETOWN UNIVERSITY,  
WASHINGTON DC**

Ms. CULNAN. Thank you very much. Thank you again for inviting me to testify. I would like to second Bob's points, but I am going to present my own from a slightly different perspective since I am not an economist. The basic issue here, I think, is disclosure, not really privacy. Consumers will disclose personal information that is

needed to drive the information economy if they perceive that the benefits of disclosure exceed the risk. So it is up to the business community to make the argument that there are benefits to having the information used, and then to also make the argument that this is a low-risk proposition. By observing fair information practices, risks are reduced and therefore, this promotes disclosure. So protecting privacy is really good for business.

One of the risks that comes up is incompatible use, as Bob Litan said, the idea that information is collected for one purpose and used for other unrelated purposes—information-sharing for marketing purposes is a primary example—when the information was not explicitly collected for that purpose.

We are familiar with the results of information-sharing among affiliates. I received a phone call Sunday night from—the source of the information was First USA. It was one of their affiliates, and they offered me two free airline tickets to anywhere in the country that I wanted to go to introduce me to this organization.

I think the current language in H.R. 10 does not adequately address the privacy concerns raised by the incompatible use for two reasons. First, it does not require the privacy disclosures to reflect the core elements of fair information practices. My recent survey of privacy notices posted by commercial Web sites clearly reflects the inadequacy of the majority of these privacy disclosures absent any core standards or core requirements for what the notice is to include.

And second, H.R. 10 does not include an opt-out for affiliate-sharing. I disagree with the argument that by disclosing privacy practices or privacy policies, the consumers can then choose among organizations by selecting the ones that have a policy that they perhaps find acceptable, because if the trend toward these mega-conglomerates materializes, this is really a false choice. Offering an opt-out will not mean an end to the information economy, because information about consumer choices and behavior can still be analyzed and shared in the aggregate for making marketing decisions.

The majority of consumers do not opt-out, but they value having the choice, and observing fair information practices addresses the privacy concerns that information-sharing raises. If really good notice and choice are given and people don't take the choice, then business organizations can feel free to go ahead and share the information and use it for marketing.

On the other hand, I think a failure to offer an opt-out for affiliate-sharing really is at odds with all of the self-regulatory programs that the other industries have been working hard to advance and that a lot of American's best companies have instituted on their own.

I also would like to say a few words about Internet privacy, because I think the Internet raises some unusual different issues than we find in the off-line world. On the Internet our behavior can be tracked even when we don't engage in any transactions or raise our hand in the marketplace. What we are learning is that when Web sites ask people to disclose information and don't tell them how the information is going to be used or offer choices about the subsequent use, what people do is refuse to disclose the information or they lie. So once again we have evidence that observing fair

information practices is really good for business because it promotes disclosure and trust and confidence.

While privacy is important to the success of e-commerce, it is important that any regulatory solution takes into account new Internet business models that involve information-sharing to benefit consumers, so I would urge not to rush to legislate without thinking through the implications for electronic commerce.

In conclusion, there are two things that you can do. One, charge the financial regulators such as the OCC to convene a series of workshops that bring together a lot of stakeholders to discuss the issues such as the ones that Mr. Inslee raised in particular, and to conduct research as necessary, and report back to Congress on a regular basis on the need to regulate or not. And I think this should be done independent of what happens to H.R. 10.

The FTC has had a similar process in place for a number of years. I think it has been very effective in terms of developing views, understanding the issues on both sides and moving the process forward; particularly it has jump-started a lot of private sector initiatives, and I think the same thing could possibly happen in the financial institutions industry.

I would also like to say briefly that technology has changed the nature of the public record. I think we need to have a national discussion about this in terms of how they benefit our society and the different ways that they are used, and to look at the current balance between privacy interests and other societal interests, and I would urge you to perhaps launch this discussion.

Thank you very much and I will look forward to your questions.

[The prepared statement of Dr. Mary J. Culnan can be found on page 147 in the appendix.]

Chairwoman ROUKEMA. Mr. Clayton.

#### **STATEMENT OF GARY E. CLAYTON, PRESIDENT AND CEO, THE PRIVACY COUNCIL**

Mr. CLAYTON. One of the things that is very difficult, and I empathize with you, how do you try to shape something that is so fluid and changing so quickly? I work with people in California and Austin that are taking technologies and changing the way that businesses are providing services. And the issue of privacy is something that I don't know how you answer the question. There is no one single answer, and it is going to change with time.

Mr. Vento made the appropriate response: Information is driving our economy, it is going to be used in ways that we never thought about before. And we see ourselves contrasted with Europe. The Europeans have taken the idea that the government can step in and form regulations and dictate how the knowledge and information is used in their society. I don't believe it will work. Technology will leave it behind.

I believe what you need to do is to be cautious, to take time to understand and study these issues, because what is going to happen, the answer today is not going to be the answer tomorrow. There are going to be new technological threats to our privacy and changes to the way that we provide services, and we don't want to undermine the thing that is driving our economy.

I would also encourage you to look at the way that the Europeans are attempting to draft their own legislation and implement this. It is in marked contrast to what we are doing in the United States. The frustration may be that we don't have one national legislation effort to resolve all privacy issues. The Europeans have tried that, but the problem is that when you do that, one size does not fit all.

We are talking about personal information and it is very fluid because it is knowledge. It changes with how it is used. It changes with how industry wants to use it. And it varies from individual to individual. Privacy is not and never has been a fundamental right in the United States in the sense that it is written in the Constitution. It is a secondary right. It is one of those things that is protected by other fundamental rights.

In Europe they claim that it is, and I will tell you that I have spent a lot of time over the last two years, and I have studied and lived in Europe. It is not something that they consider a fundamental right. We are just as concerned in the United States about privacy. They view government's involvement in having information in Europe very different than we do. They allow and accept that. One needs to travel to London to see the government uses of close captioned television with no concern about privacy issues.

In the United States we need to be very cautious about looking at what they have done in Europe and drawing some distinctions, because I think what has to happen is we do have to regulate by industry sector, and there is going to be a consensus formed that some issues have been resolved. And in the written statements that I talk about, I believe there are some general understandings about what privacy things are needed.

Notice: We go through the various things in the paper talking about consent. Notice is very important, and I would agree that you should extend the idea and require very specific notice be given about what is going to be done with information, because one of the things that I am most optimistic about is that this power of the new technology we have empowers individuals, and I think our economy is a reflection of people who have now gotten access to information of all sorts that we didn't have.

One of the things that you can enhance the empowerment of individuals by doing is to require financial institutions to disclose what they are going to do with the data. I think that applies to their affiliates as well. When given that choice, if a consumer decides to do something or not do something, that is up to the individual; but Congress should be very wary about stepping in and attempting to regulate it with great detail. I think encouraging public debate like the FTC has done is a very valid role.

One other point. Over the last two years a lot of industry organizations have gotten together to discuss this, to debate the ideas and to bring other people in. One of the groups that has been missing from those debates has been the financial institutions, and I am not certain for the reason about that, but maybe this subcommittee, through H.R. 10, or Congress can encourage through the regulators, encourage financial institutions to get more involved in the privacy debate and allow the free market ideas to come up with some solutions. I think it is too early right now to

have those, and I believe H.R. 10, in calling for a study to do that later, is entirely appropriate.

I would urge you to be cautious because I think you are attempting to regulate something that is too powerful and too useful for our economy, and that is the way that information is used. Just be very cautious. Thank you.

[The prepared statement of Gary E. Clayton can be found on page 164 in the appendix.]

Chairwoman ROUKEMA. Thank you.

And Professor Cate.

**STATEMENT OF FRED H. CATE, PROFESSOR OF LAW, HARRY T. ICE FACULTY FELLOW, AND DIRECTOR OF INFORMATION LAW AND COMMERCE INSTITUTE, INDIANA UNIVERSITY SCHOOL OF LAW, BLOOMINGTON, IN**

Mr. CATE. Thank you very much, Madam Chairwoman and Members of the subcommittee, it is a pleasure to be here. Coming last always presents the question of whether I say what I intended to say or I merely respond to what has been said before, but I think there is so much similarity I may be able to accomplish both.

Let me start with the same points that Bob Litan did. First, we see the essential role of information in this economy. We would be mistaken to think that when we talk about protecting privacy by restricting the flow of information we are not also talking about costs involved. These costs may be well worth it—recognizing those costs do not automatically lead to the conclusion of what should we do—but it at least suggests the importance of making sure when we start regulating this essential infrastructure that we be frank about the extent to which we are in fact affecting the cost at which services and products are provided, and also the unanticipated consequences of those regulations.

I know this is a phrase that you hear a lot and probably don't like hearing very much, but what we have seen in every area where we have seen regulation, and particularly in the States, and this is reflected in my written testimony, that there are ramifications of regulations to protect privacy that nobody thought of, that nobody considered were going to be likely until after the law took effect.

Now this seems particularly likely in the case of financial information because of how central it is to our society, and because of how far-reaching it is: when you touch any part of this web of financial information, the entire web vibrates, that the ramifications are likely to be quite significant.

I think H.R. 10, which in many ways offers excellent privacy protections—and I will return to those in just a moment—gives some clear examples of where these sort of unanticipated consequences might come from. How does H.R. 10 interact with the Fair Credit Reporting Act? Do H.R. 10's prohibitions on non-affiliated third parties regarding disclosing financial information also apply to credit reporting agencies? Does H.R. 10 preempt States from acting in this area? What about affiliate information-sharing, a subject on which H.R. 10 is silent, appropriately so at this point? But where does that leave us for the future debate? Is affiliate sharing now presumptively all right? Where does State law fit in there?



The debate on affiliate versus non-affiliate sharing is mystifying to me, but mystifying in the sense that many banks today, many financial institutions offer services through affiliates, services which the customer would never know were coming from a different organization. A credit card, a bank account, an overdraft credit protection account, a mortgage account may all come from different affiliates of the same institution. My guess is, certainly my own view is that most customers would not be miffed to receive marketing information for a related product.

So if, for example, I am seen to be carrying a high balance month after month on my credit card, I would receive a notice saying I could have a second mortgage on my home at a substantially lower interest rate, I don't think that is the type of thing that most consumers would think of as surprising, whether or not that comes from an affiliate or simply a division of the same company.

I think consumers experience concerns when the marketing is for an activity or a service that is unrelated to the banking industry, unrelated to the financial service. And so to some extent, I think this focus on affiliate versus non-affiliate is in many ways missing many consumers' concerns.

I want to conclude here by picking up on Bob Litan's point, however, about do we see here a market failure. If we start with the assumption that if the market is working well, then notice is what is key; and H.R. 10 certainly requires that notice, and it is commendable for doing so. Do we see a reason to go further than that? I would argue that we do not yet see that—first of all, that we are in a period of dramatic change; the FTC's conclusions with regard to online privacy are quite applicable here as well.

Second of all, I am not as ready as some of the prior witnesses to dismiss the bank's self-interest here. We see banks now responding to the publicity of the past year. We see seven major national banks have appointed executive level privacy—what the industry is calling "czars." We see the announcement of Bank of America that it is not going to market data to non-affiliated entities. I think the self-interest of banks in having that trust relationship preserved, not only for the handling of customers' money, but also for the handling of customers' data has, in fact, some significant room and should be given a chance to grow.

And finally, just to touch on Mary Culnan's point, electronic commerce, I think, also suggests a reason to be very cautious here. Financial services promise to be a central component of electronic commerce for two reasons: one, because we have to pay for the things that we purchase online, and second of all, because of dramatic cost savings available when we do our banking online.

On the other hand, the very things that we most need in the online environment—the verification, identification, authentication so we know who is on the other end of the transaction—depend on that ready access to a pool of information, just like check clearance and credit authorization services do. So my recommendation to you is not that this is not an area for attention or for enforcement of existing laws, but rather that, at present, we don't see the need for additional law.

Thank you.

[The prepared statement of Fred H. Cate can be found on page 173 in the appendix.]

Chairwoman ROUKEMA. We are going to be having a vote. I think I can get in my five minutes here—I think. And then we will have to recess for the votes.

Mr. Cate, I thought I understood you until you made your last statement. I think there has been a pretty definitive statement regarding the exceptions to practices with affiliates. Mr. Clayton disagrees with that, I believe, but I am not quite sure that I understand why you disagree.

It sounds like a general statement. It seems to me just the logic of it goes with Mr. Litan, as well as Ms. Culnan, you mostly agree with that. I don't know that you have definitively stated that. But let me ask another question, OK, for anyone, particularly to Mr. Litan and Professor Culnan, to respond to.

You have talked about the affiliates, but none of you have referenced the statement of the industry that exceptions are intended to protect industry practices. How do you respond to that? What industry practices are they speaking of and why does that justify the exception?

Mr. Litan.

Mr. LITAN. Actually I have this in my notes, and I skipped over it. If I were drafting a bill, I would take a different approach. Rather than having a broad requirement of opt-out and then a list of exceptions which can get incredibly complicated. I would take a much simpler approach.

I would just simply say that there is a requirement that there be an opt-out for information transferred for marketing purposes, period. Just make the language a lot simpler. The bill already identifies customer account information or identifiers as being prohibited for transfer for marketing purposes, so that principle is already embodied in the bill. I would just make it clear.

Chairwoman ROUKEMA. I think that—as Mr. Vento said, I think that is in the bill, but I don't know whether or not that is precise or tight enough. But we can discuss that further another time.

Professor Culnan.

Ms. CULNAN. I agree.

Chairwoman ROUKEMA. You agree that the bill is probably adequate?

Ms. CULNAN. No, I don't state that. I am agreeing with his point that the opt-out should be required for marketing purposes. I think that is a concern to people when they do not have a relationship with an organization, they do not believe it is a related organization; it is a different organization in their view. They may not be interested in hearing from this organization. Related use by the bank is fine. People don't have a problem with that.

Chairwoman ROUKEMA. Please review the language in H.R. 10 and see where that might be insufficient for your statement now.

Mr. Clayton.

Mr. CLAYTON. If I gave the impression that I was disagreeing with them, I do not. That was sort of my point. I would agree if you try to start listing a litany of exceptions you are going to—it is impossible. And my point was, I think if you make it an understanding about if you give consumers the ability to learn who is

going to get the information, and then limit it, as they are describing, I think that is sufficient.

Ms. CULNAN. In my own case, the one example was an affiliate of the credit card company that marketed me for a service that had nothing to do with my credit card and was for something I was not interested in. And just because they were an affiliate, I thought that I should still be able to opt-out of that.

Chairwoman ROUKEMA. Thank you. I appreciate, Mr. Clayton, your clarification.

Professor Cate.

Mr. CATE. I believe I agree, if I understand what this has been interpreted to mean, which is that it would be preferable rather than to distinguish between affiliate and non-affiliate data-sharing to simply say there would be an opt-out for data-sharing for marketing purposes. Then I understood the addition to be marketing an unrelated service or product.

Chairwoman ROUKEMA. I would appreciate your help in terms of defining that in legal language in the bill, because I do not believe that the bill is precise enough. All right? I thank you for that.

And I believe that we will have to recess now. We have a vote which will be followed by four five-minute votes. So we will be in recess for at least probably half an hour. We will be back within half an hour.

[Recess.]

Chairwoman ROUKEMA. I do apologize to everyone, our panelists and our observers here. That was far longer than a half-hour, and I am sorry for that. We were given the wrong information about the numbers of fifteen-minute votes and five-minute votes, but I believe now we have a time period here when we can make some progress, as they say.

I have used my five minutes, and again I would remind all our Members of the subcommittee that we are going to try to stay in every case with the five-minute rule because of the extended numbers of panelists that we have today.

And so with that, I will yield to the Ranking Member, Mr. Vento.

Mr. VENTO. Thank you, Madam Chairwoman.

Dr. Litan, you point out that the desirability of opt-out—of course, opt-in we sort of invented those words in this subcommittee, because obviously they are quickly gone by in terms of others, and you don't differentiate between an affiliate and a non-affiliate type of circumstance, suggesting that there is more commonality than difference.

Nevertheless, suggestions have been made that we might all do well to back up and say, we know what we are trying to do in terms of privacy, but is this a good tool, opting-out or opting-in? Or are we better off placing an affirmative responsibility on the financial entity to, in fact, accomplish that privacy?

Mr. LITAN. Are you specifically asking me my views on opt-out versus opt-in?

Mr. VENTO. No. I expect that opt-in is a lot more effective. In any case, the options that we have before us at this point at least, are wide open. But what about placing affirmative action on the part of the financial entity versus opt-out, which gives us less than 1

percent of the Fair Credit Reporting Act, a fraction of a percent which actually opt-out?

If it were written in less than halftones on the back of the statement, maybe consumers would respond differently, but I know what the numbers are today.

Mr. LITAN. I think over time the numbers are going to change as people become more aware of what information is out there. The difference between opt-out and opt-in, of course, is that with opt-in you certainly have more protections, but it is also a lot more costly. There are all kinds of potential unintended consequences from an opt-in requirement, and that is, you may not get a lot of information from individuals that you really need. In particular, if there are legitimate uses for fraud prevention and so forth, you may not get the information that you need.

So I think it is premature to consider an opt-in. It may be five years from now we find that an opt-out requirement does not provide enough protection, but I think at this point it would jump the gun too far to go to an opt-in.

Mr. VENTO. Trying to get some different issues on the table, the other side is that—I can remember as a kid taking the streetcar and seeing these advertisements in the public transit system, and they talked about the virtue of advertising and the way that it communicates and informs, implying if we didn't have it, we would still be using washtubs and scrub boards, and so the education age of our society.

The converse of some of this reflects some conduct on the part of financial institutions where not only are they not sharing it—in other words, they are keeping all of this information, rather than sharing it with credit bureaus. They are not sharing it at all, so you are then limited in terms of trying to go to X, Y, Z, and say, “we want credit.” They say, “we have an incomplete record of your transactional background, because it is not shared as broadly as it once was.”

Mr. Clayton, do you have any comments on that phenomenon?

Mr. CLAYTON. You have hit on the point where in an Information Age economy, we are dependent on the information and having a thin file or no information is tantamount to not being able to get credit and do business.

Mr. VENTO. As a State legislator, I recall writing laws that gave the actuarial experience to everyone so they could bid for health insurance purposes, because the health insurance companies would not share the information, and as a consequence, there was no competition. So we had to actually write laws to say, you have to give the actuarial experience on a broad basis.

So I assume, under this, there has to be transactional information for credit bureaus. We may be in a situation where we are going to compel a financial entity to share information, but with that goes an affirmative responsibility to determine how it is used. There are confidentiality agreements and privacy agreements and other factors that have to be in place.

For instance, Ms. Culnan, you referred to the fact that you are being contacted with regards to free flights, but on a credit card basis, one of the very common ways of gaining your points is through, in fact, the credit card transaction. They have to share

that information so you can get your frequent-flyer points on American or Northwest.

Do you have any comment?

Ms. CULNAN. One of the differences—I am a big fan of frequent-flyer programs, and I often joke, if you give me frequent-flyer miles, I will tell you anything you want to know. But the big difference is, I signed up for these programs. The benefits in that case exceeded the risk.

In this case—first of all, I am not sure that I was being offered a free airline ticket. In the second case, the information was being used for a use that I had not been told about.

Mr. VENTO. One of the issues is the universality. If we have a different circumstance for financial institutions, Internet, it makes it more difficult to understand it, so it argues for universality in terms of the policy, so this all fits together. That is obviously something that the industry has been trying to avoid.

I yield back the balance of my time.

Chairwoman ROUKEMA. I wonder if the Ranking Member would take over the Chair while Mr. Gonzalez asks questions. I have a very important phone call to make.

Mr. VENTO. [Presiding.] I would be delighted to. We will reserve the gavel for you, and I will give it back.

Mr. GONZALEZ. Thank you, Madam Chairwoman.

There is a general principle being suggested that we would have an opt-out for any marketing or any related purpose. That is what I gleaned from this.

Under that scenario, what do you see as any difficulties that a financial institution may encounter if, in fact, we have this in place, as a practical matter?

Things are happening out there, and again I am going to get back to what—in today's commercial world, what does the average citizen customer expect? What are their expectations of privacy when they fill out those forms?

When I talk to my constituents, I ask "What if you went to Frost Bank and opened a checking account, and they have a security arm in Dallas, Texas and they use that information to identify you as a potential customer for securities. Does that upset you to get a brochure from Frost Bank telling you about securities operations in Dallas?" They say "no." What they do object to is if they get something in the mail that is totally unrelated—a travel club that has no relationship to the financial institution. But under your scheme or suggestion, if you can tell me, what do you see is the downside?

Mr. LITAN. Well, I see virtually no downside. The banks would have a database, and for individuals that have said that they are going to opt-out, they would be segregated in that database. It is all on computer anyhow, and I don't think that it is a big deal to have separate identifiers. I actually think that the banks could end up saving money, because they would know that certain consumers don't want to hear from them.

I tend to agree that most consumers probably don't care that they have been identified by some information that they have provided, but consumers ought to at least have that choice as to whether or not this information should be shared.

Ms. CULNAN. I would agree. One issue is, they would have to come up with a definition of unrelated use and how many of these there are.

The second issue would be, how many choices to give the consumer. Are you going to give them a couple or three choices as some credit card companies do, or do you give them a whole list, and it becomes so overwhelmingly complicated that people lose interest. Also, how to communicate this to the consumer and make the choice easy for the consumer.

There is opt-out and then there is a good opt-out. We don't have a lot of good opt-outs in this country, and that would go a long way to improve the situation where it was a lot easier to make the choice.

If you look at the Harris Survey data, if you look at the differences when people are given notice and choice, whether or not they opt-out, privacy concerns go away because people have been told and are informed.

One of the issues is just the feeling that things are fair; even if you choose not to exercise the choice, the choice remains with you and you can make it at a later time. That goes a long way to remove the privacy concerns, and that is why I think that some of the opt-out rates are so low. People just do not want to be surprised.

Mr. CLAYTON. I think the problem is going to come when you start trying to define things like "unrelated services." as technology continues to blur the lines between personal information, public information, how it is shared, services are going to have the same thing. And I will tell you, the Internet world, one of the powers of the Internet world, it is blurring these lines of distinctions. You have AOL offering all sorts of things, and you have all sorts of various Internet companies which start out with one facet that they are offering and are sharing information on things that consumers want. I see a world—the Internet world is, how many e-mails do I have to get to give me information? How many times do I opt-out? I don't want to get constant, constant notices.

On the other side of this, I agree with her that you have got to have power to make that decision for yourself, and if you give me the information, maybe it is not opt-out or opt-in. Maybe the decision is that I do not do business with you. That is the ultimate opt-out or opt-in.

Mr. VENTO. If the gentleman from Texas would yield to me on that point.

I think it is a very good point. If you begin to look at not just services and related services, some of those related services are indeed the problem. Later on, the Consumer Union or Federation testimony will indicate that some of the related services like credit insurance and credit card insurance and credit life insurance are really selling services that are very questionable in terms of whether they are even usable. But that sort of propounds the whole issue: Can you protect an individual from themselves?

Some of this is, we go through all of this Truth in Lending regarding the terms and benefits, and it has to be open; and then the question comes back to whether or not we should eliminate or insulate people, because if we advertise or solicit them, they might vote

Democratic or Republican. The fact of the matter is, in terms of trying, they might buy that blue horse.

So the issue is that is what it gets back to. I don't know if the service, as an unrelated services issue, is going to be quite what we want in terms of—I appreciate the gentleman yielding. I know that he had little time. You are still recognized, clearly.

Mr. GONZALEZ. Professor.

Mr. CATE. Let me associate myself with a couple of prior points. One is that the definitional problem, which is the major issue facing the subcommittee or the legislator who drafts that is, how are you going to define that?

Second, how are you going to track those preferences so when information is supplied, for example, from a financial institution to some other institution? Data, as you well know, is often aggregated, and we should think about the cost involved in attaching preferences to how that data is used and how that will be maintained in subsequent database banks.

Third, going back to the point that Mr. Clayton made, opt-in and opt-out are clearly not the only two options here. One option is, in a competitive market, walking away from the deal, and of course, that goes back to, do you know what the terms of the deal are, which the provisions of H.R. 10 make that clear. It requires the posting of a privacy policy, which makes that particularly important.

Fourth and finally, I think we have to keep in mind that there is some sense of fairness between the customer who opts-out and the customer who does not. Presumably the reason banks are wanting to share this information and to market it is because it generates revenue, and therefore, customers who opt-out of this are presumably not participating in that form of revenue generation for that entity. So to require the bank or company to do business with someone who does not, in fact, share the same profile in terms of if their data is being used, nor is it contributing to the overall revenue of the institution, strikes me as raising a fundamental fairness issue.

Mr. GONZALEZ. Thank you very much.

Mr. LEACH. [Presiding.] Mr. Bentsen.

Mr. BENTSEN. Mr. Chairman, I would be happy to yield to the distinguished Chairman if he had questions.

Mr. LEACH. I would be happy to yield to you. You have been here much longer.

Mr. BENTSEN. Relatively speaking. I thank the Chairman.

I have a couple of observations. What I think we tried to do in H.R. 10, what is the point of creating a holding company and acquiring affiliates if you are not going to be able to share information for marketing purposes amongst them, as well as transactional information, which I think some of you have addressed briefly. But there is a transactional consideration, as well, in creating a financial supermarket that someone may or may not want to go into.

I know that some have argued that this is the wave of the future. We are only going to see these financial conglomerates. I think there still is a pretty broad market out there.

Furthermore, as my colleague brought up, the issue of credit life insurance or credit insurance and things like that, of course, cur-

rent law allows all of those things to be marketed. I get marketing phone calls constantly from the bank I do credit card business with on all sorts of insurance products in which I have no interest. That is one point.

The other is, the sort of functional aspect of this in an opt-out, and I would like you to think about this and comment about this.

Ms. Culnan talked about the credit card industry, and I think American Express and some others—and I don't want to pick on American Express—they now have a mandatory arbitration over disputes that went into effect if you used your credit card; and it was, of course, noted in the bill. I will be the first to admit I didn't happen to read it in my bill. I am not sure anybody who may have been a card holder for some time read it or not. I am sure that it was in there in the amount of data that you get, but most people tend to look just at their statement, whether or not they made the charges, how much money they have to send in. And there is some practicality, I think, to having some specifics set out, because disclosure is good in that it is done, but it is also only so good as people will actually see it and notice it.

And I think what we tried to do in H.R. 10 was to slam the door on transfer of data to third parties, prohibiting some outright and limiting others as well. And I would like you to comment on the practicality of this. We can have all of the opt-outs in the world and nobody might ever see them, and so they would be rendered useless as a result of that. So I would like you to comment on that.

But first of all, I still don't know, and Mr. Litan who I have the greatest respect for, I still don't know what the problem is, from a marketing standpoint, of an affiliate that is a controlled affiliate of the holding company that you have decided to do business with, marketing material that you may not want, other than the nuisance factor?

Mr. LITAN. Well, again I think it comes down to a fundamental issue of choice and whether the consumer ought to have a right to opt-out of that.

Mr. BENTSEN. If you will yield, they do still have the choice of the 10,000 bank holding companies that they can go down the street to Acme Bank and Trust that may not be a holding company.

Mr. LITAN. In a world of financial conglomerates that we are headed toward, there may be only a handful of those. The reality, I think, is, there are multiple attributes that consumers look at when they look at financial services. They look at price, convenience, and privacy will be one among many attributes. I am concerned that privacy will get lost in the fine print and a lot of consumers will not make intelligent choices based on privacy.

I don't think that there is any rational distinction between affiliates and third parties if you accept the proposition that consumers ought to have a right to at least have a choice. Why should it make a difference whether it is an affiliate or non-affiliate?

Chairwoman ROUKEMA. Mr. Bentsen, you were not here earlier when we made the point that we have an extensive number of panels and panelists, and I have been quite precise in holding people to the five-minute rule. I will give you one more minute.

Mr. BENTSEN. Do you consider affiliates and subsidiaries the same?



Mr. LITAN. Yes.

Mr. BENTSEN. For privacy information?

Mr. LITAN. Yes.

Mr. BENTSEN. Thank you, Madam Chairwoman.

Chairwoman ROUKEMA. Mr. Inslee, please.

Mr. INSLEE. Thank you. I would like anyone on the panel to address this Federal preemption issue. There is a State legislative hearing on Friday in Washington because there is great concern that this will preempt an ability in the State of Washington to have an opt-in or opt-out for affiliates, or to have opt-in for third parties, or both. That is going to be under consideration by the State legislature. As H.R. 10 is currently drafted, do any of you have an opinion whether there will be Federal preemption; and what do we have to do to make sure that there is not, number two?

Ms. CULNAN. I will pass on that because I am not a lawyer.

Mr. LITAN. I will take a cut at it.

As I read the statute, I don't think that there is an implied preemption.

The second question, as a policy matter, should there be preemption or not, you are taking the position that States should be able to add on what they want.

I have the opposite inclination. I think in a world where we get 50 different State privacy laws, especially when we have financial conglomerates doing business all over the country, it would be a better idea not to have 50 different privacy laws, and so I would actually favor an explicit preemption.

Mr. INSLEE. You would prefer that we do it right here then?

Mr. LITAN. Yes.

Ms. CULNAN. Yes.

Mr. CATE. I don't see preemption in the bill, and I think it would be entirely appropriate here, because not only of the situation today with banking conglomerates, as the focus increases with on-line activities, the idea of having State regulation here is practically unworkable.

Ms. CULNAN. But the key point is that Congress has to get it right at the national level.

Mr. CLAYTON. That is the key point, and one of the advantages of having this Federal experiment, I can try it in my State and you can try it in yours, and we can see what happens. The example of Europeans, they are trying one size fits all. We have decided we know the answer, let us do it. I don't think that is workable, because no one knows what this area of the world holds in terms of technology. I would rather you make a mistake in your State, and we learn from that, than have Congress make the mistake and we all have to live with it from now on.

Mr. INSLEE. Are you suggesting that we not act on this issue?

Mr. CLAYTON. Act cautiously. If you try to preempt States from doing this, they are going to be more sensitive to areas that we are not sensitive to on a national level. Using California as an example, for the supermarkets, they have bills trying to regulate how you use data collected by supermarkets and what notices you get. Congress is not addressing that issue. Other States may or may not address that, but they are responsive to local demands on that.

Mr. INSLEE. Let me ask you to comment. Mr. Bentsen asked what is wrong with allowing consumer choice or markets to resolve this issue, and I liken the situation to an attorney-client relationship where we by statute and ethical rule guard the fiduciary obligation. We guard confidential information, and we do not say, if you don't like the lawyer telling the world you have this problem, you can go to the next lawyer and he will take care of it. And the reason we do that, we respect the fiduciary relationship of that type of relationship.

I, for one, believe, and I am sure you realize, it is a fiduciary-type relationship, the banking relationship with their customer; and the reason the industry has been so successful is that it has enjoyed historically the trust of the American people. And I would ask your comments, is there some reason we should treat it with any less respect?

Mr. LITAN. I think you have just made an excellent statement. I fully agree with it.

Ms. CULNAN. It does go to the issue of trust. People have an expectation that their information is provided for one purpose and will not be used for any other purpose, especially when they were not told about it. When new relationships are established later with new organizations, this can begin to undermine trust in the whole financial services industry.

Mr. CLAYTON. I would disagree. There is a historical reason why we have lawyers and attorney-client privilege, and that is to facilitate a complete and uninhibited exchange of information. It can't be disclosed.

That same sort of societal need is not demanded in relationships with the bank in every instance, or with other commercial entities. We have for hundreds of years tried to protect the attorney-client privilege, and it gets complicated when you start getting States and having other issues about who has the right. I think it is fundamentally different.

Mr. INSLEE. We live in a great Nation where great minds can disagree. Thank you very much. Thank you for your time.

Chairwoman ROUKEMA. That concludes our first panel and I don't know what more I can add to that last statement. We can be most appreciative to be in this great Nation where great minds can disagree.

I don't know that we have resolved all of the issues here, but I think you have given us greater insights, and I think Mr. Vento agrees with that perception, that there are certain valuable things that you have laid out here which are very important for us to analyze and translate, if necessary, into further legislation. Maybe we can revisit H.R. 10, although I will not make any reference to the conference committee at this point in time.

Again, under the rules of the committee, if you want to submit further extension of remarks, you are free to do so; and we may have some individual questions to present to you as panelists for the record. Thank you very much.

Will the second panel come forward, please. I thank the second panel for waiting. We have a distinguished panel here that is representing some of the smaller financial institutions, as well as one or two other participants of the industry that have a direct rela-

tionship. Our first witness is Mr. Robert Barsness, who is President and CEO of Prior Lake State Bank in Minnesota.

Did you want to have something to say, Mr. Vento?

Mr. VENTO. Mr. Barsness frequently does represent the Independent Community Bankers.

Chairwoman ROUKEMA. Yes, and that is his capacity here today. Being from the same State, I thought you might have an observation. We all welcome you today, Mr. Barsness.

Our second witness is Robert Davis, he has appeared before us previously and is here on behalf of America's Community Bankers, and he is Director of Government Relations.

The third witness will be introduced by a colleague and friend of his from the great State of Oklahoma, Mr. Lucas.

Mr. LUCAS. Thank you, Madam Chairwoman, I appreciate the opportunity to introduce Mike Kloiber, President of the Tinker Federal Credit Union in Oklahoma City. Mike has twenty-one years of experience in the financial industry, eleven of those with Tinker Federal Credit Union. Tinker has 162,000 members and is based in Oklahoma City. In his capacity as CEO of Tinker Credit Union, Mike is actively involved in those issues which affect the privacy of member records. He is testifying on behalf of the Credit Union National Association and the National Association of Federal Credit Unions, and it is a pleasure to be able to introduce my fellow Oklahoman.

Thank you, Madam Chairwoman.

Chairwoman ROUKEMA. Thank you, Congressman Lucas.

Our fourth witness, Mr. Richard Barton, is Senior Vice President for Congressional Relations at the Direct Marketing Association, and we certainly welcome you here today.

Mr. Barry Connelly is President of the Associated Credit Bureaus, Inc. I believe that you have been President of that organization since 1994 and have an extensive background in fair credit reporting, having worked on that issue over the years, and we welcome all of you today.

Again, I will repeat my alert warning on the subject of the time limits in the hope that we can be respectful of that.

With that, we will begin with Mr. Barsness.

#### **STATEMENT OF ROBERT N. BARSNESS, CHAIRMAN AND PRESIDENT, PRIOR LAKE STATE BANK, PRIOR LAKE, MN**

Mr. BARSNESS. Madam Chairwoman, Ranking Member Vento and Members of the subcommittee, I am pleased to appear before you today on behalf of the Independent Community Bankers of America and its 5,300 community bank members. I commend you for holding this hearing to examine, among other things, the consequences of the privacy provisions of H.R. 10. Indeed, the ICBA would prefer that Congress withhold adoption of new privacy laws until the issue can be fully explored through the hearing process.

Community banks have a long tradition of safeguarding the confidentiality of customer information. If my bank employees were to spread information around town about confidential customer information, there would be a line of people waiting outside the next day to close their accounts. There are a lot of options in the mar-

ketplace and customers will not tolerate a financial institution that does not protect their privacy.

A case in point is the U.S. Bancorp lawsuit in my home State. Even before the ink had dried on the complaint, U.S. Bancorp customers were shopping around for a new bank. A number even came to us looking for a bank that would safeguard the privacy of their accounts. We at Prior Lake State Bank take this responsibility very seriously, and I know that community bankers place the highest value on customer privacy. Simply put, it is in the self-interest of every community bank to avoid the misuse of private customer information. The result of such misuse would be a loss of customer confidence in the institution and eventually the loss of customers. That is why voluntary customer privacy practices have worked well.

Community banks cannot long survive if they gain a reputation for abusing customer confidentiality. Two years ago the banking industry adopted a set of industry guidelines and privacy principles to govern voluntary privacy practices. As a signatory to those principles, ICBA has continually urged members to adopt the privacy policy and inform their customers. We believe these voluntary guidelines provide a workable framework to devise a privacy policy that will protect customer information.

I have attached a sample policy to my written testimony.

In addition to the voluntary practices, we operate under a framework of State and Federal laws and regulations which provide comprehensive privacy protection for our customers. There are at least sixteen different Federal privacy laws on the books. H.R. 10 would make number seventeen. H.R. 10 will lead to the formation of new financial conglomerates. The prototype conglomerate, unfortunately, has already taken shape. Citigroup was pulled together under a combination of legal loopholes and anticipated legislative changes. But once all barriers are removed by H.R. 10, cross-industry mergers will proliferate.

To provide a competitive alternative in this landscape, many community banks will offer non-traditional products and services. Since most community banks do not have affiliates, they partner with third-party providers to meet these needs. That is why we have urged Congress not to pass any laws that place new restrictions on these partnerships.

H.R. 10 requires financial institutions to provide notice of the banks' information-sharing practices and an opportunity for customers to opt-out on disclosing non-public personal information to third parties. But the bill does not apply the same requirements for institutions that share information with affiliates. The special carve-out for banks with affiliates will reduce the ability of smaller banks to offer a full array of products and services. This is inequitable, competitively harmful and imposes a heavy new regulatory burden on community banks.

The fact is that community banks are doing a good job of self-regulating, yet they are being singled out for more regulation under H.R. 10. The problems that have been encountered have been in large banks, yet large banks escape new regulatory requirements under H.R. 10. The logic of this escapes me. My written testimony goes into considerable detail on the use of third-party

outsourcers who provide service to banks, as well as other normal and routine third-party arrangements critical to conducting the day-to-day business. In the interest of time, I will not repeat them here.

It is true that H.R. 10 contains a number of general exceptions to the third-party opt-out requirement, and this exception should cover many of the third-party activities described in my testimony. However, with the varieties of legislative drafting, inevitable legal challenges and subsequent regulation and interpretation, only time will tell if that is the case.

Madam Chairwoman, we urge you to ensure that there is parity, whatever privacy policy is adopted. H.R. 10 fails in this important test. Congress should reject any privacy proposal that imposes new burdens on community banks while carving out an exemption for larger banks. Congress also should examine and evaluate the effectiveness of the privacy principles adopted by the banking industry in 1997. And we would recommend holding medical information to a very careful standard of protection and prohibit pretext calling.

Madam Chairwoman, we appreciate this opportunity to appear before you today.

[The prepared statement of Robert N. Barsness can be found on page 213 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Mr. Davis.

**STATEMENT OF ROBERT R. DAVIS, DIRECTOR OF GOVERNMENT RELATIONS, AMERICA'S COMMUNITY BANKERS, WASHINGTON, DC.**

Mr. DAVIS. Thank you, Chairwoman Roukema, and Members of the subcommittee. My name is Robert R. Davis. I am Director of Government Relations at America's Community Bankers. ACB appreciates this opportunity to testify before the subcommittee today on protecting personal financial information privacy.

All of us are well aware of the growing public concern about information-sharing practices both in the financial services industry and in other sectors of our Nation's economy. The news is full of stories about people receiving telemarketing calls during dinner or bundles of direct mail solicitations in their mailboxes without knowledge of how they got on the list.

While there are legitimate and even essential reasons for businesses to share information, such practices should be subject to reasonable requirements. Those requirements should be developed in large part through self-examination by businesses of their own activities.

In addition, Government should have a role in ensuring that basic standards to protect personal financial information privacy are established and implemented by financial institutions. Financial institutions, particularly our community banks, depend on the trust and confidence of their customers. While most businesses are serious about doing what it takes to maintain good customer relations, it only takes one highly publicized, isolated incident to upset the apple cart.

To complement the ongoing efforts of financial institutions to review their information-sharing practices, ACB urges the 106th

Congress to enact legislation which affirms its commitment to consumers that their basic privacy will be protected. We are pleased that the approach taken in H.R. 10 generally tracks ACB's official policy position on this issue. This policy position was based on the results of a comprehensive survey of practices at select member institutions, as well as the enlightened self-interest of our members.

Our policy position supports legislation that is balanced to ensure consumers that their personal information will be protected while not unduly interfering with the routine legitimate practices of financial institutions. We support legislation that, at a minimum, requires every financial institution to establish its own privacy policy and to share that policy with its customers, that prohibits the sharing of health and medical information without the consent of the customer, and bans abusive pretext calling practices. We are pleased to see that these provisions are included in H.R. 10.

We also appreciate the fact that the House responded to concerns raised by ACB members, and carved out critical exceptions to the bill's opt-out requirement for information-sharing with third parties. In particular, ACB requested that financial privacy legislation not unfairly discriminate against community banks that use third-party relationships for the same legitimate purposes for which some larger banks might use affiliates. Some of those activities engaged in by ACB members include the use of outsourcers providing services to banks, joint marketing arrangements with third parties for products sold under the bank's name, mortgage activities, including sales of mortgages in secondary markets, activities involving common employees, and joint ventures and cobranding activities.

An opt-out requirement on these activities could preclude many community banks from continuing to use these critical arrangements and foreclose the opportunity for other community banks to utilize them in the future. While we do not oppose the bill's opt-out provisions, we do suggest a preferred approach to reach the same goal. Instead of establishing a blanket opt-out requirement for information-sharing with third parties and exceptions to this requirement, as H.R. 10 currently does, we believe Congress should determine which activities and practices or relationships justify a required opportunity for a consumer to opt-out, and apply that requirement only to those activities. This more direct approach would still give customers the right to say no to certain information-sharing activities, and of course, there would be a full disclosure of privacy policies under the law. ACB urges Congress to consider this alternative, a targeted approach of the opt-out requirement, as well as other suggested modifications to the bill which are outlined in our written testimony.

While enactment of H.R. 10 would mark the biggest step ever taken by Congress to protect personal financial information privacy, and while this is a major step, there are still those that believe that the bill's privacy provisions could be more stringent. Given the experience of our member institutions with information-sharing practices, ACB does not believe that such proposals warrant legislative action at this time.

Finally, we should recognize that while financial information privacy has been a hot-button issue with the general public, the financial services industry represents just one segment of our Nation's economy. The information-sharing practices of financial institutions should be examined by Congress, as these hearings do, but other industries must be required to participate in the effort to reassure the public that their personal information will be protected.

Again, Madam Chairwoman, thank you for holding these very important hearings and for giving us an opportunity to testify. We at ACB look forward to working with you, the Congress, Federal regulators, and our customers as well, to ensure that the financial privacy of our customers is maintained.

[The prepared statement of Robert R. Davis can be found on page 231 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Mr. Kloiber.

**STATEMENT OF MICHAEL D. KLOIBER, PRESIDENT AND CEO,  
TINKER FEDERAL CREDIT UNION, ON BEHALF OF THE NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS**

Mr. KLOIBER. Thank you, Madam Chairwoman. As Congressman Lucas said in his generous introduction, I am the CEO of Tinker Federal Credit Union. I am pleased to provide testimony today on the credit union perspective regarding financial privacy.

From a legislative standpoint, this issue has developed with extraordinary speed, given the complexity of the technological and operational aspects and the relative scarcity of specific knowledge about the impact of any changes in the law involving privacy.

I testify today on behalf of two credit union trade associations, the Credit Union National Association, known as CUNA, and the National Association of Federal Credit Unions, known as NAFCU. Tinker Federal Credit Union is pleased to be a member of both associations. My oral testimony will highlight key points of agreement shared by both associations. More detailed written statements have been submitted for inclusion in the hearing record.

As member-owned financial cooperatives, credit unions value the unique relationship we have with our members and respect our members' right to financial privacy. This relationship stems from a long-held credit union core belief that credit unions are not for profit, not for charity, but for service. Serving our membership drives everything a credit union does, including all decisions regarding a member's personal financial privacy.

Credit unions place a high value on protecting our member's financial records, while at the same time delivering cost-effective financial services. Member service involves more than respect of a member's financial privacy; it also involves providing the widest range of financial options at the best possible price, something that cannot be effective unless a member is apprised of all of his or her choices in the marketplace. In fact, financial products that would be right for some members may not even be offered to some, often because their credit union is small and has limited resources necessary to support a full range of products.

Given that 61 percent of all credit unions have assets less than \$10 million, many credit unions work with outside companies to

promote their financial products and services. Many credit unions rely heavily on the services of credit union service organizations, known as CUSOs, because of their limited ability to perform services in-house. CUSOs perform such tasks as credit card and debit card services, check cashing, wire transfer, loan processing and accounting services. Even a credit union the size of Tinker Federal Credit Union, with over \$900 million in assets and 160,000 members, must rely on our wholly owned CUSO or outside companies to provide many of the services members request. Each outside company is required to post a non-disclosure statement, protecting the shared information, and in most cases only public information is provided.

But some services require the sharing of additional information to effect delivery. During last month's House action on H.R. 10, privacy emerged as a pivotal issue. In fact, the inclusion of financial privacy provisions now necessitates that credit unions become involved in debate on H.R. 10.

Since credit unions will be subject to the privacy requirements recently incorporated in the bill, CUNA and NAFCU have three basic questions about how the new requirements will practically affect operations. First, will credit unions and other smaller institutions that will not operate as financial conglomerates be subject to a heavier disclosure burden than those financial institutions with affiliates, as currently defined by H.R. 10?

Second, will institutions that share information with third parties be subject to greater disclosure and opt-out requirements?

Third, is the definition of "affiliate" included in H.R. 10 intended to include credit union service organizations?

Prompted by recent congressional activity, both NAFCU and CUNA are attempting to gain a clear understanding of credit union privacy practices and are in the process of developing formal principles and policies on the issue. Both organizations will be pleased to share their views with this subcommittee as their policy formulation process moves forward.

I would like to commend you, Madam Chairwoman, as well as Mr. Vento for recognizing the potential problems presented for credit unions by the opt-out provision in H.R. 10. Your work to improve the privacy section by creating reasonable exemptions for third-party information-sharing improves the legislation significantly.

Despite the improvement, there are several changes that we believe will be necessary. These changes are outlined in both CUNA and NAFCU's written testimony. I sincerely hope that the conferees will keep these suggestions in mind as the bill continues through the legislative process.

Credit unions want to play a constructive role as Congress and regulatory bodies assess this largely unexplored universe that is financial privacy. Technology has outpaced the law, and we understand that adjustments should be made. We hope that those changes are made with care and caution, so that the very consumers you are trying to protect are not disadvantaged and deterred from participating in the marketplace that lies ahead.

I appreciate this opportunity to appear before this subcommittee and will be happy to answer any questions.



[The prepared statement of Michael D. Kloiber can be found on page 244 in the appendix.]

Chairwoman ROUKEMA. Mr. Barton.

**STATEMENT OF RICHARD A. BARTON, SENIOR VICE PRESIDENT FOR CONGRESSIONAL RELATIONS, THE DIRECT MARKETING ASSOCIATION**

Mr. BARTON. It is a real pleasure to be here. The rest of the witnesses are very used to this subcommittee, but this is a very new experience for me, appearing for the Direct Marketing Association, and it is a real pleasure.

For those of you who don't know, the Direct Marketing Association is a national and international trade association of 4,800 companies, in the United States primarily, but also in 54 other countries, that deal in all types of direct marketing. More than \$1.3 trillion of goods and services were sold through direct marketing in 1998 in the United States, to give you some idea of the magnitude of this type of selling.

Information is essential to the direct marketing process. The information comes from any number of sources, including specific information about individuals, and general demographic information such as from the census. Regardless of where the information comes from, the only and single purpose of information access and use in the marketing process is to provide consumers and businesses with product and service offers that are relevant to its needs.

This being said, the DMA has long had a concern in privacy issues. As long as thirty years ago, we created, because of privacy concerns at that time, our Mail Preference Service, which now has more than 3.3 million names on it. This is a national list of people who want to get off of mailing lists and do not want to receive mailings.

Around fifteen years ago, we began the Telephone Preference Service, which has almost three million names on it, and it is growing all the time; and we are now preparing our E-mail Preference Service for the same purpose, because we believe that it is not sensible to market to people who don't want to receive our material.

Brand-new in the association, begun on July 1, although we began to develop it more than a year ago, is our Fair Information Practices Manual—a new program of mandatory protection of the privacy of our consumers. Our companies now must publish their own information policies notice and give individuals a right to opt-out of its use for marketing purposes. They are required to maintain what we call in-house suppress files so that when anyone requests that their name be taken off their list that they not be contacted again and their names and information about them not be traded. They are also required to use the Direct Marketing Association Mail Preference, Telephone Preference and E-mail Preference Service files, when it is formed.

So you can see, we are strongly committed to the concept of notice and opt-out, and we will remove a company publicly from our association if they do not fulfill these principles.

We also maintain, just for your information, our Guide to Ethical Business Practices, which outlines our concepts of information pri-

vacy as well as other ethical business practices; and our ethics committee hears cases and complaints on a variety of issues, including privacy. When we cannot resolve an issue with a company and we believe that they are violating this policy, we will publish their names, and we will remove them from the association.

So we believe in the notice and opt-out principles that are in H.R. 10. However, we are committed to a self-regulatory regime. We believe that self-regulation can handle the situation and problems.

We do have a problem with H.R. 10 where it provides an absolute ban on financial institutions and the sharing of account numbers, credit card numbers, and other similar information with telemarketers and direct marketers. In marketing cases any such information that is transmitted is transmitted in an encrypted form, cannot be read by the telemarketers or direct marketers putting together the information, and has important uses. It can provide a direct way to identify customers and verify purchases, reducing fraud possibilities. It can allow for the collection of accurate and verifiable data for customer service purposes. It is an important tool in improving the accuracy of mailing and telephone lists, and it can help a customer charge a purchase to an account without revealing the number to the direct marketer, adding an important element of security in the sale of any item.

We believe that properly encrypted data can actually enhance the security of a transaction, protect consumer privacy, and improve the accuracy of the direct marketing process; and that the provision, as it is written now in H.R. 10, would do little to protect privacy and could undermine consumer choice and hurt an important segment of the economy.

We think that provision certainly is fixable, but we think that it needs to be looked at carefully.

We certainly thank you again for the opportunity to testify and certainly will be happy to work with the subcommittee on any privacy legislation. Thank you.

[The prepared statement of Richard A. Barton can be found on page 261 in the appendix.]

Chairwoman ROUKEMA. I thank you very much.

Mr. Connelly, please.

**STATEMENT OF D. BARRY CONNELLY, PRESIDENT,  
ASSOCIATED CREDIT BUREAUS, INC., WASHINGTON, DC**

Mr. CONNELLY. Thank you, Madam Chairwoman and Members of the subcommittee. My name is Barry Connelly, and I am President of Associated Credit Bureaus, headquartered here in Washington, DC. ACB, as we are commonly known, is the international trade association representing over 1,000 consumer credit and mortgage reporting, as well as employment and resident-tenant screening agencies, throughout the United States and around the world. Also 400 of our members are in the collection service business.

We certainly commend you for choosing to hold this oversight hearing on financial privacy. Our country has a strategic global advantage resulting from the legitimate and balanced use of information. As an example, the Tower Group, a Boston-based consulting firm, says that the consumer reporting industry's information prod-

ucts are the infrastructure upon which our country has built a mortgage-backed securitization process that results in a net savings of 2 percent off the cost of a mortgage for the average consumer.

Economic advantages, consumer benefits and consumer rights are all elements of a balanced equation. It is the art of maintaining this delicately balanced equation which remains crucial to your thinking as our Nation's lawmakers.

Consumer reporting agencies are essentially libraries, libraries of information on individual consumer payment patterns associated with various types of credit obligations. The data compiled by these agencies is used by creditors and others permitted under the strict prescription of the Fair Credit Reporting Act to review the consumer's file.

Consumer credit histories are derived from, among other sources, the voluntary provision of information about consumer payments on various types of credit accounts or other debts from thousands of data furnishers, such as credit grantors, student loan guarantors, child support enforcement agencies, as well as collection agencies. A consumer's file may also include certain public record items such as a bankrupt filing, a judgment or a lien.

For purposes of accuracy and proper identification, our members generally maintain information such as a consumer's full name, current and previous addresses, Social Security number, and place of employment. This data is loaded into the system on a regular basis to ensure the completeness and accuracy of data on each consumer.

It is interesting to note the vast majority of data in our members' systems simply confirm what most of you would expect; that consumers pay their bills on time and are responsible, good credit risks. This contrasts with the majority of systems maintained in other countries, such as Japan or Italy, which often store only negative information and do not give consumers recognition for the responsible management of their finances.

In discussions of consumer credit histories, I have also found it helpful to point out some facts about the types of information that our members do not maintain in consumer credit reports. Our members do not know what consumers have purchased, using credit cards, like a refrigerator or clothing, or where they are using their credit cards, such as which stores or restaurants they frequent. They also don't know when consumers have been declined for credit or another benefit based on the use of a credit history. Medical treatment information is not a part of the database, and no bank or brokerage account information is available in a consumer report.

Let me reiterate that our members don't track data on what consumers purchase or where they shop. We compile data on how consumers pay their bills. The FCRA is an effective privacy statute which protects the consumer by narrowly limiting the appropriate uses of a consumer report. Often we call this a credit report. The limitations are under section 604 of the FCRA, entitled "Permissible Purposes of Reports."

Some of the more common uses of a consumer's file are in the issuance of credit, subsequent account review and the collection

process. Reports are also, for example, permitted to be used by child support enforcement agencies when establishing levels of support. A complete list of these permissible purposes can be found in Appendix A of this testimony.

A question that we hear with some frequency relates to how data found in a consumer's credit report may be used, other than for credit reporting. Let me first point out that any data defined as a consumer report under the FCRA may not be used for any purpose other than those outlined in section 604.

However, it is a fact that some of our members do use consumer identification information to develop high-value information-based products, such as fraud prevention and authentication products, risk management systems, locator services, just to name a few. Some of our members use direct marketing lists in order to stay competitive in the marketplace. Note, the data used for direct marketing purposes is not credit history information defined as a consumer report under the FCRA.

In conclusion, let me urge the subcommittee to consider carefully the strategic importance of information in our country and how it benefits consumers. We have moved beyond an industrial economy, and information use is a critical catalyst for our new service economy growth. Balanced laws, such as the Fair Credit Reporting Act, which was significantly amended in the 104th Congress, is an excellent example of the balance needed.

We do believe that there are times when innovative solutions can be found that don't require new laws. The creation of responsible self-regulatory systems can create a flexible bridge between the call for consumer protections and the unintended rigidity of new laws.

Thank you, Madam Chairwoman.

[The prepared statement of D. Barry Connelly can be found on page 278 in the appendix.]

Chairwoman ROUKEMA. Thank you, Mr. Connelly and the whole panel.

We have, as I understand it, just one vote, and so we hopefully can all be back here within a fifteen-minute time period or less and get on with our questioning. You have opened a number of interesting avenues for follow-up questions. Thank you very much.

[Recess.]

Chairwoman ROUKEMA. Thank you. I do appreciate your patience, but we do have some business to take care of here on the floor every once in awhile. Voting, I think, is what the Constitution expects us to do.

But at the same time, we want to get back to this very important subject. There are a number of questions that I have, but given the time, let me give you a general reaction and let any one of you who wants to respond. I would think particularly Mr. Barsness and Mr. Davis would want to respond with more explanation.

I have listened very carefully here, and if you heard my opening statement, I said something to the effect that I certainly would expect the industry to be precise as to what they mean with respect not only to unintended consequences, but what they mean with respect to: "exceptions intended to protect current industry practices."

Now, I have heard some of your references, but I don't think that it is precise enough to explain to me what you mean. Without precision, it sounds to me like a huge loophole that would justify almost any practice. I don't believe that you mean that, but we have to have a little more detailed explanation of what those practices are. Again, I am not limiting it to Mr. Barsness and Mr. Davis, but I would think that it would most focus on the groups that they are representing.

So, again, not only the question of sharing information with affiliates, but also as to what you mean and how you can justify that this broad exception, which is intended to protect current industry practices, is not simply an open loophole that would justify any kind of information-sharing which, in my opinion, would lead to violations of privacy.

Who would like to be first?

Mr. Davis.

Mr. DAVIS. Let me respond first. I understand the nature of your concerns, and let me assure you that we certainly are not looking for a loophole. What instead we believe is the case is that community institutions frequently serve as stewards in their communities to identify important financial services.

There is a level of trust and personal relationships frequently with community-based institutions that communities rely upon. What we do not want to do is chill the process under which most community institutions frequently serve as a gateway for people in their communities by carefully selecting partners to offer products.

A smaller institution is not going to operate a mutual fund or underwrite insurance or underwrite annuities or other sorts of services, but it will frequently scour the financial landscape and find those companies that are the best partners to offer quality products that it wants its members—its customers—

Chairwoman ROUKEMA. For example?

Mr. DAVIS. A small institution is not going to underwrite annuities, but it may offer them. It is not going to develop and operate mutual funds, but it may want those investment opportunities available. A small institution is not going to operate a brokerage service, but it may want to help identify to those customers joint venture products with a larger company that it wants to, in essence, endorse by marketing those products through the offices of the bank. So in those cases, community-based institutions are helping to identify, after a lot of due diligence, the sorts of quality services that should be brought to a community as that institution seeks to broaden its provision.

That is the sort of thing that we don't want to see impeded. In those sorts of circumstances, the institution is more closely identified and more potentially damaged by inappropriate use of information than any other type of financial institution.

For one thing, the community institution is right there in the community, and the Chamber of Commerce meeting and church on Sunday and everything else. Whoever is running that institution is going to see the people affected in the community, and I can assure you that none of these community banks are making calls to their neighbors during dinner to market products, but they are partnering in-agency relationships with some of the best service

providers to broaden their offering of services and products in their community, and that is the type of thing that we don't want to inadvertently chill.

Chairwoman ROUKEMA. Thank you.

Mr. Barsness.

Mr. BARSNESS. Madam Chairwoman, trust is the thing that is critical to our community banks, and we certainly do not want to support any kind of loopholes in this process. We scrutinize the entities that we deal with and develop contractual relationships, such as with an insurance company, to provide an insurance policy. We ensure that they protect that information and they can only use it to the extent that we want that product available to our customer.

As I said before, if the public does not have trust in a community bank, that is all we have is with our relationships with our customers, so we guard that extensively. We have continual meetings with our employees and talk about it on a regular basis. We ensure that our information does not get out to the general public because, if we don't, we are going to lose business, and we cannot afford to do that. That is our value in our community, that relationship that we develop over the years. So that relationship is so critical to us that we deal with that on a constant basis. Privacy, to us, has been a watchword as long as I have been in the business, long before it was even discussed in Congress.

Chairwoman ROUKEMA. Is there anyone else that wants to comment on this?

Well, I would have a follow-up, but I don't have the time. I will submit it to you and see what your reactions are in writing as to how you select those partnerships. What basis, what objective standards do you use to select—and I would like that in writing—and who would judge or what standard would judge whether or not the industry practices are not anticompetitive or conflicting in terms of consumer privacy?

We will present that to you in a defined way and for anyone on the panel, but particularly for Mr. Davis and Mr. Barsness, as a follow-up.

My colleague, Mr. Vento.

Mr. VENTO. Mr. Barsness, you comment on some of the concerns or disadvantages. One is that you did not think that there is a \$1,000 policy that is extended to some consumers or some individual members of banks that have consumers or customers in the organization.

What would stop you from extending that particular benefit? Would that not be a point in terms of asking for the information for that purpose?

Mr. BARSNESS. You are going to have to explain yourself.

Mr. VENTO. You suggested that there is a \$1,000 life insurance policy that you extend in your testimony?

Mr. BARSNESS. Yes. We offer an accidental death policy to all of our deposit customers, free of charge, no cost to them to do that.

Mr. VENTO. What is the problem?

Mr. BARSNESS. Well, they have to select that and opt to take that, but to do that we have to share that information with the insurance company that provides that; and that information, as I read the statute, as it would be in H.R. 10—

Mr. VENTO. Wouldn't they cooperate in terms of doing that specifically if you have to have the information? You are talking about the fact that it is an inconvenience?

Mr. BARSNESS. Cost-wise, I am not sure how we would determine who gets the opportunity to opt-out and how many times you send it. It is a low-cost item, but it develops a relationship, so it is a matter of how much additional cost will there be to ensure that our system will keep track of all of that? Our systems are not as sophisticated as they might be, and I am not sure that we can keep track of all of that on that basis. That would be the concern.

Mr. VENTO. Do you think that some marketing will take place by some smaller financial institutions or security firms that in fact—in terms of safeguarding information and privacy?

Mr. BARSNESS. Marketing the privacy issue, you mean?

Mr. VENTO. Uh-huh.

Mr. BARSNESS. We do that now publicly and through our media with our customers, that we are concerned about their privacy and we want them to understand. That is a marketing tool, that we do protect their privacy.

Mr. VENTO. The point is if you have a relationship with a larger institution, a megabank or financial entity, there is a tendency that they may be more open. You approach the question of whether I am going to have confidence in Robert Barsness' bank, an institution, it might be a different question in terms of sharing or opting out of information, as opposed to whether I am involved with Citibank and Travelers?

Mr. BARSNESS. I think there would be a difference. I think people perceive us as protecting that privacy. We think that we have done that very well and will continue to do it.

Mr. VENTO. That may permit you to make some decisions with regard to third-party marketing that would not be the same level of confidence that one might have with Citibank?

Mr. BARSNESS. That is certainly possible.

Mr. VENTO. You hope that is true?

Chairwoman ROUKEMA. Don't put words in his mouth.

Mr. VENTO. I am leading the witness. I didn't mean to do that. I think there is a qualitative difference, and I think it ought to be recognized for what it is.

Do credit unions, Mr. Kloiber, do they pay CUSO for the services?

Mr. KLOIBER. No. The credit unions actually have an investment and own the CUSO itself. They try to offer complementary services through the CUSO that they cannot directly do, or to complement their direct products and services to meet the member's needs.

Mr. VENTO. Do they serve any other entities besides credit unions with the information that is provided by credit unions?

Mr. KLOIBER. No, they do not share any of the information. The credit union controls the flow of information into the CUSO.

Mr. VENTO. I think there is a perception that they are covered by the exceptions for transactions and operations in the bill.

Mr. KLOIBER. The major concern is that they don't fit the definition directly. And, in fact, in many cases they are in an investment on the part of the credit union, and there could be more than one credit union.

Mr. VENTO. I understand that.

Mr. KLOIBER. We have shared branching where we have—say, in the State of Oklahoma we have seventeen credit unions that own a shared branch network, and that is a CUSO. So there is concern that we want to be sure that the term “affiliate” covers CUSOs, because we do. A shared branch—

Mr. VENTO. No, I don't think that it covers it under that basis. I don't think that is accurate. But under the transactional data, it may be exempted.

Mr. Barton, all direct marketers are not members of the Direct Marketing Association. What is the percentage of membership, do you know?

Mr. BARTON. No, I don't know out of the total universe of direct marketing. We estimate that about 90 percent or more of national direct marketing is done by companies who are members of ours.

Mr. VENTO. We appreciate your efforts, but I think it does give rise to questions about self-regulation, what the baseline requirements have to be, especially since one-in-ten are not members.

We will submit more questions in writing.

Thank you, Madam Chairwoman.

Chairwoman ROUKEMA. Thank you, Mr. Vento.

Again, we are going to try to question in the order of people's arrival, and I think that would mean that Mr. Gonzalez is next.

Mr. GONZALEZ. Thank you very much, Madam Chairwoman.

First, I have an observation and—maybe for later, and I am going to follow up on what was previously stated.

I would appreciate concrete examples of those activities which you believe benefit consumers, that you are presently able to do, that you believe will be jeopardized by any opt-out scheme. These are things that we take back to our communities; we talk about at the town hall meeting. So we can say, “Do you realize, when you talk about privacy that which is being offered by Broadway Bank may not be offered to you?”

You are out there. You know exactly what is in jeopardy.

The other question is very limited. Credit unions, the situation that you pose under the current language, are in conference, I think; maybe they will work over the definition of what is “processing” and, as Mr. Vento said, it is “transactional” in nature as opposed to “marketing.” if they address it adequately, will it take care of some of the fears that you have because you have to outsource? You don't have all of the resources available that maybe a bigger financial institution would have with affiliates and so on.

Do you believe that is that a way of addressing it?

Mr. KLOIBER. I would agree. Since most of the credit unions are small, they do have to rely on outside companies to provide a lot of products and services, and they end up sharing what is mostly public information, which could become even greater, depending on the product. A lot of times members have to request to come back to participate in that product or service, but we have to address that service so that smaller credit unions, they would be impeded from delivering some of these products and services if it was too restricted in the legislation.

Mr. GONZALEZ. Thank you very much.

I yield back the balance of my time.



Chairwoman ROUKEMA. Mr. Barsness would like to respond.

Mr. BARSNESS. Our insurance program provides accidental death insurance for our customers at no cost to them and there is an encrypted account number for identification purposes. The way that I read the statute, we would have to cancel that program, and that will be coming out very shortly; unless I hear otherwise, we will cancel that program and not be able to provide that. In my judgment, to be sure that I don't have to worry about it, I am just going to cancel the program so I don't have to worry about dealing with regulatory issues.

It is a benefit. We recently had a ten-year-old boy that was insured under the policy pay benefits. We had a couple last year; both of them were killed in an auto accident. Those are free policies that they get. But under the current statute as it proceeds under H.R. 10, I would cancel that program.

Mr. GONZALEZ. I appreciate that. I yield back the balance of my time.

Chairwoman ROUKEMA. I am not quite sure about your position there, but we will go over that. I don't know if that is precise as to the implications, but I will have legal counsel maybe come back to you with any questions we might have. You may be absolutely right, I am not sure.

Mr. Inslee.

Mr. INSLEE. Thank you, Madam Chairwoman.

Mr. Barsness and Mr. Davis, I have talked to some smaller community banks since all of this has come to the surface, particularly about what some of the larger banks have been doing with information, and their perception is that some large banks in the Minnesota case have actually sold lists of depositors with, actually, their credit card numbers to telemarketers or direct marketers; and they have expressed to me quite a bit of anger at the larger banks for doing that, because they viewed it as giving a black eye, if you will, to the whole industry. And they perceive that has mostly gone on with the larger banks.

Is that anger justified in that regard? The community bankers who express this sentiment to me—

Mr. BARSNESS. I deal with community banks specifically, and my contacts and my knowledge would suggest that—although I can't tell you categorically that no community bank has done that, I can tell you, as a matter of practice, community banks don't do that. I certainly do not sell my customers' names for telemarketing, and I don't know anyone who does.

I am not going to suggest that all big banks do that. Those that do are known and have to suffer the consequences on that basis.

From my perspective, the community banks do not do that, and I am offended by that also. People came to us during that time-frame in Minnesota and said, "What do you do?" I said, "Not today and not ever." That is our position, and all others will have to justify their own actions.

Mr. DAVIS. The *U.S. Trust v. Minnesota* situation was troubling to a lot of banks. In my oral statement, I noted that one problem like that can upset the apple cart, because it has an effect on public confidence, and it unfortunately affects all banks.

H.R. 10 specifically addresses that situation, and we think that a lot of progress was made in the debate on H.R. 10. We were generally supportive of the provision, even though we would like to do some fine-tuning.

The thing that we want to guard against is that while we are trying to protect against that type of activity and empower the regulators to step in, and so forth, that we don't impede by opposing an extra cost on a third-party relationship which a smaller bank established with significant due diligence, such as the insurance program that was just mentioned. It might be a program which actually generates fee income, but the additional regulatory burden of keeping up makes the institution decide not to operate it.

So where it is something that is carried out under the scrutiny of the regulators, I can guarantee that the bank regulators look very closely at all of our activities in uninsured products, and it is going to get a lot of scrutiny, and there is a lot of due diligence, that we don't add a regulatory burden in that type of relationship.

Distinguishing can be difficult, but our interest has been to look at the mainstream of these relationships where smaller banks actually operate in—they provide stewardship and a gateway in identifying other companies that have good products, and other areas, we think, are problematic.

Mr. INSLEE. I appreciate your answer, but let me sneak in another question.

Mr. Barsness, you said if H.R. 10 prohibits small banks from providing some of these services and marketing, in essence, with third parties, but larger banks who will have affiliated structures are allowed to essentially do the same kind of operations, but simply through affiliates, that that would be a competitive disadvantage essentially for the smaller banks.

I tend to agree with you, and I would like you to expound on that, and I would like you to tell me, do you believe there is any reason why, if this prohibition is put on sharing with third parties, it thereby affects community banks, that we could not also create a similar prohibition that deals with that specific type of conduct which involves sharing with affiliates?

Is there any reason that we could not do for larger banks and their affiliates what has an impact on smaller banks with third parties?

Mr. BARSNESS. Well, I am not here to push for additional regulation for any privacy activity, because I think it is best done on a voluntary basis, because of privacy principles and the like; and because of our relationship with our customers, we adhere to that and that is not a problem for us. But whatever Congress decides, they need to decide and act now.

I would certainly hope that Congress would act so that all entities are treated in an equitable manner; and currently the way that it is written is not equitable to community banks.

Mr. INSLEE. Thank you.

Chairwoman ROUKEMA. Thank you.

Mr. Bentsen.

Mr. BENTSEN. Mr. Barsness, in your capacity on the banking side, what sort—and I realize that you are representing ICBA today, and not ABA. But are there transactional—is there sharing

among affiliates and/or subsidiaries that are transactional in nature and not marketing in nature? Could you give us a couple of examples?

Mr. BARSNESS. It would be difficult for me to answer. We do not have affiliates, probably never will. I am not sure what areas that would lead to.

Obviously, from our perspective, our relationships are invariably with third parties, so the issue of affiliates will never come to the forefront. The problem is, as this legislation evolves and comes to pass, obviously the world is going to change and we are going to have to make more arrangements. We are going to have to do more things for our customers. That is what H.R. 10 allows to have happen with the merging of securities and insurance and the like.

So we are going to have to provide these services for our customers to do competitive—it will not be through affiliates, it will be through third-party arrangements. It is the nature of the beast.

Mr. BENTSEN. Current law provides for smaller banks to enter into joint agreements with other providers, insurance agents or brokerages, where you share space. There is some profit-sharing arrangement. Now staff advises me that they think that is dealt with in the language in H.R. 10. That is not treated as a third party, if there is that sort of arrangement. Is that your understanding as well?

Mr. BARSNESS. I would hope so, but based on this evolution of products and services that are going to come out by these conglomerates, I am not sure. You have made an effort to do that, but our concern is, as the world changes and these financial products and services change, I very likely will be put in a position that I can't do things that others can because of the affiliate relationship.

I like to think that all of that has been covered, but somehow regulation and litigation and all of those things come into play and I am really not sure that it will and I am concerned about that for our membership. There needs to be a law for those products and services. We need to be competitive and provide those things for our customers.

Mr. BENTSEN. The gentleman from the credit union brought this up: You have third-party service agreements for non-transactional issues for marketing purposes. Is it then ICBA's position and CUNA's position, and others', that there should be a further exemption for third-party service activities for marketing or that opt-out should be extended to affiliates for those that are big enough to have affiliates?

Mr. DAVIS. Let me try responding to that.

I agree with your staff observation that there is pretty broad exemption provided now where there are common or joint employees. Also, under H.R. 10 as it is written, in a variety of third-party relationships, that would also include marketing of products. If I am a bank and I have a relationship with an insurance company to market their annuities, or it can go the other way, that sort of arrangement of co-branding or joint marketing or operating through dual employees is covered in the list of exemptions. So we think a good job was done in trying to carve out.

One of the points that we made in our testimony was that perhaps it would be better—rather than saying there is opt-out for all

third-party relationships, but then adding most activities in which most banks currently engage covered by an exemption, it may be better to go directly to the types of *U.S. Trust v. Minnesota* sorts of cases and say, no, these are the ones that explicitly require opt-out.

Mr. BENTSEN. With the Chair's indulgence, may I ask a question?

Chairwoman ROUKEMA. It depends on how long the response will be.

Mr. BENTSEN. In your opinion, even with the opt-out and the way that the language is written and the sharing of information with affiliates or a third party in the joint arrangement, does the bank or the thrift still retain liability for the misuse of personal information for fraudulent use of personal information?

Mr. DAVIS. Well, with respect to the activities of the third party, it is my understanding—and I will be happy to clarify this for the record, but it is my understanding that obviously the third parties will be contractually bound to abide by the bank's privacy policy, but the bank would not be directly liable for breaches of contract by the third party.

Mr. BENTSEN. Thank you.

Chairwoman ROUKEMA. I think we may need further clarification. Feel free to submit for the record, any one of the panelists, a response to that. It is an important question and we want to be precise. If there is lack of clarity we have got to look at it with respect to H.R. 10. Thank you very much.

I thank the panel, and as you can see, we do have some open questions and again, for clarification, we will look forward to your written responses. Thank you.

The third panel, please.

Each of our three panelists is now seated, and to balance out and complete the picture, the pros and cons of this issue, we have this consumer panel, and in order of their appearance, I acknowledge and welcome Mr. Edmund Mierzwinski, who is Consumer Program Director for U.S. Public Interest Research Group. Mr. Mierzwinski has been a member of the Federal Reserve Board of Consumer Advocacy group, and has considerable experience there.

You raised your eyebrows. Is that not correct?

Mr. MIERZWINSKI. I am sorry, I thought you were going to say I had been a member of the Federal Reserve.

Chairwoman ROUKEMA. Oh, no. I know the difference there.

Mr. MIERZWINSKI. I know you do.

Chairwoman ROUKEMA. But what would the Federal Reserve Board do without your guidance?

Our second witness is Mr. Marc Rotenberg. Mr. Rotenberg is Director, Electronic Privacy Information Center and is Adjunct Professor of Law at Georgetown University Law Center.

And the third and final witness is Mr. Jack Brice. Mr. Brice is representing the American Association of Retired Persons—as we all know them, AARP. He has been a member of the Board of Directors since 1998, and has many years of military experience to recommend him to us today, and now he has his own consulting business.

Mr. Brice, we also welcome you.

Without further ado, we are trying to limit ourselves to five minutes. Please be respectful of the time limits.

Mr. Mierzwinski.

**STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PUBLIC INTEREST RESEARCH GROUP**

Mr. MIERZWINSKI. Thank you, Madam Chairwoman, Mr. Vento and Members of the subcommittee. My testimony today is on behalf of the U.S. Public Interest Research Group, Consumers Union and Consumer Federation of America. Our views are quite simple on this matter.

First, we believe that the Congress should act in response to the growing concern from the public that their privacy is not being protected and will not be protected by ever-larger corporate entities. As Mr. Brice will point out, several AARP surveys of both their own members and of the general public have shown very strong support for consumer privacy. Customer outcry over the driver's license photo sales by several States, consumer outcry over the know-your-customer regulations are just some of the other examples that lead us to believe that the public is well ahead of the industry in calling for changes to the laws to protect our customer information.

What consumer groups believe should be done is that the financial sector should be subject to privacy laws that provide us with an opt-in for the sharing of our personal information with any inside affiliate or outside company and additional consumer protections to guarantee that that opt-in is protected. We believe that H.R. 10, as passed in the House, fails to provide that protection. It provides a limited opt-out for some third party purposes, allows a number of third-party uses without the opt-out and allows affiliate-sharing to continue without any privacy protection at all. Our message on what is provided for affiliate-sharing is very simple. Disclosure is not privacy protection.

Instead, however, of enacting what is in H.R. 10 and in lieu of enacting the opt-in provision, which is our preferred provision, we would have at least hoped that the Congress would have enacted the compromise Markey-Barton opt-out provision.

I want to point out, by the way, that that provision was partially based on the Inslee provision from this subcommittee that you yourself supported, Madam Chairwoman. The opt-out across the board for affiliate-sharing and for third-party uses would have made a great deal of sense and would have solved a lot of problems that H.R. 10's provision will not solve.

It is particularly important to recognize that privacy problems are caused not only by third parties, but also by inside affiliate-sharing, and we think that the NationsBank case of 1998, where they settled a \$7 million SEC complaint for sharing CD holder information, confidential customer information, very similar to the information shared by U.S. Bancorp with Memberworks, where they shared that information with a securities subsidiary that then put the people into risky hedge funds, is indicative of the problem and suggests that affiliates are doing the same thing third parties are doing. We should have the same protections across the board.

I want to point out, and this is not in response to anything any member has suggested to me, but in response to what I hear industry saying in the newspapers, the consumer group position is not against information-sharing; it is for giving customers control over their information. We do not believe that our provision, the preferred Markey-Barton provision, would stop H.R. 10, would condemn banks to living without the benefits of financial modernization. We find that to be absurd.

I want to make two other brief points. First, the idea that we have operated successfully on a sector-by-sector approach, and we believe that is obsolete as sectors are converging. We believe that voluntary self-regulation just will not work. We believe that financial information should at least be subject to the same level of protection as video store rental records, and it is not in this situation.

The last point I want to make is that when Comptroller Hawke spoke on the U.S. Bank situation he actually spoke on two issues, and the other issue in his speech I want to urge the subcommittee to take a close look at, he strongly pointed out that consumers are no longer getting the benefits of the Fair Credit Reporting Act, which governs the use of information for credit decisions, and affiliate-sharing is only going to make things worse.

What Comptroller Hawke talked about was the increasing number of financial institutions that are no longer sharing their customer records with credit bureaus. So if I apply for a loan, my credit report will not be complete, because my bank may have chosen to keep my information for proprietary reasons. If banks, under H.R. 10, get bigger and bigger and no longer need to use credit bureaus, then consumers will not have the protection of the Fair Credit Reporting Act, and they will only have the limited protections provided under affiliate-sharing; and not only will privacy protections be denied, but I think it will have a very significant effect on both competition and the marketplace.

Thank you very much.

[The prepared statement of Edmund Mierzwinski can be found on page 283 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Mr. Rotenberg.

#### **STATEMENT OF MARC ROTENBERG, DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, DC**

Mr. ROTENBERG. Thank you very much, Madam Chairwoman, and Members of the subcommittee. I appreciate the opportunity to be with you today. I have submitted for the record a lengthy statement that tries to answer all ten questions. I was asked to go into some detail about specific changes that could be made to Title V and H.R. 10, as well as Section 351, which is the medical record provision, as well as describing some of the larger concerns relating to the international privacy protection and the EU data directive.

I would like to make a few general comments on this particular issue and start with the point that was made just a few minutes ago by Congressman Inslee on the nature of the disclosure of personal information in the financial sector context. At the Electronic Privacy Information Center we have become aware that there are

two types of information that raise the greatest level of public concern. The first is medical and the second is financial.

It is clear that in both of these settings, when individuals give up information for a particular purpose, they consider the information to be related to that purpose. If, for example, I fill out a loan application and indicate my period of employment, what I have been paid, account holdings and so forth, I don't expect that information to be used in another context for another purpose. My willingness to provide information to receive a particular financial product or service is based in large part on the trust that I have in that relationship with the financial institution; and our privacy laws, by and large, reflect an intent to allow individuals to exercise control over their personal information so that the data will be used for the purpose that it is provided for.

Now, the problem with affiliate-sharing is that viewed from the consumer's perspective, the corporate relationship between the entity that now is in possession of the personal information really does not bear on the question of whether that should allow for uses in unrelated settings. The central question for privacy protection is still, does the individual have the ability to control the use of the information in that particular context?

And so it is for this reason that I very much agree with the experts on the first panel, and also Mr. Mierzwinski and the consumer groups, that to realize privacy protection in the financial services sector, you have to give individuals the ability to control the use for unrelated purposes; and that means, specifically, in the context of affiliate-sharing, there has to be a strong notice and opt-out provision. Even with a notice and opt-out provision, I don't think that provides adequate privacy protection, because one of the other critical areas where the present privacy provisions come up short, as measured against other privacy bills, is they do not give individuals the ability to get access to their own personal information that is held by the financial institution.

Now, you understand well the significant role that this plays in mortgage determinations with the Fair Credit Reporting Act, where a person's ability to see the information contained in the credit report that will bear on the likelihood of the loan and the closure and purchase of a house is absolutely critical to a person's ability to operate effectively in the marketplace.

Similar rights should be extended to other financial services, particularly as the amount of detailed information about individual consumers increases.

And this, then, is my final point. As we enter the 21st Century, I think it is important to keep in mind that the amount of data collected on consumers in this country is going to accelerate rapidly. In the old days, if you walked into a bank and picked up a brochure because you were interested in opening an IRA or something similar, until you contacted the bank about the IRA application that brochure sat in your pocket and was basically a private fact.

In the online world, where more and more companies will be offering financial services to customers, when you click on the ad for that IRA, when you download more information about that financial product, a record is going to be created that you, as a known individual, have an interest in a certain type of financial product.

That information is going to be added to a database long before you fill out any application or before you actually enter into an agreement with a financial institution.

And so it is for this reason, in particular, that on the issue of privacy protection in the area of financial modernization, I think it is very important to err on the side of stronger safeguards and stronger protections for customers, because the growing demands for personal information and the ways in which individuals may lose control over personal information, I think will be increasingly threatened.

Thank you very much.

[The prepared statement of Marc Rotenberg can be found on page 294 in the appendix.]

Chairwoman ROUKEMA. Thank you.

And Mr. Brice.

### **STATEMENT OF JACK BRICE, MEMBER, AARP BOARD OF DIRECTORS, DECATUR, GA**

Mr. BRICE. Thank you, Madam Chairwoman and Members of the Subcommittee on Financial Institutions and Consumer Credit. My name is Jack Brice. I live in Decatur, Georgia, and I serve as a member of AARP's Board of Directors. The Association appreciates this opportunity to present our views regarding the important issue of protecting the personal financial information and medical records of individual Americans.

AARP recognizes the potential that a modernized financial services industry may offer in the way of new and useful products and services, as well as the potential for cost savings to the consumer. However, the Association is concerned about the risks involved in allowing the integration of the financial services industry without also updating consumer information privacy protections.

The issue of financial privacy has emerged from a recognition that our Nation lacks a consistent binding process for protecting the privacy rights of consumers with regard to personal financial information collected and disseminated by private financial enterprises. It is clear from the AARP survey that midlife and older Americans feel truly vulnerable to the complex and fundamental changes which have already occurred in this period of financial transformation. Survey respondents were concerned that they will be put at further risk by the financial mergers that are yet to occur if adequate personal privacy safeguards are not put into place.

Extensive personal information is already routinely gathered and distributed by a wide range of financial institutions. As banks merge with securities and insurance firms, financial privacy protection for confidential information grows increasingly important. It is clear that the financial privacy of consumers should not be considered incidental to the modernization of the financial services industry, but rather an inherent part of it.

The financial services industry and consumer interest advocates have another opportunity to work together. One opportunity concerns "pretext calling." While the House and Senate have passed different versions of financial modernization legislation, both include provisions that would make it a Federal crime to use false



pretenses, so-called "pretext calling" to gather private information about an individual from a bank.

However, many of the personal information privacy protections included in the version of H.R. 10, the Financial Services Act of 1999, reported out of the House Commerce Committee, were dropped from the version finally passed by the full House. AARP was encouraged by Commerce Committee bill provisions requiring:

First, financial firms have and disclose their privacy policy;

Second, consumers be given the opportunity to say no or to opt-out of personal information being transferred among financial firms, business affiliates as well as unrelated third parties, such as telemarketers; and

Third, consumers have access to their information held by third-party companies, as well as the ability to correct that information.

AARP believes that financial services modernization legislation should go even further to protect consumers. Specifically, AARP believes that consumers should not be compelled to pay to block such information dissemination, nor should they be forced to comply with cumbersome procedures to ensure that protection.

Consumers' explicit and recorded consent should be obtained before any sale or sharing of their non-publicly-available financial records to third parties or to businesses affiliates. At a minimum, this notification and opportunity to prevent distribution of their information should be reviewed when new data is being collected or added, as well as instances of business mergers or acquisitions, and consumers should be provided avenues for redress if they are harmed by inappropriate disclosure or use of their personal information.

Unfortunately, the version of H.R. 10 that passed the House allows financial services providers to continue the practice of sharing individual financial information with its affiliates, as well as unrelated third parties that market products in alliance or partnership with the data collecting institution. Without the customer's consent, the House-passed H.R. 10 only requires the customer consent before allowing the financial services providers to share private account information with telemarketers and other unrelated third parties.

The medical records provision of H.R. 10 is also of deep concern to AARP. The Association believes that a medical history contains some of the most important information collected about any individual. It is critical that individuals be able to actively participate in decisions about how these data will be used and to approve who will have access to their personally identifiable medical information.

Section 351 of H.R. 10 would legislate to financial institutions more authority to share confidential health care information than currently exists within the health care business. AARP, therefore, strongly recommends that issues related to the privacy of medical information not be addressed in the Financial Services Act. It is felt that Congress, instead, should continue the extensive legislative work that has already been done on this complex issue and enact separate comprehensive Federal legislation applicable to the entire health care system.

Thank you, Madam Chairwoman.

[The prepared statement of Jack Brice can be found on page 315 in the appendix.]

Chairwoman ROUKEMA. And thank you. I am going to reserve my questions until the end, and I will defer now to Mr. Vento.

Mr. VENTO. Thank you, Madam Chairwoman.

Today the Health Policy Project released a detailed report on how States are legislating medical records confidentiality, entitled "The State of Health Privacy and Uneven Terrain." Based on their review of State laws conducted over the past eighteen months, the office concluded that on the whole, State laws are weak and incomplete in the broad areas Federal legislation seeks to regulate, such as patient access to medical records, limits on disclosure of health information, law enforcement access to records, remedies for violations of privacy laws; and pointing out that in some specific illnesses, such as HIV, AIDS or genetic diseases, States have enacted detailed legislation.

The intent of this legislation, of course, at the last moment, was to try to prevent health insurance companies from sharing that information with banks and securities institutions and other firms, to put some limits based on the banking modernization.

Of course, most of the answers that come back are that somehow we are affecting or preempting States, which I think is unclear; second, that the Department of Health and Human Services would in fact put in place a strong definitive policy with regard to this. But I would remind the witnesses and others that they have to go through the Administrative Procedures Act, and it is a long way down the road. So I would think that we don't want to preempt States or to preempt the Department of Health and Human Services from dealing with that, that we need to have some modicum of limit in terms of a safety valve in this legislation, which is what this was intended to do.

One of issues that we brought up, the opt-out provisions, even given their effectiveness, you heard the Direct Marketing Association suggest that they have 3 or 2 percent of the persons that opt-out that seek to have their names removed from the Direct Marketing Association, which I think is a little more provocative in terms of having your names removed, especially since they have people pushing and soliciting to have their names removed, as opposed to the opt-out provisions that we get for fair credit reporting or what I would anticipate would occur under either an opt-out for affiliates or an opt-out for third parties in this legislative provision.

It is very limited in terms of the demonstrated participation by individuals in that particular means. In terms of trying to deal with their privacy and for other reasons, I don't think when they are opting-out they are dealing with it for privacy. There can be a lot of reasons: Maybe I don't want to be bugged by XYZ.

Do you have any response? For us to fall on our sword over opt-out seems to me to be, when it has such a limited application or utility in this case, although we claim it gives choice—anyone?

Mr. Mierzwinski?

Mr. MIERZWINSKI. Representative Vento, my understanding is that in California some 40 percent of consumers opt-out of having their names disclosed in the telephone book. So some opt-outs do work.

In terms of—I agree with you that a bad opt-out is a real problem. That is why our preferred position is an opt-in. If we are going to have an opt-out, it should be statutory and clear disclosure. The fair credit reporting prescreening opt-out is not subject to any kind of disclosure statute.

Mr. VENTO. I only have so much political ability to do things around here. When we are making decisions around here, we can't say, my preferred position is over here on this pole.

Mr. MIERZWINSKI. But on the opt-out, the ones that we have are terrible. The fair credit reporting affiliate-sharing opt-out has been condemned. Former Acting Comptroller Williams gave several speeches and her staff pushed for a disclosure rule on that.

Mr. VENTO. I am going to run out of time. I think if I am going to spend my political capital on something—I am trying to get something done inside. The concern is that from my efforts in terms of working on the affirmative responsibility, and disclosure is not enough, I agree, and dealing with limiting the account numbers and—you know, which obviously was helpful because it says you have to have an affirmative responsibility. And I know that you would like to have a legal action based on that. But banking and financial institutional law works on the basis of standards and it works on a different basis.

Mr. Rotenberg.

Mr. ROTENBERG. I just wanted to say, Congressman, on this particular point there is plenty of data and plenty of polling information that shows that the American public, if asked, would much prefer an opt-in regime to an opt-out regime, and these questions have been asked by Time, CNN, by Lou Harris and other organizations. And in some sense, the opt-in regime is the common-sense regime. It is the one that says "we have received your information for this purpose, thank you. We would now like to use information for other purposes. Is that OK with you?" It is not a prohibition. It does not say that it cannot be used. It simply puts the burden where it properly belongs, and that is on the institution that knows what the subsequent use is going to be.

You see, the problem with opt-out is that people can't exercise this choice effectively. They don't know what they are opting out of.

Mr. VENTO. I think that is very important. I think most of us can agree on transactional and other credit information not permitting people to opt-out or opt-in if we can develop a commonality with the list of exceptions that might exist here, to permit business to go on.

And then we get to questions that you have raised. The counterposition is, if you make this so difficult to get information that some banks and institutions become their own credit bureau, and you don't share any of this information anymore. So that is the other side, and it would put us in a position that they don't want to share it because they want it as proprietary information. That is sort of an ironic problem. Or the example I cited from thirty years ago, when I was a State legislator working on insurance actuarial data that they would not share because they didn't want competition in terms of bidding on the public contracts for health insurance.

I can cite you some examples, and I think—so you know, I just think that the issue in terms of trying to address this, the universality of it and the way I feel is that we are going a lot further with financial institutions than we have gone with other commercial entities. We are looking for something that will work. And I agree with the universality of how this will shape up. I hope that we have a common touchstone in terms of what we are doing and what we are doing on the Internet.

I don't think that we should go the way that the FTC has advised in terms of self-regulation, as they have done with Internet. That has failed with banks and with other financial institutions.

Thank you, Madam Chairwoman.

Chairwoman ROUKEMA. Thank you.

Mr. Inslee.

Mr. INSLEE. Thank you. I appreciate all of your work on this, obviously, and you have all articulated the arguments for this better than any of us. I want to ask you a process question if I can. You heard my opening statement where I asked folks, how do we draft something that will prevent affiliate-sharing that would allow them to do marketing with affiliates, and how can we do that in a way that would not destroy a bank's ability to provide financial services; and I did not get much of an answer from the first couple of panels.

Has the industry talked to any of you to try to work out language of that sort? Or have they simply taken the position that we are not going to allow any regulation of affiliate-sharing, we are not going to talk about it or try to find language that would meet our mutual requirements?

Mr. MIERZWINSKI. Congressman, I did go to one meeting that industry was present at, but they were not talking to me, and they have not approached us individually to work on this; and I don't think that they have approached the other groups that I am representing today.

Mr. ROTENBERG. I have heard nothing about this.

Mr. BRICE. Nor have I. The Association is just as concerned, and rightly so, that consumers have the right to reject unauthorized use of personal financial information and medical information.

Mr. INSLEE. I have heard a lot of people say we have to be cautious about this, if the industry did not want to talk about language, how to prevent affiliate-sharing for marketing purposes, but some language which would allow them proper use of it. Would you be willing to do that?

Mr. ROTENBERG. The answer is yes. In fact, in my written statement I went into some detail in terms of various changes that could be made. Most of the changes are actually surgical, changes that I think could survive some of the industry concerns.

Mr. MIERZWINSKI. I think that the Markey-Barton-Inslee amendment is highly appropriate and would have been an ideal solution that answers industry's and our questions.

Mr. INSLEE. When you say that, I think you appreciate we tried to take some of the industry concerns when we drafted that. Were any of those inappropriate from your perspective?

Mr. MIERZWINSKI. My understanding, Congressman, is that you tried to preserve the right of companies to conduct affiliate-sharing or third-party sharing when it dealt with completing the customer's

transaction for his existing accounts; but you tried to give the customer control over sharing that dealt with secondary uses. That is our position.

Mr. ROTENBERG. I think it is important to keep in mind the comments that were made by both Bob Litan and Mary Culnan on the first panel. They said that by establishing common-sense procedures, notice and opt-out, some clear privacy policies, you build trust that enables people to disclose information so it can be used to receive the services they want to receive.

And on the second panel they said that they do not want to market to people that are not interested in the products and services. The way that you sort of put this all together is that where you have a good privacy policy, one that respects the rights of consumers, but protects the interests of business, then people can go forward. But in the absence of good privacy policy, then you have a lot of unease and mistrust, and these problems, I think, just get bigger.

Mr. BRICE. I think that is the crux of this matter. We feel that Congress must put into place performance standards that take advantage of the efficiencies and the conveniences that information technology brings forth to us, while at the same time providing security, confidentiality and privacy for the consumer.

Mr. INSLEE. I appreciate that. I would like you to know that I would personally prefer an opt-in provision. I was on a radio talk show today and a fellow said, "You are doing a great job fighting for consumer privacy, but how come you have to opt-out instead of opt-in?" Unfortunately, there are folks who are listening to other voices rather than our constituents, frankly. I would love if you have majority support for that and I appreciate your efforts. Thank you.

Chairwoman ROUKEMA. Mr. Bentsen.

Mr. BENTSEN. Thank you, Madam Chairwoman.

I have a number of questions, so if we can get through them in the time. When you used the term "affiliate," do you also believe that to mean subsidiary, wholly owned subsidiary?

Mr. MIERZWINSKI. Yes, we do.

Mr. ROTENBERG. Yes.

Mr. BENTSEN. So to the extent that there was an operating subsidiary structure, that NationsBank owned Nations Security, which is actually Section 20, but if it was a wholly owned subsidiary, you would oppose information-sharing of customers of NationsBank or vice versa without an opt-out?

Mr. MIERZWINSKI. Again, I think our intent is to define "affiliate" broadly for the purposes of privacy to include subsidiary.

Mr. BENTSEN. Mr. Rotenberg.

Mr. ROTENBERG. I take a somewhat different perspective on the issue.

From the privacy perspective, the corporate structure of the entity that the consumer is dealing with turns out to be less significant than the use of the information. Now, I appreciate, from the regulatory viewpoint, that is a little bit complicated. But from the privacy viewpoint, that is really what it is about. If a person is providing information for a certain reason and it is being used for

other reasons or it is being disclosed to other entities, that is where the person will be able to exercise some control.

Mr. BRICE. That would be our concern, too. We are trying to say that we are concerned that the financial information and medical records outside of the original business context is a threat.

Mr. BENTSEN. Let me ask this follow-up. Would you oppose—and of course there is no current law right now; there is H.R. 10 and the Fair Credit Reporting Act, although H.R. 10 is not law yet, there are some State laws out there. Would you oppose the ability of a bank to share information between the deposit side and the trust side that is allowed within the current bank structure?

Do you understand my question?

Right now, you know how a bank is set up. You have the deposit-taking side and the consumer side, and presumably they can share information. If I have an account with Texas Commerce Bank and they want to start marketing their trust benefits to me, they can do so. Would you oppose that as well? That would be sharing among departments within the bank itself.

This is getting to a critical question.

Mr. ROTENBERG. I understand the question, and I have not thought about it enough to say yes or no. What I would say is that whatever the answer would be, the more information that the bank provides to the customer about how the information that is collected will be used, the more likely you are to produce an outcome that the customer will be satisfied with.

In other words, I think the customer needs to be made aware that there are potential uses within the one institution of the personal information that is being provided for a particular service, and at least on that basis people can make some assessment.

Mr. BENTSEN. Let me step back for a second. It is not really that complicated when you talk about structure, because in my mind that is where the problem is.

Some of us believe in Congress that the marketplace demands a new bank charter model or bank structure with additional powers. Now we have disagreements as to what powers to allow in the bank or out of the bank for safety and soundness reasons, and so we either use a holding company model that allows for affiliates to do securities and certain types of insurance and other types of activities, or there is a matter of dispute over using a subsidiary model for certain types of activity. But we have done that.

Now, some may oppose that, but to the extent we get to that level, then we have a question as to what synergies do you allow within the new bank structure that are already accepted practice within the bank itself; but now for safety and soundness reasons, we have created this new model, but we are going to give you a different set of rules. And that is where I find that there is a real problem. Yes, there is the marketing nuisance of getting phone calls or excess mail, saying will you buy this or buy that, but that is not the issue. I mean, that is one issue; and how do we deal with that?

The other issue, Mr. Mierzwinski brought this up with respect to NationsBank and Nations Security, is the bigger issue which is not so much sharing. Yes, there need to be privacy issues with respect to medical and things like that, but it is not the access as much

as the misuse of the information; and I don't see in H.R. 10 where we shield from liability, and I would be opposed to doing that.

And second of all, the fact is, in the end NationsBank had to pay \$7 million in a civil penalty. We should always be concerned about fraudulent activity, and I don't see anywhere in H.R. 10—and if there is, I would like to know—where we are saying, certain types of otherwise fraudulent activity are OK. We should be always on guard for that, and that is really a different issue.

The fact that somebody is going to market something and you may make a bad investment, even given the disclosure you have, is another issue; and that is where the privacy thing comes for me. You are getting marketed this data by a new bank structure with certain protections, which are absolute, that we set in the bill, but you should not confuse that with fraudulent or misuse of the data or fraudulent behavior toward investors or consumers.

Mr. MIERZWINSKI. Very briefly, I am aware and you make the point correctly that that civil penalty was not for a privacy violation. But our view is that in addition to their protections against fraud and unsuitable investment marketing, customers should have the right to say no to even receiving the marketing from either a subsidiary or an affiliate.

Mr. BENTSEN. But opt-out would not have done anything with Nations Securities if people had bought the securities with bad information.

Mr. MIERZWINSKI. Some would not have received the offers so some would have been able to say no. Again, we would prefer that they say yes.

Chairwoman ROUKEMA. I was very generous with Mr. Bentsen, but he really hit on part of the question that I have remaining in my mind.

Mr. Gonzalez, are you here to ask questions?

Mr. GONZALEZ. It is always dangerous to ask questions when I have not heard the testimony. My question is more in the nature of philosophy, Madam Chairwoman.

I have a note as to what you basically agreed to, and I guess what it comes down to—and you heard the first panel kind of summarize things—and that is, it is a fundamental right or question of fairness. It is fairness to the consumer, not necessarily to the business entity, who makes that choice on whether the information should be used for any purpose; and the rights should remain with the individual, the consumer, the customer, to determine whether that information is to be provided to anyone else for whatever purpose.

In general, is that in principle what you are telling me today?

Mr. ROTENBERG. Yes.

Mr. MIERZWINSKI. Yes.

Mr. BRICE. Yes.

Mr. GONZALEZ. Thank you very much.

Chairwoman ROUKEMA. Mr. Moore.

Mr. MOORE. Madam Chairwoman, I missed the majority of this testimony this afternoon, so I don't think it would be appropriate for me to ask questions, but thank you very much.

Chairwoman ROUKEMA. Thank you. I don't know quite how to conclude this.

As I have listened this afternoon—first, I will say categorically and without exception that Mr. Vento spoke exactly to my conflicts over the questions of opt-in and opt-out. In addition, I agree with what you said, and I have forgotten the follow-up way you characterized it, with respect to the medical privacy. There is a modicum of progress—I think it is a modicum, but it is a foundation on which we can build. And so in those two areas, I want to totally agree with what Mr. Vento said.

I would also go beyond it in terms of the opt-in/opt-out provision. I hear what you are saying, but rather than putting it as Mr. Vento did, about falling on my sword, I would rather say that if we make it a statutory requirement with rather precise disclosure provisions, it seems to me then we are hair-splitting over whether it is opt-in or opt-out. The opt-out provision should serve everybody's purposes if those disclosure requirements under the statute are precise.

I would think that would be the way it is, and I think Mr. Vento made a reference to, can't we get you together with the industry. And if, as the industry says, that is their intention as well, then I would think that we would be able to accommodate this.

Do you take strong exception to that or not? No?

Mr. MIERZWINSKI. Well, getting together with the industry, our major concern—

Chairwoman ROUKEMA. No, if you agree that clear disclosure could resolve the problems as to opt-in or opt-out?

Mr. MIERZWINSKI. It would go some way toward doing so. However, this bill does not provide an opt-in or opt-out for the majority of purposes, and that is our bigger problem.

Chairwoman ROUKEMA. But you are not suggesting that we not address the subject at all and build on it in terms of separate legislation, either in that case and/or the question of the medical privacy as well?

Mr. MIERZWINSKI. Our view is, of course, we are always happy to work with you, but since H.R. 10 is the major bill dealing with increasing the size and ability to cross-share by institutions, we feel that it is the bill to try to build the biggest foundation in.

Chairwoman ROUKEMA. Mr. Rotenberg.

Mr. ROTENBERG. I certainly think that it is an area that should be explored, and it may be possible through good notice, as you say, to kind of narrow the gap.

I can tell you the debate on opt-in or opt-out, basically it comes down to the question of who carries the burden. It really is that simple. In an opt-in regime, it is the company that wants to make subsequent use of the data that is going to have to get permission. And they will say that that is costly; they prefer not to do it if they don't have to.

In an opt-in regime, it is the customer that is going to have to find out how is that information going to be used?; do I need to renew on an annual basis?; and that is why, frankly, you don't see a lot of people exercising opt-out, because the burden falls on the consumer.

Now, if there is a way to narrow that gap so it is more fairly allocated, I think that may be the right way to go.



Chairwoman ROUKEMA. Mr. Brice, do you want to comment on this?

Mr. BRICE. Not really.

Chairwoman ROUKEMA. Not really. You don't want to split any more hairs? OK.

Well, I would simply conclude we don't have easy answers here. I guess there are no simple answers. Simple answers are for the simple-minded. I think we have more insight as to the complexities of the privacy issue that we have been dealing with today. Maybe by tomorrow there will be even more complexities, but I do not believe that they are irreconcilable. I believe we have the ability here in H.R. 10, through the conference as well as—and I stressed it in my opening statement, I believe that the foundation is in H.R. 10, but it is not exclusive. The purpose of these hearings is to set the stage for further action on more comprehensive privacy legislation.

Mr. Vento.

Mr. VENTO. I think that the comments that he made that he wants to build the strongest foundation that he can, I understand that because nothing else is moving on this particular issue in spite of the fact that he referred to the privacy provisions in the other bills.

I think that the first panel also made a difference between—in terms of opting-out on service and related services. In other words, if they are related services, that that would be helpful. But it seems to me that some of the examples that you gave in terms of credit life insurance and credit card insurance are exactly the ones that you are most concerned about.

In the best opt-out circumstance, where you have people soliciting business to opt you out of direct marketing, they are saying you get 2 or 3 percent. Maybe 5 percent, but that is an aggressive program. They say, would you like your name removed from this list of folks that are calling you on the telephone or sending you mail? So that has got to be—I don't know how much better you are going to get it. I understand halftone on the back of a bank statement is not the best modus operandi for opting-out. I understand.

I think the idea—I don't mind laying down most of your effort for something that was workable, but it obviously—and we do have a problem here, as is indicated. I think that we have not got into the issue of whether or not you can do due diligence, whether you have mortgaging servicing rights or other products that you are going to sell within these financial entities and if you can, in fact, share that information. Most financial institutions get into confidentiality agreements. They don't share this on an open-ended basis, and so we are obviously recognizing that in the context of what is in H.R. 10.

There is all sorts of concerns about securitization and—not just that, but the expectation, if I am doing business with Citibank and I go over to the mortgage entity, that I don't have to fill out a three-page application again. So there is—we do let them use that name, Citibank Mortgage, Citibank Bank, Citibank Insurance. So there is some expectation that it is the same entity that you are doing business with.

Chairwoman ROUKEMA. I think that having been said, we will adjourn for today and return tomorrow for the second installment. Thank you so much.

[Whereupon, at 2:55 p.m., the hearing was adjourned, to reconvene on Wednesday, July 21, 1999.]

## FINANCIAL PRIVACY

---

WEDNESDAY, JULY 21, 1999

U.S. HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS  
AND CONSUMER CREDIT,  
COMMITTEE ON BANKING AND FINANCIAL SERVICES,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:00 a.m., in room 2128, Rayburn House Office Building, Hon. Marge Roukema, [chairwoman of the subcommittee], presiding.

Present: Chairwoman Roukema; Representatives Bereuter, Royce, Vento, C. Maloney of New York, Watt, Sandlin, Moore, and Gonzalez.

Also Present: Representatives LaFalce, Dingell, and Inslee.

Chairwoman ROUKEMA. I think we will try to come to order here. I would appreciate it if everyone will take their seats at the table, the panel I mean. It is a busy day for all of us, I know. We are ready to move on with this very important hearing. I will try to keep my opening remarks brief by summarizing yesterday's hearing and setting the stage for today. As most here will understand, this is the second day of hearings on financial privacy. As we mentioned yesterday, the privacy issue is addressed in H.R. 10. There are several significant new privacy protections in H.R. 10. Of course, mandatory opt-out for consumers and information sharing with unaffiliated third parties is the focus in H.R. 10, and it is dealt with in a very constructive way.

There is also prohibition on sharing account and credit card information with marketers and the practice of "pretext calling" is criminalized. I think frankly that the financial privacy provisions in H.R. 10 are a good start. In fact, I think it is more than a good start. I think it lays a strong foundation on which we are hopefully going to build as a consequence of the constructive things that we learn here in the first two hearings, and which may result in additional hearings.

In our hearing yesterday, the witnesses included academics and privacy experts, representatives of our smaller financial institutions, credit bureaus, and marketers as well as the consumer groups. We covered a lot of ground. I don't think that we have necessarily digested all of the points that were made, but virtually all witnesses warned against further privacy protections unless extensive hearings and analysis is done. They outlined a few concerns. The majority of them advised against an opt-in approach at this time. They were quite definitive on that, but not unanimous, so

that question is an open question. I am sure that our panelists today are going to address the opt-in approach in depth.

One particular point that I think was well made is that consumers have a right to know who is collecting their information and how that information is to be used. Also, privacy policies must be clear and easy to understand. That there must be agreement. To be meaningful, the customer opt-out process must be clear and straightforward. What does that mean? It means that we have to look carefully at the statutory requirements on the opt-out disclosure provisions. I am hopeful that we will hear more about that today.

Then there were references to the small financial institutions using third parties for many common everyday practices. They pointed out that contracting with third party service providers is vital to the small institutions and that those practices must be protected. One example that they gave, but there are many more, is the check printing. It was also pointed out that data processing by third parties was particularly common and limiting this ability would complicate matters for small institutions.

Many other issues remain with respect to privacy and State laws. Does H.R. 10, or should H.R. 10, preempt State privacy laws? What will do in the future with respect to State-Federal relationship? Should customers be permitted to opt-out of information sharing by financial institutions with their affiliates? That in particular is a key issue of controversy.

In addition, it is possible that good disclosure of privacy policies, that if we have really good statutory disclosure requirements, we may be able to, if not eliminate, at least greatly diminish this intense debate over opting-in and opting-out. Quite frankly, I think this area—disclosure—is going to be a focus of my own attention. I am anxious to hear what our panelists have to say about that today.

Then we are also going to address Section 351 and medical privacy. Do we need to make it clear that the Secretary of Health and Human Services retains his authority to promulgate comprehensive medical privacy rules even if H.R. 10 becomes law? There seems to be some question about that. Mr. Ganske's intention was to preserve the Secretary's authority. Perhaps the statutory language in Section 351 is not as precise as it should be. In addition, we may have not considered all of the ramifications of the medical privacy provisions. This is an issue of particular concern to me.

I think we must be very, very deliberate in terms of medical privacy. The subcommittee will be looking at all of these issues today, and of course with that in mind I will now relinquish the time to my Ranking Member, Mr. Vento, before we introduce the witnesses.

[The prepared statement of Hon. Marge Roukema can be found on page 359 in the appendix.]

Mr. VENTO. Thank you, Madam Chairwoman. I think we made progress yesterday. Of course, we are trying to translate the culture of privacy that pervades financial institutions, which is the basis for trust and confidence of the people we represent in our economic and financial system and taking that culture and translating it into rules and finally trying to codify it for essentially the first

time. As privacy applies to this relationship between our banking and financial entities with the consumers, it is not an easy task.

Of course, it is especially a problem when throughout our communities there is an explosion and so many changes which are affecting the very target that we have in mind. Of course that is exactly the case.

And when we are the first, when other entities frankly are being given the policy path of self-regulation or no regulation and no rules with regards to in fact what is going to be the rights of privacy, financial institutions and those involved in modernization are in an unusual circumstance. I think we did well in terms of what we put together to build a foundation in the House bill. The Senate bill is practically silent on the entire topic except for something called "pretext calling."

So I think we did a good job. Obviously this is not going to be the last word. I dare say that Congress and the public will be looking for policy changes and perfection of this privacy issue down the road. I think it is important that we put in place a foundation. I think that the actions and the interactions of traditional privacy issues that we have taken for granted are very much at risk and very much up for grabs in the electronic communication age, and I think the point that we are trying to do is to maximize the benefits that are inherent in these changes and in the discoveries that are being made in communications to maximize that benefit and to minimize the effect or impact on our own individual privacy.

Those are two goals which may be difficult to reconcile, but at least I think it is what is at the base of this anxiety and the concerns we have heard from consumers. To find and establish policies which in fact achieve that is easier said than done. We have practically invented, or at least have overused, the words opt-out and opt-in in this subcommittee, and have discovered with the instantaneous nature of transactions that take place, not only does it speak to efficiency, but it speaks to great risks in terms of privacy.

So I hope that we in our process in terms of financial modernization will at least help in setting a foundation. Of course it is important that we start to look on a global basis at what the European Union is doing and to establish a policy that is consistent. I think in that consistency develops an understanding in terms of the public in terms of responding to a commercial firm, to the financial entity, to the Internet, to others that are outside the gamut of financial modernization.

Second, I think with the steps that we put in place we do not want to create an avalanche of paper without any positive benefit to the people that we represent. So I think we are on the right path. I am sure that it will take adjustment down the road. We look forward to the help and guidance of the regulators here today and those that have testified in the past on these topics.

Thank you, Madam Chairwoman.

Chairwoman ROUKEMA. Thank you, Congressman Vento.

Any other comments?

Yes, we have the pleasure of having Congressman LaFalce, the Ranking Member of the full committee, with us today.

Mr. LAFALCE. Thank you, Madam Chairwoman. I am delighted that you are having these hearings. I consider them to be ex-

tremely important, and I simply wanted to come to advise the panel how important I think these hearings are.

We have been struggling for years for financial service modernization legislation. We have not struggled for a great many years too with the issue of privacy, but primarily because of the technological explosion which has taken place and the tremendous number of citizens, especially within the United States, but also globally, not nearly to the extent as American citizens' use of that technology, the issue of privacy has come to the forefront of our considerations, the American public's considerations.

Now it is possible for everybody to know every book that you buy. It is possible for everybody to know every video cassette that you rent. It is possible for everybody to know when you go to the grocery store what your favorite products are, and so forth. And virtually everything about your financial status and transactions.

Independently of financial services modernization, this is an extremely important issue. As a matter of fact, I think it is profoundly more important than financial services modernization. I just want to make that clear. The opportunity to do something about this has presented itself during the course of markup, and then it took on a life of its own.

I think we should do as much as we can as part of the financial services modernization. But since it is a related issue, but also independent, as much as we can independently of it, too. The difficulty is we don't have a majority in the Congress. I am not sure how much we will be able to achieve independently, so we have to take up every opportunity to do as much as we can. We did that during the course of the Banking Committee markup. We got so far. We did that in our deliberations with the Rules Committee and we got much further than I ever thought we would.

We had opt-out provisions with respect to third parties, and prohibitions with respect to certain types of marketing, telemarketers, and so forth, and so forth. We created an affirmative obligation on the part of financial institutions to have privacy policies, and we gave you, the regulators, the ability to articulate the standards that would have to be met by the financial institutions. Otherwise they would be in breach of an affirmative obligation. This was significant. The first thing that I am interested in hearing from you is an evaluation of what we did, what we did right and what we did wrong, what we might be correcting.

Second, as part of that, I am a little concerned about what we did with respect to medical privacy. We do not have tremendous expertise within our committee on the issue of medical privacy, and I want to make sure that what we did with respect to medical privacy in no way infringes, in no way infringes no matter what we pass, the ability of the Secretary of HHS to promulgate regulations effecting medical privacy standards above and beyond anything we might do.

Additionally, I want to make sure that the exceptions within the present law with respect to medical privacy do not create loopholes that we will be sorry for later. If that is the case, we ought to just omit that entire provision.

Then whether we will be able to do it as part of financial services modernization, and I think it is problematic, because I don't know

if we will be able to go beyond where we have gone in the House, there is the issue of opt-out, not just for third parties, but for affiliates. A lot of us believe that can be done certainly at the appropriate time with the appropriate vehicle. I want your thoughts on that issue, too.

Yesterday I was here when the professor from Georgetown said yes, this can and should be done. It is a matter of technology, is a matter of cost, yes, absolutely. If you have thoughts on that issue, because the industry monolithically is saying, no, no. We are not talking about an opt-in, we are talking about an opt-out there. What are the concerns of the—what are the validity of the concerns of the industry? We would not be prohibited, we would not be calling for an opt-in, simply for an opt-out basically for marketing purposes with affiliates, something they desire to do, and probably could do with 99 percent of their customers even if there were an opt-out provision.

But that is a focus of debate within the Congress and I appreciate your thoughts on that issue, too. And I thank you all very much.

Chairwoman ROUKEMA. Mr. Bereuter.

Mr. BEREUTER. Madam Chairwoman, I commend your role in holding the hearings. I look forward to hearing the panel.

Chairwoman ROUKEMA. I might say as a follow-up to what Mr. LaFalce has given us in terms of the background of H.R. 10, I was a co-sponsor of the privacy provisions in H.R. 10. I think everyone here should know, and if they don't, I will inform them, that the privacy amendment passed overwhelmingly in the House, 427-to-1.

But I also want to state that I took the initiative of setting up these hearings prior to floor consideration of H.R. 10. These hearings were planned prior to any thought that we would be able to link privacy, appropriately in my opinion, to H.R. 10. Indeed, I felt that there were large questions of privacy that demanded our attention and that it would be irresponsible if we did not have a set of hearings on the subject and explore the whole range of issues that are connected.

So again to repeat, I feel as though we have made a start. We have set a foundation, but it is not complete until we give due consideration to all of your concerns here and those of the other panelists.

Now we will hear from Mr. Moore. Excuse me, Mr. Inslee, I believe you were here first.

Mr. INSLEE. I just want to thank the Chair for holding this hearing, and I want to point out that the Chair had the foresight to really plan these hearings even before America knew about these sordid practices because this Chairwoman had the foresight to recognize the importance of this issue even before the exposé hit the newspapers, which showed that banks were taking Americans' personal financial information and selling it to marketers across America. Those suspicions have been confirmed in Minnesota and various other States across the country.

I am convinced while we have made a start in the House version of H.R. 10, we have made a start involving third party sharing with telemarketing, marketing purposes, we have left an enormous loophole that you can drive an armored truck through to allow

marketing purposes to allow that personal intimate financial information to be used by affiliates for not banking purposes, for not purposes of checking accounts, for not purposes of savings account, but for marketing purposes. And we need to find a way to plug that loophole and find a way that does not interfere with the legitimate banking operations of the industry.

I am here to ask the panels to address that issue. How do we plug that loophole and allow Americans to allow their personal information to be used for the purposes intended and not for marketing purposes. I believe 30 years plus one day ago we put a man on the Moon, and we can certainly plug this loophole, and I would like to ask you to help us figure out how to do that.

Thank you.

Chairwoman ROUKEMA. Thank you.

Mr. Moore.

Mr. MOORE. I would just like to echo the eloquent comments of Congressman Inslee and I appreciate the fact that he submitted an amendment during the hearings on this bill, and I also wanted to mention the fact that during the hearings on this bill, H.R. 10, we were promised that we would have an opportunity for hearings on the privacy question and so, Madam Chairwoman, I really appreciate your convening this hearing and giving us an opportunity to hear all of the expert witnesses who have testified today and yesterday about the privacy issues.

Thank you.

Chairwoman ROUKEMA. Thank you very much.

Now just a few administrative announcements. According to the rules of the committee, for those witnesses here today you should know that all of your written testimony will be automatically included in the official record of this hearing. Witnesses are limited, or at least we try to limit ourselves to what we call the five-minute rule. Those lights in front of the witnesses will give you an idea of when your five minutes are up. I will try to be respectful of you, but please try to cooperate and condense your comments to meet the five-minute rule. I would make that same comment also for my colleagues on the subcommittee. We should try to keep our questioning period within the five-minute rule. Your written testimony will be part of the official record. Members will also have the opportunity to submit questions to witnesses in writing as follow-up questions under the rules of our committee. The hearing record will be left open for the customary period of time for additional comments or additional statements that you want to include in the hearing, the official record of the hearing.

With that let me introduce our first panel. The first panel is regulators who regulate, in one capacity or another, components of the financial institutions. We have Federal and State regulators represented here today. Let me introduce all of you and then we will begin with Mr. Gensler.

Mr. Gary Gensler is Under Secretary for Domestic Finance, Department of the Treasury. The Under Secretary has appeared before us previously and we welcome him here today. We look forward to his testimony, which I have a sense is going to be very instructive and opposite of some of what we heard yesterday.



Governor Edward Gramlich, we welcome you today. Governor Gramlich is a member of the Board of Governors of the Federal Reserve System. Mr. Gramlich, I believe you have been on the Board since 1997. We welcome you here today. You have significant experience and I don't know whether you are speaking on behalf of the Chairman, Chairman Greenspan, but he has given you permission to be here today.

Mr. GRAMLICH. For the whole Federal Reserve Board.

Chairwoman ROUKEMA. Our third witness is the Comptroller of the Currency. We appreciate Comptroller John "Jerry" Hawke, Jr., being here. Comptroller Hawke has been here several times and is always constructive in his testimony.

Our fourth witness is the Chairman of the Federal Trade Commission, Robert Pitofsky. The FTC has primary legislative responsibility over the Fair Credit Reporting Act. That legislation is central to some of these privacy issues that we are dealing with here. It is the Federal law which permits entities to share customer information with affiliates in a holding company structure. That gets right into the heart of the issue—financial institutions sharing customer information with affiliates without getting customer consent. I understand that you have recently made some somewhat controversial comments, or definitive if not controversial, regarding internet privacy. We will follow up on that.

Our fifth witness represents the Securities and Exchange Commission. Annette Nazareth is Director of the Division of Market Regulation, and is testifying on behalf of the SEC.

Then we did say that we are going to include the State regulators and we have one here today, Connecticut Commissioner of Insurance, Mr. George Reider, Jr. Commissioner Reider is the current President of the National Association of Insurance Commissioners. We welcome you, Commissioner Reider.

You are going to have significant work to do here today.

Thank you, and without further delay I will defer to Mr. Gensler of the Treasury.

#### **STATEMENT OF HON. GARY GENSLER, UNDER SECRETARY FOR DOMESTIC FINANCE, DEPARTMENT OF THE TREASURY**

Mr. GENSLER. Madam Chairwoman, Ranking Member Vento and Members of the subcommittee, I am pleased to have the opportunity to present the Administration's view, not just Treasury's view, the Administration's view on financial privacy.

Today many Americans increasingly feel their privacy threatened by those with whom they do business. Americans want the ability to earn, invest and spend their money without having to expose their lives to those who process that information, just as they would not expect a letter carrier to open their mail. Americans deserve that right. For much of our history, consumers were justifiably confident about their financial privacy. That confidence is on the wane today due to three important developments.

First, today's ordinary desktop computer has significantly more power than the mainframes of 30 years ago. Vast amounts of information can be stored, sorted, manipulated and analyzed at lower and lower costs.

The second key change is the growing integration and consolidation in financial services firms.

Third, Americans increasingly use credit cards, debit cards, electronic bill payments, and direct deposit in lieu of cash, and thus financial services firms are able to collect far greater amounts of information.

Taken together, these three trends provide the means, motive and opportunity for financial services firms to mine consumer information for profit.

Our challenge therefore is to protect the privacy of consumers while preserving the benefits of competition and innovation.

On May 4, the President outlined the Administration's financial privacy and consumer protection initiatives. Protecting financial privacy led the list of key principles for consumer protection. When the President announced this agenda, some may have viewed the proposals as ambitious. Only two months later, however, leadership by the President and the Members of this subcommittee and the House have sparked a debate that has produced dramatic results. Most overwhelmingly, the privacy vote in the House. Today I will address five basic issues that we believe Congress ought to consider as privacy legislation moves forward.

First, scope. We believe that the transaction and experience data must be protected regardless of the type of financial institution at which it is held.

Second, the concept of notice. The Administration believes that every financial institution should establish and disclose a privacy policy that covers information sharing with both affiliates and third parties. Disclosure of an institution's information practices is a precondition to consumers choosing how their information will be used or choosing to do business elsewhere. The Administration believes that this should be meaningful notice and be provided to customers upon account opening and annually.

The next issue is choice. The Administration believes that consumers should have the choice to opt-out of—that is to say “no”—to the use of their data by both third parties and affiliates. Choice allows consumers to make their own decisions as to the potential tradeoff between on the one hand, their financial privacy, and on the other hand, the marketing opportunities and other potential benefits of information sharing. This is a very personal decision which is most appropriately left to an individual.

Congress has embraced notice and choice—for both affiliates and third parties—in the Fair Credit Reporting Act. The FCRA has given consumers the right to notice and the opportunity to opt-out before a company shares certain credit information with an affiliate. Financial firms have a proven record in finding how to work with notice and opt-out.

The fourth issue is exceptions. While the Administration is firmly for choice, we also believe that there is a need for balance. There are some types of information sharing where consumer choice may not be appropriate. In approaching any exceptions, we think three questions are appropriate. First, what is the consumer's reasonable expectation of privacy? Second, what is the purpose of the transfer? Third, what are the costs of allowing choice? Any decision should be based on a balance of these factors.

The Administration strongly believes that in most cases the balance counsels for choice, whether sharing with a third party or an affiliate. We also support strict limits on reuse of information shared pursuant to any exception.

Perhaps the clearest case for choice is in the area of medical privacy. We strongly oppose, however, the medical privacy provisions of H.R. 10, which undercut stronger and more comprehensive protections to be promulgated later this year.

The sale of marketing information to a third party also appears to be a clear case where no exception is appropriate. In some cases though, the case for an exception may be stronger. Financial services firms may wish to provide customers a consolidated account statement so they can see the picture with the whole organization.

Other cases present more difficult tradeoffs, and we think these three principles are the best way to think through these as we move forward. But I think that it is important that where a consumer is spending his money and the purposes for which a consumer is obtaining credit should remain subject to notice and opt-out. How we live our lives, what we believe, the choices we make, all of these very personal pieces of information should not be shared without our consent.

Last, the complexity and uncertainty of this task leads to one further point, the need for regulatory flexibility. We should allow many of the details to be worked out by the regulators that know the financial services industry best, after taking into account public comment.

I wish to thank you again for allowing me to appear here today, and I look forward to any questions.

[The prepared statement of Hon. Gary Gensler can be found on page 365 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Mr. Gramlich of the Federal Reserve Board.

**STATEMENT OF HON. EDWARD M. GRAMLICH, MEMBER,  
BOARD OF GOVERNORS, THE FEDERAL RESERVE SYSTEM**

Mr. GRAMLICH. Thank you, Madam Chairwoman, and other subcommittee Members. You are all to be commended for efforts to resolve the vital issue of customer financial privacy. Information about individuals' needs and preferences is a cornerstone of any system that allocates goods and services within an economy. The more information about needs and preferences available, the more accurately and efficiently will the economy meet these needs and preferences. But though the availability of information promotes economic efficiencies, there is also a long recognized value in permitting individuals to maintain a zone of privacy. To date, conflicts between the two goals have been largely handled in the marketplace where the competitive value to the companies of customer information has been traded off against the competitive value of providing customer privacy.

The current privacy debate concerns information that banking and other financial institutions derive from their relationships with customers. This may include information submitted by a customer in order to obtain a loan or deposit, information about transactions or information obtained by a bank from third parties such as a

credit report. The economic value to a bank is unquestionable, but the information also has value to others who may wish to sell goods or services to the customer.

In the area of financial information, many customers clearly believe that an implicit contract exists between the financial institution and the customer requiring the financial institution to keep information confidential. Control of information about ourselves is a fundamental means by which we manage our relationships with each other. The feeling that financial information should be private has deep historic roots, and bankers and customers have long viewed their business relationship as involving a high degree of trust which could be threatened by violation of privacy.

The testimony goes on to give a few examples of how customers value both economic efficiency and privacy, examples that are in the testimony and that I won't read.

The environment presents the Congress with a series of important questions. Are banking practices involving customer information developing so quickly that customers will be unable to respond to these practices effectively? If so, can market processes be made more efficient without lessening privacy protections? If not, must Congress strike the appropriate balance between these competing interests? Congress has already addressed the issue. In the Fair Credit Reporting Act, governing the exchange of customer data by and with consumer reporting agencies, Congress balanced the issue of privacy and efficiency by allowing institutions to share information related solely to the institution's transactions and experience, but by also requiring that each customer be provided with a right to opt-out of sharing between affiliates of any other type of customer information. There are a few other examples in the testimony of how Congress has already addressed some of these privacy issues.

The additional privacy protections of H.R. 10, particularly those giving customers the right to opt-out and thereby limiting the sharing of the institution's own experiences and other transactional information with third parties, would generally improve the privacy protections for bank customers. There are a number of important details here and without getting into some of the questions that Gary has just raised, we would emphasize a few points in this dispute.

One is the importance of exceptions necessary to make the payment system work smoothly. Another is to establish consistency across markets to ensure that any limitations imposed on one industry, such as financial services, do not place that industry at a competitive advantage. Our lawyers have gone through H.R. 10, and there are some points in which the drafting might be clarified, and we would be happy to offer our assistance on that score.

Finally, the time period for adopting or implementing regulations is very ambitious. Perhaps the implementation period could be extended to at least a year.

Thank you very much for an opportunity to testify on this very important matter.

[The prepared statement of Hon. Edward M. Gramlich can be found on page 382 in the appendix.]

Chairwoman ROUKEMA. Thank you, Mr. Gramlich.

The Comptroller of the Currency, John Hawke.

**STATEMENT OF HON. JOHN D. HAWKE, JR., COMPTROLLER,  
OFFICE OF THE COMPTROLLER OF THE CURRENCY**

Mr. HAWKE. Madam Chairwoman, Congressman Vento, and Members of the subcommittee, thank you for the opportunity to testify about an issue that has enormous ramifications for the banking industry and their customers—financial privacy. The relationship between banks and their customers is built on the pervasive assumption of customers that their banks will maintain the confidentiality of that relationship. While technological advances and the demands of a competitive marketplace have placed a premium on the availability of personal information, often at the expense of personal privacy, the way in which banks respond to these pressures is of enormous importance. If banks fail to honor customer expectations that personal information will be kept in confidence, they will impair the most priceless asset of their banking franchises—the trust of their customers. Thus, privacy is not just a consumer issue; it is an issue with long-term implications for the vitality and stability of the banking system.

By its very nature, banking is driven by information. Bankers have always relied on access to personal financial information to make fundamental judgments about their customers' qualifications for financial products and services. Information exchange has thus served a critical market function which has benefited consumers and financial institutions alike by facilitating credit and other financial transactions.

Recent advances in technology that permit the efficient collection, storage, analysis and dissemination of vast stores of information, coupled with the changing structure of the financial services industry and the development of efficient new delivery systems, have increased the market value of customer information. Although financial conglomerates may profit from the cross-marketing opportunities and consumers may benefit from the availability of a broader array of custom-tailored products and services, there is a serious risk that these developments may come at a price to individual privacy. The challenge is how to balance those competing considerations.

H.R. 10 as passed by the House adopts a measured approach which provides consumers with notice and choice about certain of the information-sharing practices of financial institutions, without impeding the flow of information essential to doing business. This is a positive step in assuring customers that their information will be handled appropriately and providing consumers with increased control over their personal information.

In my view, however, a serious question can be raised whether H.R. 10 adequately protects the confidence of customers in the confidentiality of their relationship with their banks. In his May 4 proposal regarding privacy, the President indicated his support for legislation that would give consumers control over the use and sharing of all their financial information, both among affiliates and with non-affiliated third parties. H.R. 10 is a good first step toward meeting that goal, but I believe customers will expect more. In particular, the distinction that H.R. 10 makes between information

sharing with affiliates and non-affiliates, allowing customers to opt-out with respect to the latter, but not the former, is, I believe, likely to erode customer confidence rather than enhance it.

Is it realistic to think that customers will see a meaningful distinction between information sharing within the same corporate family and with unrelated entities? Will customers believe that the legislation adequately covers their reasonable expectations regarding the use and transfer of confidential information they have imparted to their banks? If the answers to these questions are in the negative, the failure to provide protection for the sharing of information with affiliates could have a profound effect, particularly in a world of expanded financial conglomeration on the willingness of customers to maintain the kinds of relationships with the banking system that they have had in the past. I should mention when I was with the Treasury Department in Mr. Gensler's position, we did a survey of the unbanked and found that at least 25 percent of the people who do not have bank accounts gave concerns about confidentiality as one of their reasons. While the desire of bankers to take advantage of new cross-marketing opportunities is entirely understandable, a primary objective of policymakers should be to assure that doing so does not cause fundamental damage to the banking system.

I cannot overstate the importance of addressing consumer expectations about the confidential treatment of financial information to maintaining the public's confidence in the banking system. And I urge that, in crafting an appropriate response to consumer privacy concerns, banks and Congress put themselves in the shoes of a customer and ask, "Will my financial institution use my personal information in a manner consistent with my expectations, and will I have any control over the use of my information?" Whatever legislative formulation ultimately results, American consumers deserve the right to be able to answer "yes" to those questions.

Thank you, Madam Chairwoman.

[The prepared statement of Hon. John D. Hawke, Jr. can be found on page 394 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Mr. Pitofsky, Chairman of the Federal Trade Commission.

#### **STATEMENT OF ROBERT PITOFSKY, CHAIRMAN, FEDERAL TRADE COMMISSION**

Mr. PITOFSKY. Thank you, Madam Chairwoman, and Mr. Vento and Members of the subcommittee. I appreciate the opportunity to present the Commission's views on H.R. 10. The FTC has been involved in developing consumer rights in the area of privacy for some time. I am pleased on behalf of a majority of the Commission to support fully H.R. 10, which concerns privacy in the financial sector.

Privacy is not a set of issues where one size of regulation fits all. But when it comes to financial records, Congress and the regulatory agencies have been consistent and clear that privacy rights are especially important. All studies that I am aware of show that consumers care deeply and have expectations about the way in which their personal financial information will be treated. The heart of privacy protection must be notice, which is a clear and con-

spicuous disclosure of what are the privacy policies of financial institutions, and consent, opportunity for consumers to deny to financial institutions the ability to sell or otherwise transfer personally identifiable information. H.R. 10 does that.

Now, just a week ago on behalf of the Commission I testified before another committee with respect to privacy in the online universe and the majority of the Commission looking at the progress of self-regulation took the view that at this time we ought to allow self-regulation to proceed awhile to see if it really gets to the finish line. If it does not, then legislation would be appropriate. But I want to emphasize that the Commission unanimously does not believe that is the right prescription in this area. On the contrary, financial information is different. It is different for the reasons that I have already stated. Consumers believe it is different, and they have a different set of expectations. Congress has treated financial information differently time and time again. The regulatory agencies have acted as if it is different.

Now, I do believe that H.R. 10 should go a step further. It should include a provision that applies these essential rights of notice and consent not just to financial institutions when they transfer information to third parties, but also to transfers between financial institutions and their affiliates. Typically consumers do not appreciate the complex ownership and control relationships between conglomerate corporations and therefore are not aware that privacy protections might not apply to a transfer of information to a financial institution to one of its affiliates. I don't know myself all of the affiliates of my bank or other financial institutions that I deal with, and I can only assume that consumers are a little bit like me. If they should have the right to notice and consent generally, they ought to have the right to notice and consent when it comes to affiliates.

Finally, I am pleased to support the important provisions of H.R. 10 that outlaw the practice of obtaining personal financial information by deceit or pretexting. The Commission supports civil and criminal sanctions against pretexting and in April of this year, brought what I believe is the first and only Federal court challenge involving pretexting. The complaint alleges that the defendants violated Section 5 of the Federal Trade Commission Act when they obtained consumers' private information from a bank by impersonating bank account holders and making false statements to financial institutions to induce the disclosure of consumers' private financial privacy. Statutory confirmation that pretexting is unacceptable is useful and the right thing to do.

In conclusion, the financial modernization which is the heart of H.R. 10 can produce great improvements to the economy and benefits consumers. On the other hand, it is important, as the sponsors of H.R. 10 recognize, to ensure that this step forward is not accompanied by strong measures to protect consumer privacy.

Thank you very much.

[The prepared statement of Robert Pitofsky can be found on page 425 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Ms. Nazareth, Director of the Division of Market Regulations of the SEC.

**STATEMENT OF HON. ANNETTE L. NAZARETH, DIRECTOR, DIVISION OF MARKET REGULATION, SECURITIES AND EXCHANGE COMMISSION**

Ms. NAZARETH. Thank you, Madam Chairwoman, Congressman Vento, and Members of the subcommittee. I am pleased today on behalf of the SEC to testify regarding financial privacy.

The Commission supports the legislative efforts that are currently being made to enhance financial privacy and believes that H.R. 10 is an important step in creating a consistent and enforceable privacy protection framework for American investors.

To begin with, I think it is fair to say that most of us expect our financial transactions and financial information to be private. Meeting this expectation is one way that financial services providers demonstrate their integrity and earn their customers' confidence. That confidence is essential to the continued success of our financial markets and institutions, including those that the Commission regulates. Although the Federal securities laws do not contain an express requirement for registered broker-dealers, investment advisers or investment companies to safeguard their clients' personal financial information, the Commission has reminded these entities that as financial professionals they should protect this information. More particularly when broker-dealers, transfer agents and investment advisers deliver personal financial information through an electronic means, the Commission has required them to take reasonable precautions to ensure the integrity, confidentiality and security of that information.

In addition to being regulated by the Commission, broker-dealers are regulated by securities self-regulatory organizations, or SROs. We believe that these SROs, which are required to have rules to promote just and equitable principles of trade, have the authority to address privacy concerns. SROs have used this authority to bring disciplinary actions.

Until recently the privacy of customer financial information has not been an issue for most businesses. As a practical matter, the inability of business to share information on a large scale has protected customers' financial information. In addition, businesses, had and still sometimes have, commercial reasons for wanting to retain control of their own customer information.

The landscape is changing. The exponential growth in electronic commerce and technology means that more information can be collected, not to mention stored, sorted and analyzed more quickly than ever before. Financial modernization and the consolidation among banks, securities firms and insurance companies portends the development of huge databases of customer information.

There is, however, another side to the coin. Financial institutions often have a legitimate need to share personal financial information. A good example of this is credit checks. Another example is when a customer does business with two affiliated companies, and the companies share information in order to save the customer time and trouble.

So what is the difference between legitimate information sharing and violations of a customer's privacy? The key here is the customer's expectations. If a bank customer opens a bank account linked with a securities account offered by a bank's securities affli-



ate, the customer might expect and even intend for the bank to share information with the securities affiliate. The customer might not, however, expect the bank to share this same information with a third party that was marketing other financial services. As Congress considers the many issues inherent in reforming financial services regulations in this country, it is appropriate that privacy be among these issues. The Commission agrees that Congress, as well as financial regulators, should evaluate how to insure that financial services customers' expectations of privacy are met.

The Commission supports the provisions in H.R. 10 that enhance the privacy protections available to American investors. More specifically, we support requiring financial institutions to disclose their privacy policies to their customers. We are also sympathetic to giving customers the ability to decide whether their financial information will be shared in some instances even among affiliates, and particularly when it is to be used for marketing purposes.

Any legislative proposal to heighten financial privacy protections needs to balance a number of concerns. Financial services providers may have to engage in a certain amount of information sharing in order to do their job. They may also use information sharing as a cost saving device. As firms consolidate, they enjoy many efficiencies of scale, including the ability to avoid duplicative information gathering. Customers as well as firms can benefit from these efficiencies. Customers, however, should know when their personal information is going to be shared and they should have a voice in saying how far that information should go.

The Commission also strongly supports an exception for information shared in the context of executing transactions. Elements of apparently seamless securities transactions often involve parties that must share customer information in order to continue to provide the services customers have come to expect. Depending on the size and structure of the firm involved, these parties may or may not be affiliated.

In conclusion, I appreciate the opportunity to testify today on behalf of the Commission. We would be happy to work with you and your staff going forward in addressing these issues relating to the SEC, investors and the securities industry generally.

[The prepared statement of Hon. Annette L. Nazareth can be found on page 443 in the appendix.]

Chairwoman ROUKEMA. I thank you very much.

Mr. Reider, President of the National Association of Insurance Commissioners.

**STATEMENT OF HON. GEORGE M. REIDER, JR., COMMISSIONER OF INSURANCE, STATE OF CONNECTICUT; PRESIDENT, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS**

Mr. REIDER. Good morning, Madam Chairwoman, and Members of the subcommittee. My name is George Reider, and I serve as Insurance Commissioner in Connecticut, and President of the National Association of Insurance Commissioners. I am pleased to be here today to testify on financial privacy issues.

At a time when it seems that anyone can retrieve your financial information at the click of a button, it is important for consumers

to know that protections are in place so that their personal financial information is not unfairly used. The challenge for Congress and the States is to determine how much disclosure is acceptable so companies can do business, regulators can enforce the laws and consumers' personal financial information is protected.

I will address this balancing act by making four points. My first point: privacy means keeping personal information confidential and protecting the integrity of the regulatory system. Like banks and security firms, insurers collect and have access to personal financial information about their customers. Similarly, State insurance regulators have access to personal information about insurance consumers in their States. Both face the need to share information in order to do business the right way, but both must also protect consumers. People legitimately expect that companies holding personal information will not use it to take unfair advantage of them. At the same time, consumers are realistic. They understand that disclosure of some of their information is necessary for typical business needs, like billing and record keeping. And they know that sometimes disclosure of information can result in real advantages for them in the form of cost savings and convenience.

Protecting privacy also entails protecting the integrity of the regulatory system. People must have confidence that information is being used to protect them.

My second point, the States and the NAIC have taken actions so that insurance companies and agents will protect personal financial information. We are constantly working with our fellow States through the NAIC to monitor insurance privacy issues and assess the need for further action. I will give you two examples of privacy laws that we have enacted in my home State of Connecticut.

Several years ago we enacted a comprehensive insurance information privacy law based upon the NAIC's Insurance Information Privacy Model Act. The law establishes standards for the collection, use and disclosure of insurance information. It seeks to maintain a balance between the need by insurance companies and agents for information and the need of consumers for fairness in insurance information practices.

In addition to the comprehensive privacy law, we have specifically addressed the sharing of financial and other insurance information by banks that sell insurance and annuities in Connecticut. Like the privacy law, the insurance sales law requires the prior written consent of the customer before the bank may share information.

My third point. The States and the NAIC are working to ensure that regulators protect confidential information. First, we are revising confidentiality provisions in NAIC model laws to strengthen the ability of State insurance regulators to keep sensitive regulatory information confidential. This will help preserve the privacy of individuals and entities in addition to providing a strong platform for States to use in entering into confidential agreements with State, Federal and international regulators.

Second, we are addressing confidentiality issues and regulatory information exchanges with other regulators, including some of the Federal agencies represented by the distinguished members of this panel.

The NAIC recently approved a model consumer complaint information sharing agreement with the Office of the Comptroller of the Currency. The purpose of this model agreement is to ensure that consumer complaints about bank sales of insurance are routed to the proper regulator. Ten States have already implemented agreements based on the model and several other States are scheduled to sign agreements in the coming weeks.

The NAIC is also working with the Office of Thrift Supervision and the Conference of State Bank Supervisors to develop broad-based regulatory cooperation agreements. We expect these agreements to be completed soon. The model regulatory cooperation agreements have strong confidentiality provisions, making it clear that confidential information is to be protected to the fullest extent possible.

My final point. Congress should consider improvements to facilitate the protection of confidential regulatory information. In order to protect personal information, the States need to be able to share information to stop bad actors, and we need to be able to prevent the disclosure of that information.

Congress could take several steps that would strengthen our ability to protect the privacy of personal and financial information. These include amending Federal law to clearly protect confidential information exchanged between State insurance regulators and Federal and international regulators, giving State insurance regulators access to the FBI criminal database so we can better guard against fraud and abuse and protecting insurance information databases operated on behalf of the States from frivolous lawsuits.

My written testimony contains more information on these proposals and I would be happy to discuss them further here today or in the coming weeks.

Madam Chairwoman, I applaud you for holding these hearings on this most important matter and certainly appreciate the opportunity you have provided for our testimony here today. Thank you very much.

[The prepared statement of Hon. George M. Reider Jr. can be found on page 465 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Well, I have two aspects of this and they may be closely inter-related, and I referenced them in my opening remarks, and in one form or another you have addressed them, but not with the precision that I am looking for. Perhaps you could, and Mr. Gensler, I did understand your reference to regulatory flexibility, but—I don't know, did you say not statutory, but regulatory flexibility? The implication is that nobody has recommended statutory language which is clear enough, but don't go into that quite yet until I get to the question of disclosure. Everybody is for disclosure. What my concern is is that someone's definition of appropriate disclosure could be another person's definition of huge loopholes. In my opening statement I did say that the disclosure issue came up in my mind over and over again yesterday: Do we not need a clear Federal statutory requirement regarding what the disclosure should entail and the timeframes? That is question one.

The other issue I want as many of you as possible to give me a little more specificity on this affiliate question. I tend to agree with

you about the affiliate issue as I have understood at least three of you. But the industry, which we will hear from later as well as those we heard from yesterday, is strongly opposed to any interference in the sharing of customer information with affiliates. They oppose additional disclosures, opting-in and other new requirements, because they feel strongly that it will interfere in their business operations and their daily operational needs.

I would like to hear from you who specifically referenced the affiliate question and the disclosure, Mr. Gensler.

Mr. GENSLER. Thank you, Madam Chairwoman. First regarding disclosure, on disclosure we think it should be addressed in a statute, and that there should be disclosure both for third parties and affiliates. H.R. 10 did provide for it for third parties. We think that it is critical for consumers to also have an understanding of what is happening with affiliates, that disclosure should be clear and conspicuous—and by that we mean meaningful, that people can see it and understand it—it is not the small type at the end on the back of the documents, and that it be provided at least at the initial account opening and annually thereafter. If that were provided for in the statute, there still, with developments in the future, would be some need for regulatory flexibility to implement that statutory guidance.

On the affiliate matter, we think that it is critical to address both affiliate and third party notice and choice. With industry consolidations, consumers' expectations of privacy can relate equally to affiliates and third parties. If I am a bank customer of a Maryland bank and that bank happens to affiliate with a California insurance company or it may affiliate with a travel magazine, as could be provided for under H.R. 10, I think it is a reasonable expectation that my private information with a Maryland bank is still with that Maryland bank. H.R. 10 does provide for affiliation with institutions which may be incidental to financial activities and to some extent even activities complementary to such activities.

In addition, I would also like to note that restricting only third party sharing would tend to confer a competitive advantage on large banks which have many affiliations as opposed to small banks which tend to use third parties to service customers.

As I noted in my prepared remarks, banks have found that this can work. Under the FCRA, there is notice and opt-out for both third party and affiliate, but particularly I wanted to focus on the affiliate matter and it does work.

Chairwoman ROUKEMA. Thank you. I am going to violate my own five-minute rule, Mr. Ranking Member, but I do have to hear from one or two others. Would you like to address the affiliate question or the statutory question on disclosure, Mr. Pitofsky?

Mr. PITOFSKY. Let me say a word about disclosure. That is an area that we have 85 years of experience. First, I think it does make sense for the statute to address the question of content and timing. On clear and conspicuous it is sort of a common law rule. We have a lot of precedent in that area and rule, what is clear and conspicuous in terms of size, and I would be glad to furnish that to the subcommittee in a separate writing.

Chairwoman ROUKEMA. you may address either the affiliate or disclosure question.

Mr. Hawke.

Mr. HAWKE. I would simply repeat what Mr. Gensler and Chairman Pitofsky have said about the affiliate question and disclosure.

I think the distinction between affiliates and non-affiliates is untenable. I don't think customers make that distinction. But, the point that concerns me most is what the failure to have that protection means for the long-term health of the banking system.

There is another point here, Madam Chairwoman. The chamber of horrors described by the industry with respect to the burdens of an opt-out from affiliate sharing needs close examination by the subcommittee. I think that organizations that want to share customer information with affiliates can make a pitch to their customers as to why it is in the customers' interest to share, and I think a great many customers will be persuaded that it may benefit them to allow information sharing. It is not simply a passive proposition where the institution cannot tell customers about the benefits of information sharing.

Chairwoman ROUKEMA. Thank you.

Ms. Nazareth, did you want to add something?

Ms. NAZARETH. Yes, I generally support everything that has been said here. I don't want to lose sight of the fact, however, that the underpinning of this is that we care about the customers' expectations, and I think the bill as currently drafted does rightfully note that there are certain areas where exceptions to disclosure might be appropriate because it comports with the customers' expectation. They would not necessarily need an opt-out if what you are doing is sharing information among affiliates to do something, such as settle a transaction.

Chairwoman ROUKEMA. That is where we get into more complexity.

Mr. Gramlich.

Mr. GRAMLICH. We did not focus on this issue in our testimony, and I don't want to take a strong position on it. Some of the things said on the panel are undoubtedly true; that is, consumers don't really know all of the affiliates of their financial corporation. There may be a competitive advantage issue, but I would just like to put in a word of caution. What H.R. 10 is all about is permitting the synergies of financial combinations, and so there may be some ways in which it is difficult for people here in Washington to figure out all of these synergies.

It may be necessary to go through and put in more exceptions into the bill. There are eight now and there may be more if you get into sharing within affiliates. This is just a word of caution. There may be some hidden complications here.

Chairwoman ROUKEMA. Thank you very much. That is very helpful. But again, we don't have a clear road map here. We will have to keep working on it together.

Mr. Vento.

Mr. VENTO. Thank you, Madam Chairwoman. A lot of focus has been on this opt-out and trying to analyze what works. We say that we have 90 percent of the people that are polled want this, but only a fraction of 1 percent actually exercise it. So there is some discrepancy here between the 80 percent and the less than 1 percent that exercise it in my mind's eye.

There may be a lot of reasons for that. You can blame it on the modus operandi in which the regulators have put the material on the back and the sort of confusing statements that deal with fair credit reporting and if we had it on this issue it would be much more clear. We all know what consumers want. Consumers want to be left alone and not be cross marketed whether it is with a third party or an affiliate. I understand that. I suppose, though, we should recognize that if I am going to do business with a small institution versus a large one, I obviously should expect some differences with regards to what they can and cannot do for me.

Mr. HAWKE. If surveys show that 90 percent of customers want the ability to opt-out, but only 1 percent are exercising that option under present law, in my mind it would raise an important question about the adequacy of the disclosure of the opt-out. We are not permitted under the FCRA to examine banks except upon complaint. One of the things that H.R. 10 would do is—

Mr. VENTO. I know. Since 1996 I favor that particular change that you are referring to, Comptroller Hawke. So I understand that issue.

I am concerned about having some affirmative responsibilities. As you look at the universe and the magnitude of what this privacy legislation and what effects H.R. 10, we are going to go with every bank in the country, with each insurance firm, State and Federal, the magnitude of this is pretty significant considering what we are doing. Obviously if we are cautious about it, and make certain about what the consequences of our actions are, it is important.

So I appreciate the guidance and help, but I also want to make sure that we do things that are effective. At the same time, Mr. Pitofsky, I went after the FTC because of their avowed devotion to self-regulation with regards to the Internet, but yet of course their enthusiasm for us to go further with the category of institutions which I think ought to have a higher standard as financial institutions, but yet I am trying to understand the difference between the Internet and some of the transactions that might take place on it and the information that is conveyed on it which is financial in nature and personal in nature, and the type of policies that we have before us, and I don't see the differences.

Mr. PITOFSKY. Well, Mr. Vento, we all want to get to the same place. We all want to ensure that consumers have the opportunity to be told what will happen to personally identifiable information and to opt-out, to consent or not consent. The only question is how is the best way to get there. In the online universe you are dealing with an extraordinarily dynamic new sector of the economy in which self-regulation has moved from notice—14 percent, which we criticize as being terribly disappointing—to 66 percent in one year. So the Commission's view, they have gone from 14 to 66 in one year, let's wait a little while and see if we get all of the way there through self-regulation.

Mr. VENTO. We are about 66 percent with banks, too, in terms of disclosure statement.

Mr. PITOFSKY. I don't know what the percentage is there. All I am saying is that the industry was challenged. They went from 14 to 66. Under the circumstances we said if you can get all of the way there through self-regulation, fine. If not, we will be back be-

fore Congress after a thorough evaluation. If it bogs down, we will be there recommending regulation. But in light of the progress that has been made, we thought it was premature at this time. That is our only reason for—

Mr. VENTO. Don't you think that there is a necessity to have a universality in terms of what the foundation is in terms of privacy that would be reflected both in the financial modernization and in terms of the Internet and other commerce and commercial firms?

Mr. PITOFSKY. No, that is the point that I was trying to make in my testimony when I said this is not an area where one size fits all.

Mr. VENTO. But some of the foundation should be the same in terms of disclosure in terms of opting-out or opting-in. I think there are certain predicates that should be in place. I think that they need to be adjusted to meet the need, but there should be some common touchstones in these matters. Otherwise regardless of the disclosure, we are going to end up confusing the public. I think there is going to be an avalanche of paper.

As you look at the legislation, the distinction between commerce and financial institutions is one that is very much blurred within the States, within the class of institutions and the international scene, it is very much blurred. So the weakest link of the chain in terms of commerce and what is lacking in terms of the Internet and the electronic transmission are very much integrated in terms of what is going to happen. So we can build a solid wall here, but it is going to be made of paper in other areas that are going to affect it so it is not going to protect the privacy. We would be misrepresenting that unless we have the type of cooperation and the type of harmonization in terms of privacy issues that are necessary because just the very use of these particular mediums to exchange and communicate and in fact to actually do legal transactions is very much going to undermine anything that we try to do here unless there is some consistency. So there is plenty for everyone to do, including the regulators at the table, that deal with financial institutions and the FTC and of course in cooperation with our trading allies.

Madam Chairwoman, I have overrun my time. I did want you to know that I was criticizing the FTC for their lack of action in this part, Mr. Pitofsky, coming from a little different view than the minority views that you have.

Mr. PITOFSKY. Very briefly.

Chairwoman ROUKEMA. I will give Mr. Pitofsky a moment to respond.

Mr. PITOFSKY. I wonder whether it is fair—I agree with your essential point, that everybody is entitled to a certain minimum, the only question is how to get there. Lack of action by the FTC, I think we have been out front on this issue for three years now. We were the first one to do a study on how much privacy disclosure there is on the Internet. We brought cases in this area time and time again. The issue is not lack of action, the issue is whether the better way to get there is through, in this area, self-regulation as opposed to legislation at this time.

Chairwoman ROUKEMA. Thank you.

Mr. Royce from California.

Mr. ROYCE. Thank you, Madam Chairwoman.

I would like to get the perspective of the Board of Governors of the Federal Reserve, Mr. Gramlich, who is with us on that very question, on the question of what the principal problems will be in terms of privacy protection as banks begin to offer more and more of their services over the Internet and the definition of traditional banking products becomes blurred. We see an exponential increase here with Internet activity, and those were considered historically as non-financial, but with this evolution we see these becoming quasi-financial. What do you see the privacy problems are here?

Mr. GRAMLICH. Well, this is I think what makes this whole issue so hard. The definition of banks is evolving. On the issue that we are just talking about, sharing information among affiliates, as the definition of banks and let's say insurance companies or brokerage firms blurs, it may be harder and harder to know what is an affiliate. More and more activities may be done as departments of the bank.

So I think the whole question of how you make some of these important definitions is in play here. We are not taking a strong position on a lot of these issues, so I don't want to be anti-privacy or tilt the development of H.R. 10 in any way. It is just that these questions are complicated. They are evolving. It is very difficult to impose a level playing field, if you will, in this area.

So the subcommittee has to exercise a good bit of caution. That is really my only point. There are a number of legal aspects of this. I am not a lawyer, but we can certainly offer our help to the subcommittee in trying to sort of tiptoe around some of these complications.

Mr. ROYCE. Thank you. I would also want to ask the Chairman of the Federal Trade Commission a question.

That has to do, Mr. Pitofsky, with the EU decision that the United States law does not provide adequate privacy data protection consistent with their European Union privacy directive. Could you give us the reasons for the determination and the status of the negotiations that the Commerce Department is having with the European Union over this issue?

Mr. PITOFSKY. I really cannot. We have not been parties to that negotiation. I know that they have been complicated and difficult for quite a long time, and whether or not the European Union will eventually come around to the view that the United States protection for privacy is comparable to theirs and adequate, I just don't know. I am not really a party to those negotiations.

Mr. ROYCE. What would the ramifications be if we passed legislation and ended up at odds? Tell me what the ramifications would be?

Mr. GENSLER. Bob, on behalf of the Administration, as we are working very closely with the Commerce Department, the European Union directive lays out various privacy protections which they believe, the European Union believes, go further and do capture these concepts of notice and choice, access and other affirmative privacy protections.

The talks continue at this time, and I think that no finding has been made as of this time, but talks continue and they have been active and ongoing.



Mr. ROYCE. Was Britain in accord with those changes that the EU was making?

Mr. GENSLER. I believe so. It is part of the European Union, is part of those deliberations within the EU directly.

Mr. ROYCE. So there is solidarity among the European Union, and the United States is the odd-man-out at this point?

Mr. GENSLER. As I said, the talks continue. There has been a dialogue. There was some sharing in dialogue as to whether there may be some safe harbors—that the U.S. financial services firms could have safe harbors around notice and choice and access that are sometimes similar to what we are talking about today and sometimes actually go a bit further, and that if American firms comply with those safe harbors, the Europeans would find that we were in compliance. Those talks are ongoing and active.

Mr. ROYCE. Thank you, Gary. Thank you, Madam Chairwoman. Chairwoman ROUKEMA. Thank you.

Mr. Inslee.

Mr. INSLEE. Thank you. Just a general question, one of the panelists suggested where we all are headed and we all want to end up in the same place, and not to be the wet blanket, but I am not sure that is true. The reason is it is my perception that the industry, or at least some of the larger institutions, have a clear and manifested desire and goal to use affiliates, to use private financial information, to use it to mine prospects for marketing purposes, and they are very jealous of their ability to do that and they want to retain the ability to do that.

The reason that I have that perception or fear is that as we were drafting and working on trying to deal with this issue, I continue to solicit the industry for ways that we could write something to protect consumers' rights not to have their personal information mined for marketing purposes, and still allow banks to do some of the other things that they have to do, prevent fraud, allow checks to clear, and so forth.

Despite an effort to do that, I never got a specific proposal from the industry on how to do that. Instead I got a rather conscious decision, hey, we want to do this. The question is: Is my perception accurate, and were you ever involved in discussions, any of you, with the industry about how to draft a bill that would in fact meet the bank's legitimate needs to share information for some purposes and meet consumers' needs to be able to prevent that sharing for marketing purposes? Have you ever had proposals from the industry on how to do that?

Mr. GENSLER. Congressman, we believe that that balance can be found in statute, that exceptions, as we talked about in testimony, can be found. As Governor Gramlich said, maybe there are some additional exceptions necessary in affiliate situations, particularly as it relates to a consolidated account statement, that might be appropriate.

We have found some hesitancy, as you have noted in the industry group, but we think that it can be found, and with the leadership of Congress and the President hopefully we can move forward and find that right balance.

Mr. INSLEE. Was there ever—from any of the panelists' knowledge, did the industry ever make a proposal about how to do that

that was somehow rejected by the Administration? Has there ever been a proposal about how to reach that balance from the industry that you are aware of?

Mr. GENSLER. Not that I am aware of at the Administration. Around the Fair Credit Reporting Act, we have found that affiliate opt-out can work. I would also take note of another Act that Congress wrestled with a number of years ago, the Telecommunications Act that deregulated significantly that industry—not at all dissimilar from the actions of this subcommittee and this House on banking and insurance and securities. Incorporated in that Act is privacy protection as it relates to your telephone records. There is clear notice and consent on affiliate sharing of your telephone records. That had to be grappled with and handled sensitively, and have various exceptions in that context.

So I think industry can do this, and Congress has wrestled with it with a number of acts—in the cable area, the Department of Motor Vehicle Act a few years ago—as this subcommittee is wrestling with this now on this industry.

Mr. HAWKE. At the risk of belaboring a point, there is nothing inherent in the concept of affiliation that is likely to give consumers any greater sense of confidence that sharing with affiliates is going to be less of a threat to them than sharing with non-affiliates. The definition of affiliates that presumably would be used here relates to 25 percent common stock ownership. So you theoretically could have two companies whose only relationship is that one has a 25 percent stock holding in the other, and they would be deemed affiliates, and information could be shared without giving an opt-out even though the affiliate did not have any particular incentive to protect the bank's fundamental relationship with its customer that we are so concerned about.

Mr. INSLEE. A quick question. My perception is that the American public has absolutely no clue what has been going on in this marketing situation in that when these news reports hit it really was a bombshell, at least in my district, on people's perception. And I believe, and I am going to ask you if you share my belief, if, in fact, the CEOs of major banks called their consumers and said "We are going to do computer profiling of you, and we are going to find out if you have some cash, and then I am going to tell my affiliate to call you at 6:00 at night and try to sell you hotstock.com stock because we think you need it." I believe there would be a very high percentage of people who would opt-out with vigorous language to the CEO, and I wonder if you share my perception?

Mr. HAWKE. One of the problems that we encountered in connection with the telemarketing episode was that the telemarketers were not indicating that they had information from a bank. They had customer account numbers or access to customer account numbers, but it wasn't until the customer saw charges appear on their bank statement or credit card statement that they realized that there must have been a connection. At the time of the contact, no bank was identified.

Mr. INSLEE. Thank you.

Chairwoman ROUKEMA. Thank you, Mr. Inslee.

Mr. Bentsen.

Mr. BENTSEN. At the outset, I want to publicly thank Mr. Hawke and Mr. Pitofsky as well as Ms. Nazareth. I recently had some public hearings in my district on fraud prevention among the elderly and Sam Golden and Craig Stone from the Comptroller's Office were there and did a great job. Mr. Pitofsky, Jim Elliot from your Dallas office and Andrea Foster from your Atlanta office came and did a very good job, and Harold Degenhardt, who is the Regional Administrator of the SEC, came down as well. There were also people from the FDIC and OTS, and at the appropriate time I will publicly thank them. I was surprised at the quick reaction I got from the financial regulators to my request, and very appreciative.

I have a number of questions. Governor Gramlich, you raise a point in the broad sense that the Congress needs to think about, which is why are we doing H.R. 10 in the first place, if we are creating a new bank charter model that allows for additional powers, but we are trying to keep them somewhat out of the bank. We are not looking to try to create a structure that is the sum of the parts of the revenues. You might as well have a holding company that has a widget company and a ranch and something else and not have any synergy among it, and we will see if that works versus some other. We are trying to create a new bank model that meets the current demand in the marketplace and creates some synergies that are there. Consumer privacy notwithstanding, I think we should think long and hard about that before we take some strong positions, which I think the Administration has taken today without really thinking them through, and I regret to say that because I have the greatest respect for all of you on this.

The questions that I would like to get answers to, Mr. Hawke, you talked about an affiliate in the context of the Bank Holding Company Act, 25 percent joint stock ownership. Would you have the same viewpoint toward a wholly owned subsidiary of a bank; say if you had an operating bank subsidiary structure, would you treat that the same as an affiliate under the current definition of a bank holding company?

Second of all, under the Fair Credit Reporting Act, if I read your testimony correctly, transaction and experience information may be shared with affiliates and is not subject to an opt-out or is it subject to an opt-out because the way that I read it, it is not subject to an opt-out and other personal information is, and should we apply that same standard in the context of H.R. 10? Functionally, can you have an opt-out with respect to information sharing that doesn't require subsequent opt-in, and I think Ms. Nazareth mentioned this point on stock clearing and things such as that. I don't know, but is there a situation that would be out there where you would have an opt-out and then in order to make a transaction work you have to come back and say gee, you opted-out and now you have to opt-in and how does that work? It may just be a functional problem that exists there. Is there anything in H.R. 10 or in current law which in some way shields liability to the bank for misuse of private consumer information?

Mr. HAWKE. Let me answer the first question. If Congress in its wisdom were to adopt the version of H.R. 10 passed by the House, we would be only too happy to apply an opt-out from information sharing with operating subsidiaries.

Mr. GENSLER. Congressman Bentsen, let me answer your broader question because I think it is a very good question and a challenging one. I think the Administration supports financial modernization and there are many benefits to consumers and to the markets of financial modernization.

The efficiencies that come with consolidation, potential industry consolidation, we think are broader than just in the area of cross marketing. There are many efficiencies in providing service, there are many benefits of mergers that come with having geographic diversity or product diversity.

We do also think that the benefits of cross marketing still would exist even if there were notice and choice. As has been pointed out, many consumers would still decide to let the cross marketing occur, and it would be only some who would decide not to through an opt-out.

What we think is important is to notify consumers how information is shared, and then recognize the diversity of the American people. Some would value their privacy protection above those benefits.

At the same time, we are supportive of a series of exceptions so that transactions can occur, so that many of the benefits can occur. But as it relates to that which is profiling the individual and his lifestyle, we think that we should recognize the diversity of Americans and allow Americans the option to choose to opt-out and allow financial institutions to gain the great benefits of consolidation that exist.

Mr. BENTSEN. With respect to fair credit reporting?

Mr. GENSLER. I'm sorry, your question on fair credit reporting was whether today there is notice and opt-out for the affiliate for the credit report. As I understand it, there is. There is currently not for transactional experience data, and we are suggesting complementing that and adding transactional.

Mr. BENTSEN. So you would expand fair credit reporting?

Mr. GENSLER. No. Again I don't know if there is a technical question with regard to that. Through H.R. 10, as you have complemented privacy protections for third parties, we would complement it for the affiliates. I don't know if the vehicle would be specifically in the Fair Credit Reporting Act, if that was your more technical question.

Mr. BENTSEN. And legal liability?

Mr. GENSLER. The question on legal liability, if I can have a moment just to see if anyone—could you repeat it?

Mr. ROYCE. [Presiding.] Why don't you repeat the question.

Mr. BENTSEN. Is there anything in current law or H.R. 10 that would shield liability to the bank or the provider from the consumer for the misuse of private financial data? Are we creating any safe harbor?

Mr. HAWKE. The first question is whether there is any damage to consumers. There is a whole body of common law that has recognized rights of action by customers against banks when confidential information has been used in a way that causes injury to the customer.

Mr. ROYCE. But Mr. Hawke, Mr. Bentsen's question, is there some precedents in the legislation, H.R. 10, which puts in a safe harbor or in some way overturns common law in that regard?

Mr. HAWKE. I am not aware of anything in H.R. 10 that affects that.

Mr. GENSLER. With the benefit of terrific staff work, we are not aware of any preclusion of liability in H.R. 10. We are not aware of any additions in H.R. 10, and we have not taken a position on private right of action. We have just said there should be a regulatory authority to enforce the provisions of H.R. 10.

Chairwoman ROUKEMA. [Presiding.] Thank you.

Mr. Gonzalez of Texas.

Mr. GONZALEZ. Thank you very much. The question is more directed to Mr. Gensler than to anyone else. However, if anyone else has an opinion, if you would please address the question.

Under the statutory scheme that you describe as far as maybe addressing certain problems, exempting certain people, things that we always call "exceptions," if we address these exceptions legislatively, the question is would we be able to respond on a timely basis as the marketplace changes and technology changes. The legislative process has never been characterized as timely, especially with the speed of change in today's marketplace. Is there any other way to address it other than through "exceptions" language?

Mr. GENSLER. I think, Congressman, you raise a very good point. What we anticipate and suggest is that statutorily you provide for a series of exceptions which we believe can be appropriately drafted. Drafted in a narrow sense with a clear prohibition on reuse. If there is an exception, you don't want to have a large loophole. Then provide for regulatory authority through the customary public comment process to write rules and to enforce those rules going forward. So there would be some flexibility around the regulatory process with some clear, narrow exceptions as this subcommittee and the House work on H.R. 10.

Mr. GONZALEZ. Anyone else?

Mr. REIDER. Just a brief comment. As I commented in my prepared remarks this morning, as a State regulator and part of the NAIC, we constantly monitor what we feel are concerns on the part of the consumer, and we go out and do an on-site review of a company, and if we see any abuse, that can result in a penalty or a recommendation of a regulation or statute to protect that consumer.

Let me give you an example. In the State of Connecticut we have the Privacy Act, and in this last legislative session there was concern over medical privacy. So the law was changed so that information cannot be shared in any way, shape or form, even among affiliates without express permission of the person.

I do agree that we pretty much all come from the same place here and that is we have that responsibility, but it is a moving target. We have done some work with the Federal people on the Citi-Travelers situation, and we are prepared to work closely together to monitor what occurs in the coming months.

If you look at affiliates today, that may mean one thing. And in a conglomeration, it may mean something different. And as that unfolds, we are going to have to see if there is abuse.

There was also mention of encouragement of the industry to police themselves. The American people may not understand all of the specifics, but I can assure you being close to the home base, and as your offices know from contact that the American people are concerned and want to be sure that we approach this in a very balanced fashion.

Chairwoman ROUKEMA. Thank you.

I believe that Mr. Sandlin of Texas is next in order.

Mr. SANDLIN. Thank you, Madam Chairwoman. I have no questions right now.

Chairwoman ROUKEMA. Ms. Mahoney.

Mrs. MALONEY. It is Maloney.

Chairwoman ROUKEMA. I apologize. I know who you are.

Mrs. MALONEY. I would like to follow up with the comments, I guess, that was the State regulator, George Reider.

Do you think that Federal law should be a floor and that tougher State laws should remain regarding medical and financial privacy?

Mr. REIDER. Let me comment on this specific matter. The NAIC has deep concern, and we have expressed our thoughts on H.R. 10 and have attempted to work with others. We have not taken a specific opinion on privacy. As a practical standpoint, we do not believe in the preemption of State laws. Under H.R. 10, and we strongly support the fact that there should be financial services modernization, but we have to be certain that consumers are protected, and in H.R. 10 it states that the State regulators shall have the authority to regulate the business of insurance, but conditioned on Section 104. I am not here to make a statement other than to say as you are looking to protect privacy and the States already have laws protecting consumer privacy, as I shared with you the recent change in the legislature, I don't think that you want to do anything to disturb those State laws.

Again, I think that it is important as you are changing the playing field that we be sensitive to this particular matter. But we believe that we should work in a cooperative way, and I can say clearly that we do not believe in State pre-emption.

Mrs. MALONEY. Are you aware of any State laws that would be in jeopardy of being pre-empted with regard to affiliate sharing?

Mr. REIDER. We will review that legislation and review what is said here. When it refers back to Section 104 we do have a concern that there is some pre-emption, and we would want to be sure to protect people's privacy.

Mrs. MALONEY. I would like to ask Governor—

Mr. GENSLER. Just on that, I did want to try to answer your question.

There are numerous State privacy laws with regard to medical privacy that, it is the Administration's belief, the provisions as currently incorporated in H.R. 10 would run the risk of pre-empting; and the Administration is very concerned about allowing H.R. 10 to pre-empt those, in some cases, stronger State laws.

With regard to financial privacy, while we think it might be appropriate to clarify that on financial privacy, H.R. 10 does not pre-empt State laws. We believe it has been written in such a way that it does not pre-empt those laws.

Mrs. MALONEY. Thank you. Governor Gramlich.

Actually Mr. Reider, you mentioned earlier the talks with the Citi and Travelers negotiations on privacy and medical privacy protections. Do you think that H.R. 10 as drafted, helps, harms or maintains the principles that you have been striving for in that particular approval?

Mr. GRAMLICH. In medical privacy?

Mrs. MALONEY. Medical and financial privacy. All privacy.

Mr. GRAMLICH. Well, in financial privacy I think the testimony said on balance it does, but there are differences because the Fair Credit Reporting Act, as you have heard, already applies to affiliates, though to a narrower type of information. If H.R. 10 were changed in the way that the Administration wanted it, then it would clearly strengthen privacy. I think there is no question there.

So I think on balance since it applies to a broader set of information, that there would be strengthening.

On the medical privacy, we are a central bank. I don't want to get into that issue. We did mention in the testimony one example, but it was just an example to show how consumers value privacy. I meant to use that as an example, not to wade into the whole question of medical privacy.

Mrs. MALONEY. If we are going to be limiting sharing for purposes of marketing, I would like to ask any or all members how would you define marketing and are there other secondary uses of information that might not be covered by this?

Mr. GENSLER. The approach for some of the reasons that you have just raised, the approach that the Administration has suggested is that consumers get clear notice and choice and that they be allowed some exceptions, but the exceptions would sort of work down. So rather than saying it is prohibited or there must be choice for marketing, it would be that there is choice for all of the uses of this private information, and yet here are the exceptions, as H.R. 10 did in eight categories, here are the exceptions where that choice would not be allowed to stop that sharing, but for some of the reasons that you just raised in your question.

Mr. REIDER. I would like to say when I spoke of the change in the law regarding personal medical information, that was not specific to the Travelers by any means. That was a more general comment.

Chairwoman ROUKEMA. I might say that you have raised an important question with respect to whether or not these State laws are preempted. My position is that we will have to work on this issue and see how it can be addressed in conference. But my interpretation, or at least our staff interpretation, is that the State laws are not preempted. There may be some need for clarification on this point. I do not believe that was the intention. I would be happy to have any further comments or legal analysis that you have on this point. Please send it to us and address it to the Members of the subcommittee.

Mr. GENSLER. We would be glad to share that, particularly on the medical side.

Chairwoman ROUKEMA. Yes, I was referring to medical privacy.

Mr. VENTO. If there are exceptions in this bill, it has been implied that it is riddled with exceptions that are unnecessary, if you

come across those that are unnecessary, I would like you to point them out for me. I know that there is one for marketing which applies to small institutions that generally do their marketing through third parties which deals with some of the disparity referred to by Mr. Gensler. If that is the case, I would like to know about it.

We also have the debate about the unrelated service and products issue. That might be a way to deal with some of the marketing for affiliates to come back and look at it a different way. If it is just a matter of writing a software program, I would like to know that. Nobody has asked that question. But I think it probably involves more than that. The exceptions written in work for third parties, but they may not be workable for affiliates. So a lot revolves around these exceptions; and I think, Madam Chairwoman, you would agree that trying to understand that or get through that is important.

Chairwoman ROUKEMA. Yes. We have to understand that if we are going to avoid these so-called unintended consequences.

Mr. VENTO. Or the suggestion that the regulators will not regulate. I guess at some point we have to hand this over to you and ask you to make it work. So if you have problems with the exceptions or it is not clear—and one of the examples I was giving the staff, does disclosure and affirmative responsibility apply to all affiliates, and the language is not clear that it does. So clearly that needs to be established, that they are under the same presumption of responsibility that the initial institution is.

Chairwoman ROUKEMA. Mr. Watt, do you have questions? I am trying to conclude this panel before a vote. Of course you can never predict when that vote will occur.

Mr. WATT. I think I will pass in light of the fact that I had to be late coming in, and I don't want to duplicate any questions that have already been asked.

Chairwoman ROUKEMA. And of course under the rules, Mr. Watt, you are free to submit follow-up questions in writing to the panel. All right.

Yes, Mr. Dingell.

Mr. DINGELL. Madam Chairwoman, thank you for the privilege of joining the subcommittee and asking one quick question.

Your testimony emphasizes the President supports the right to say "no" as to financial privacy being shared and sold. Is this option the best response or should we be looking for something new? Or is the opt-out provisions in the statute the best we can do and maybe if the panel can respond to that.

Mr. GENSLER. I think the Administration supports all of the dramatic effort that the House has done, but sees the House provisions in H.R. 10 as a floor and not a ceiling. We think that it would be appropriate to have opt-out and choice provisions for affiliate sharing as well. And we have commented in our testimony regarding the importance for exceptions, but they need to be narrow exceptions. And then we have highlighted some of our concerns on medical privacy, as well and the concerns around the medical privacy provisions as provided in H.R. 10.

Mr. DINGELL. Does anyone else on the panel wish to respond to the question? Thank you, Madam Chairwoman.



Chairwoman ROUKEMA. Thank you. We express our extreme appreciation for all of your help here today. I know that this will be an ongoing process. We look forward to working closely with all the witnesses from the first panel for your advice.

Mr. Vento had to leave for a vote in the Resources Committee, and he advised me to go ahead and introduce the second panel and begin the testimony. We hope to get the second panel underway before we have a series of votes.

We are looking forward to the second panel with great anticipation. You have heard the first panel so you can understand that there are some issues here between regulators and groups representing the banking, securities, and insurance areas, as well as medical trade associations. There are some differences of opinion. I hope that they are not going to prove to be irreconcilable, but they do deserve a full hearing here. We welcome you all here today.

In the order in which you will be giving testimony, Mr. Richard Fischer is a Partner in the law firm of Morrison and Foerster. He is testifying on behalf of the American Bankers Association, the Consumers Bankers Association and the Financial Services Roundtable and Visa, U.S.A., Inc. That is quite an array of talent there.

Mr. FISCHER. It is quite a challenge.

Chairwoman ROUKEMA. The second witness will be Mr. Brandon Becker, who is also a partner with a law firm, Wilmer, Cutler & Pickering. Mr. Becker is testifying on behalf of the Securities Industry Association, SIA.

The third witness is Roberta Meyer, Senior Counsel, Consumer Affairs Unit of the American Council of Life Insurance. Ms. Meyer is representing the life and health insurance industry here today.

The fourth witness is Mr. Matthew Fink, President of the Investment Company Institute. Mr. Fink is representing the trade association for the mutual fund industry.

The fifth witness is Dr. Donald Palmisano. Dr. Palmisano is a trustee of the American Medical Association and is speaking on their behalf today.

Our final witness is Dr. Richard Harding, who is Vice President of the American Psychiatric Association.

Just to alert our final two panelists, I cannot resist this. I use this line all the time as part of my confessional. I am married to a doctor and I worked his way through medical school. The confessional part of this is he and others have accused me ever since of practicing medicine without a license. I am just putting you on the alert. I have some firm beliefs on medical ethics and the practice of medicine.

Thank you very much.

Mr. Fischer.

**STATEMENT OF L. RICHARD FISCHER, PARTNER, MORRISON AND FOERSTER, ON BEHALF OF THE AMERICAN BANKERS ASSOCIATION, CONSUMER BANKERS ASSOCIATION, FINANCIAL SERVICES ROUNDTABLE, AND VISA U.S.A., INC.**

Mr. FISCHER. Madam Chairwoman and subcommittee Members, my name is Rick Fischer. I have worked on privacy issues for nearly 30 years. I appear today on behalf of the American Bankers As-

sociation, the Consumer Bankers Association, the Financial Services Roundtable and Visa U.S.A.

These past two days you have heard much about financial privacy. The testimony shows that privacy is very complex. Because this is the last panel, I will avoid many of the issues that have already been covered by others, such as the industry's history of protecting privacy and the many laws that already deal with the subject. They are discussed in my written statement.

The organizations I represent here today have been active on privacy issues for years, and they have supported privacy legislation, when appropriate, including recent congressional efforts to address identity theft and pretext calling. I first appeared before this subcommittee in 1978 to support passage of the Financial Privacy Act to restrict Government access to bank customer records.

Nevertheless, the importance of information to the American economy in general cannot be overstated. Many experts, including Federal Reserve Chairman Greenspan, credit the strength of U.S. economy today largely to the availability of information, and it is particularly important to financial institutions. It is critical, for example, to a bank's ability to control risk and combat fraud.

It also enables banks to improve services in countless ways that benefit consumers. Information sharing allows banks to offer one stop shopping. A customer can through one monthly statement or through telephone calls make decisions about a checking account, mortgage loan, and other services from a bank and its affiliates. Information sharing also is key to the secondary mortgage market and its lower interest rates. It also allows a bank to offer higher savings rates or lower loan rates to customers of its affiliates.

These are examples of information shared for marketing purposes—an appropriate use of information which directly benefits consumers. More is set forth in the written testimony.

In fact, as Governor Gramlich pointed out this morning, one of the principal benefits of H.R. 10 is that consumers will be provided with greater choices and opportunities from banks, and banks will be able to broaden their relationships with customers. Thus, further redistributions on the flow of information could have unintended effects on the U.S. economy, consumers and banks alike. Such restrictions would harm consumers by reducing the availability of products and services consumers demand today. New sharing restrictions also could stifle the development of new products and services.

With this in mind, I want to make three points about the privacy provisions of H.R. 10. First, we believe that clarifications are necessary to avoid significant unintended effects. I think earlier testimony makes this quite clear of the need for those clarifications. For instance, H.R. 10 could threaten popular programs that provide frequent flyer miles, gas rebates and other benefits to consumers. We have also heard this morning questions about competition between large and small financial institutions. I don't believe that the legislation was intended to create those problems. I think clarifications would solve them.

Second, as you have heard, privacy is a complex issue. Every single member on the prior panel talked about the complexity of this issue. As Governor Gramlich and Chairman Pitofsky have said, en-

acting new privacy legislation requires a careful balancing effort. This is especially true in a competitive industry like banking. No bank could survive with a reputation for indifference about customer confidentiality. I think the actions and reactions on the West Coast demonstrate that the market works in this regard.

Third, as the panel of experts said yesterday, if Congress enacts the H.R. 10 privacy provisions, they should be the uniform law of the land so that the same requirements apply to all financial institutions, and the same protections are given to all consumers across the country. In the meantime, we look forward to working further with the Congress and bank regulators on privacy matters. For example, we would welcome the opportunity to undertake joint Government-private sector efforts to further educate consumers about privacy issues.

Thank you. I would be happy to answer any questions.

[The prepared statement of L. Richard Fischer can be found on page 474 in the appendix.]

Chairwoman ROUKEMA. Thank you. There are going to be a series of votes on, but I believe we have time for Mr. Becker of the SIA to give his testimony. Mr. Becker, please.

**STATEMENT OF BRANDON BECKER, PARTNER, WILMER, CUTLER & PICKERING, ON BEHALF OF THE SECURITIES INDUSTRY ASSOCIATION**

Mr. BECKER. Madam Chairwoman and Members of the subcommittee, my name is Brandon Becker and I am a partner in the law firm of Wilmer, Cutler & Pickering. Today I am appearing on behalf of the Securities Industry Association. Madam Chairwoman, we commend you and other Members of the subcommittee for holding these hearings which fill an important gap in the record concerning financial modernization.

As you know, last June SIA called for hearings such as these when it stated its support for the House financial modernization legislation. Accordingly we very much appreciate your prompt consideration of these issues.

The most important point to underscore today is that the best and most dependable constraint on the misuse of customer information is the competitive marketplace. A firm that uses customer information in ways customers find objectionable quickly will lose investor confidence and market share as well.

Moreover, wholly apart from the privacy provisions of H.R. 10, consumers already enjoy legal protection against the misuse of their financial personal information. A broad set of common law principles, statutory provisions and administrative regulations impose on securities firms a duty to protect private information that customers entrust with them. Thus, it is important to recognize that Congress need not address in H.R. 10 all potential types of misuse of customer information in the financial services industry. Other safeguards do exist.

In the context of financial modernization legislation, however, SIA supports the privacy provisions of H.R. 10 because those provisions take a market-based approach for protecting consumer privacy. Instead of imposing a set of new one-size-fits-all regulatory burdens, the privacy provisions of H.R. 10 promote privacy by en-

hancing consumer choice and thereby bolstering the operation of competitive market forces.

Nevertheless, additional privacy regulation is unnecessary and could in fact be harmful to consumers. For example, restrictions on information sharing among affiliates would impose significant administrative costs on diversified financial services firms. An opt-out right that applies to the internal sharing of information among affiliates would effectively prohibit the use of shared computer systems and require firms to incur substantial development costs to develop and maintain stand-alone bank office systems for each of their affiliates leading to duplicative costs and inefficiency.

Accordingly, Congress should amend H.R. 10 to preempt State laws that might impose additional, more burdensome regulations. Several States are considering such proposals today. In today's national market for financial services, however, firms cannot reasonably comply with 50 different and sometimes conflicting standards for privacy protection. Thus the State that adopts the most restrictive privacy regulations will set the policy for the Nation, because national financial services firms will have to conform their nationwide operations to that State's regulations.

Congress should not let individual States override its judgment that with H.R. 10's comprehensive information disclosure provisions in place, further privacy regulations are unnecessary. Although the SIA supports the privacy provisions in H.R. 10 as part of Congress's financial modernization initiative, two of its specific provisions need modification.

First, the language in Section 501 describing the congressional purpose behind the privacy provisions has the potential to be misconstrued as providing a basis for a private cause of action under State common or statutory law.

Second, the language in Section 503 requiring annual notification about privacy policies is unduly burdensome and unnecessary. This provision would appear to require a firm to make annual privacy disclosures even to customers that are inactive and that do not otherwise receive any regular notices from the firm. Congress should modify or eliminate this annual disclosure requirement.

Finally, SIA believes that it's crucial that Congress not alter the exceptions in the legislation that are carefully tailored to ensure the disclosure and opt-out provisions do not impede standard and appropriate industry practices.

In conclusion, I would again like to thank the subcommittee and Madam Chairwoman on behalf of the SIA for providing this important opportunity to share our views on the privacy provisions of H.R. 10. SIA believes that the prompt enactment of financial services modernization is essential for the Nation's growth and the enhancement of consumer services. Within that overall context of reform, SIA believes that notwithstanding the existing protections for consumer privacy interests, the H.R. 10 privacy provisions are an acceptable way forward to address both business concerns and consumer expectations.

Thank you again for this opportunity. I welcome any questions. [The prepared statement of Brandon Becker can be found on page 493 in the appendix.]

Chairwoman ROUKEMA. I thank you, Mr. Becker.

I think this is an appropriate time for us to break now. We are going to have a fifteen-minute vote and two ten-minute votes. I'm sorry, it will be three five-minute votes in succession. We should be back here in hopefully 25 minutes to continue this hearing. Hopefully we will be able to gather more Members here at that time for the rest of the hearing. The subcommittee hearing will stand in recess.

Thank you.

[Recess.]

Chairwoman ROUKEMA. The hearing will come to order.

Mr. Vento has left word that he will be back as soon as possible. He has advised me however, that given the voting schedule that is in progress today, that we begin without him. Of course you do know that all of your testimony will be made a part of the official record. Many Members who cannot be here will be reviewing the official record later. I hope that all witnesses understand that and it is not diminishing the value of your testimony or its impact.

I would also note for the record that the comments of Mr. Fischer have been noted by MasterCard, which associates itself with the testimony that Mr. Fischer has given. Under the rules of the committee, with unanimous consent, their written testimony will be submitted for the official record.

[The information referred to can be found on page 546 in the appendix.]

Mr. FISCHER. Thank you, Madam Chairwoman.

Chairwoman ROUKEMA. Thank you.

And with that I would like to recognize Ms. Meyer of the American Council of Life Insurance.

**STATEMENT OF ROBERTA B. MEYER, SENIOR COUNSEL, CONSUMER AFFAIRS UNIT, AMERICAN COUNCIL OF LIFE INSURANCE**

Ms. MEYER. Thank you. The ACLI wishes to thank you for holding this hearing, and for taking the lead on these emerging privacy issues. We appreciate being given the opportunity to present our views on these issues which are critically important to ACLI member companies, as well as to their customers. The very nature of the life disability income and long-term care insurance business involves personal and confidential relationships between insurers and their policyholders, but in order to do business insurers must be able to obtain, use and share their customers' personal information to perform traditional, legitimate insurance business functions. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers.

The ACLI companies also believe that the sharing of information with third parties and with affiliates is often the only way that customers can receive the level of service, the efficiency and the product choice that they demand, both in the existing marketplace and in the marketplace that will be created upon passage of H.R. 10. Insurers are fully aware of the unique position of responsibility that they have regarding an individual's personal medical and financial information. ACLI policy on privacy has been to long sup-

port the NAIC Insurance Information and Privacy Model Act which has been enacted in nineteen States across the country.

It is noteworthy that many, if not most, of our member companies that do business in any of the States that have enacted this law actually adhere to it across the country. While insurers are constantly concerned with protecting the confidentiality of their customers' personal information, in order for them to do business, they must share such information to perform traditional legitimate insurance business functions, to underwrite the applications of prospective customers, to administer and service existing contracts, to perform related or service functions or even to deliver a policy through an agent who is paid by, but may not be an employee of, the company. Insurers must also disclose personal information in order to comply with regulatory or legal mandates or in furtherance of certain public policy goals such as to detect or deter fraud.

It is also necessary for insurers to share information in connection with various ordinary business transactions like reinsurance transactions or in connection with mergers and acquisitions.

In our written testimony we did go into great detail with respect to the number of situations in which insurers must share information in order to best serve our customers. We tend to think of insurance as a product that is provided by a single business enterprise, but in reality insurers often use affiliate or unaffiliated third parties to perform essential and core business functions that are related to individual insurance policies.

They also use affiliates and third parties to perform functions not necessarily related to an individual policy, but related to the servicing and administration of insurance products generally.

I want to comment briefly on the medical privacy provisions in H.R. 10. The insurance industry recognizes that this language is not intended to be a final solution and that more comprehensive legislation is needed. It is noteworthy that the language of the medical privacy provisions themselves actually provide that the language is designed to sunset when an omnibus bill is enacted as required under HIPAA. While we believe that these provisions are worthwhile we do suggest that they should not be an impediment to enactment of H.R. 10.

With respect to the financial privacy provisions, we believe that the ultimate effectiveness of these provisions will not be known for some time and may be determined in large part by the regulations that are eventually promulgated. We do believe, however, that they are reflective of a conscious effort to balance consumers' legitimate privacy concerns with equally important consumer demands for convenient, prompt and efficient service and innovative products.

Importantly from our perspective, we believe that the language would also permit the sharing of information to the extent necessary to accomplish appropriate and traditional business insurance functions as well as for us to pass on to our customers the potential benefits and opportunities connected with the ability to affiliate as permitted under H.R. 10.

We do believe that the measured approach taken by the House on H.R. 10 was well advised, and will protect consumers without eliminating the incentive of the financial service industries to continue their pursuit of financial services modernization.

The ACLI appreciates having had the opportunity to present our views and we look forward to working with the subcommittee as it deliberates on these important issues.

We particularly appreciate the sentiment expressed in your opening remarks yesterday, Madam Chairwoman, that the need to address the privacy issue in a thoughtful and comprehensive manner could proceed on a separate track from H.R. 10.

[The prepared statement of Roberta B. Meyer can be found on page 505 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Mr. Fink of the Investment Company Institute.

#### **STATEMENT OF MATTHEW P. FINK, PRESIDENT, INVESTMENT COMPANY INSTITUTE**

Mr. FINK. Madam Chairwoman, Mr. Vento, and Members of the subcommittee, I am Matthew Fink, President of the Investment Company Institute, the national association of the mutual fund industry. The mutual fund industry has enjoyed steady success over the last sixty years, and the foundation of that success is the confidence of millions of individual shareholders. For that reason, our industry has always taken very seriously issues concerning the use and protection of our shareholders' personal financial information.

In fact over a year ago—before this subcommittee and other committees of Congress got heavily into this issue—we urged the National Association of Securities Dealers, a self-regulatory organization for securities firms and mutual funds, to adopt a rule governing the sharing of confidential customer information by NASD members.

Mutual funds have a very unique and rather complex business structure, and it is necessary to understand this structure when you look at issues concerning information sharing which are at the heart of privacy discussions.

Attached to my written testimony is a rather complicated chart that shows you the typical organization of a mutual fund company. The mutual fund itself is simply a pool of assets and does not have any employees of its own. Therefore, the fund's operations are conducted by a wide number of both affiliated and non-affiliated service providers. This includes the fund's adviser, which is the company that runs the fund and picks the stocks or bonds for the fund, the fund's principal underwriter, which is in charge of distributing the fund shares, the transfer agent, which keeps records of shareholder accounts, and the fund's custodian, which holds the fund's assets.

To allow a mutual fund to operate, it is essential that shareholder information flow unimpeded among the mutual fund and these various service providers. Information sharing must occur simply to maintain a shareholder's account: for example, to provide the shareholder and the Internal Revenue Service with tax information every year. Information also needs to be shared to properly service a shareholder's relationship with the entire mutual fund organization: for example, to advise the shareholder of the creation of a new fund that is available for purchase or to prepare consolidated account statements that give the shareholder information about all the different funds the shareholder is invested in.

I think it is fair to say that this type of information sharing is unlikely to give rise to the concerns over financial privacy because, as a practical matter, I think most of us, when we invest in a mutual fund, do not realize that it may be a series of five or ten separate affiliates, but look at the fund organization as a whole.

I think few, if any, shareholders would be concerned with the fact that as a technical and legalistic matter, each of the entities in the fund complex is a separate corporation. In contrast to this type of what I will call "harmless" information sharing among affiliates, I am not aware of any mutual fund organization that sells its shareholder personal information to unaffiliated third parties or that views the shareholder information as a source of additional revenue.

I cannot emphasize too strongly the importance of assuring that any legislation addressing financial privacy recognizes the unique structural characteristics of mutual funds. Standing back to be a bit philosophical, I think what you have been struggling for, as I heard the earlier panel and read the testimony yesterday, is a balance between two very important customer needs. One is to give customers, in our case mutual fund shareholders, control over their personal information and prevent use that they might consider objectionable, and second, ensuring that customers efficiently receive financial products and services. I have concluded that the privacy provisions in H.R. 10 as recently passed by the House effectively strike such a balance. They would require all financial institutions, including mutual funds, to disclose their policies to customers on sharing personal information. They also would permit customers to opt-out of any arrangements that involve sharing of information with unaffiliated entities for reasons not related to servicing customers. I think those provisions should be in the final bill.

Proposals that would impose additional restrictions on the sharing of information might very well diminish the range and quality of services that mutual funds provide to their customers. For example, if a mutual fund was required to allow its shareholders to opt-out of information sharing between the fund and these various service providers, funds simply might be unable to service the accounts as they have traditionally done. Because mutual funds operations are invariably carried out by third party and affiliated service providers, this problem of blocking or requiring an opt-out would be a very bad problem for mutual funds.

At the very minimum, if there was opt-out for information sharing among affiliates, fund organizations would have to develop and maintain systems that track opt-out information on an ongoing basis. In addition, they would have to institute procedures to train personnel on compliance, and the costs I think would be quite substantial and very difficult to justify—given what I call the "harmless" nature of this information sharing and the small number of people likely to opt-out.

There is one issue I would like to raise in conclusion, although I think H.R. 10 strikes about the right balance. There is one major problem that the subcommittee needs to be aware of, which other witnesses mentioned, and I gather there is a difference of opinion on the subcommittee; that is inconsistent State law requirements that could upset the balance. Such requirements would be very



burdensome for companies like mutual fund organizations that operate on a national basis.

And I might say, Madam Chairwoman, we lived with such a system for about fifty years. From 1940 until 1996, mutual funds, though heavily regulated under the Investment Company Act of 1940 by the Securities and Exchange Commission, also were subject to changing laws and regulations in the 50 States, and it was a tremendous nightmare that Congress rectified in 1996. I would hate to see a repetition of that problem in the privacy area.

Therefore, I would think that if there is final legislation to protect financial privacy, it should clearly override inconsistent State laws. Thank you.

[The prepared statement of Matthew P. Fink can be found on page 520 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Now, Dr. Palmisano of the American Medical Association.

**STATEMENT OF DR. DONALD J. PALMISANO, M.D., J.D., BOARD OF TRUSTEES, AMERICAN MEDICAL ASSOCIATION**

Dr. PALMISANO. Thank you and good afternoon. My name is Donald Palmisano. I am a general and vascular surgeon in New Orleans. I am also on the Executive Committee on the Board of Trustees of the American Medical Association. I would like to thank Chairwoman Roukema on behalf of the AMA for the invitation to talk with you today about the medical privacy issues in H.R. 10.

Quite frankly, physicians and patients are quite concerned that private medical records could be widely shared among affiliated entities under H.R. 10. I think it comes down to the fact that health insurers play a double role here. In their role in H.R. 10, insurers are financial services institutions that seek to benefit from affiliating with banks, mortgage companies, holding companies, brokers, dealers and other insurers. Yet in the context of the debate on comprehensive medical privacy legislation, insurers style themselves as providers, seeking only to improve the quality and efficiency of care for populations.

Well, which is it? Health insurers are privileged and it is a privilege to have access to our most personal medical information so they can pay claims for medical care. But when insurers function as financial services institutions, our medical record becomes more and more like an item of commerce, a consumer market profile. The AMA believes very strongly that health insurers should not be able to use the privileges of one role to exploit the opportunities of the other role.

Once the provisions of H.R. 10 tear down the current barriers that prevent affiliations among banks, security firms and insurers, nothing much prevents our personal medical information from being disseminated among any of these new affiliates and, while well intentioned, we do not believe that the medical privacy provisions in Section 351 of the bill cure this problem. So as I said before, we appreciate attention being focused on this issue.

So what will we do to help cure the problem? The AMA favors an explicit opt-in provision for medical information, we think the most prudent course is to modify H.R. 10 to completely prohibit the transfer of medical information, even among affiliates, without the

explicit consent of the individual. Use and redisclosure should be limited to what the individual knowingly and voluntarily consents to.

This position reflects AMA policy that as a general rule patients have the right to control disclosures of their personal medical information, with narrowly tailored exceptions for certain defined public benefits. As a doctor, I am constantly creating new records. These records serve as clinical tools to help in the diagnosis and treatment of my patients. When the record migrates from its primary purpose as a clinical tool, patient consent becomes even more important. These secondary issues are just not currently anticipated by patients and they need a constant process to inform them and give them a choice.

Financial institutions, including insurers, their affiliates, and any unaffiliated third parties, should all be required to affirmatively get an individual's consent to disclose their personally identifiable medical information. An opt-out provision just is not enough, even if it did apply to medical information disclosures under the terms of the bill, which it currently does not.

Two quick points I would like to make before concluding. First it is our understanding, from the Dear Colleague letters, that Dr. Ganske fully intends his medical privacy provisions to not preempt State laws, not now, not in the future. We agree and think it is essential to allow for protective State laws to remain in force. This would certainly be consistent with the preemption language in Title V of this bill.

Second, we are not arguing that H.R. 10 should become a vehicle for comprehensive medical privacy legislation. Still, if provisions are included at all, they should afford the full range of protections for medical information, at least as it would be shared and used in the financial services context. If Congress is unable to significantly improve these provisions, we would rather see the entire section struck than to pass into law so-called protections that allow personal medical information to flow freely in commerce without individual's knowledge or consent. It is not our preferred outcome but it is preferable to passing a version of H.R. 10 that codifies sweeping access to private medical information.

If you take one thing away today from my statement on behalf of the AMA let it be this: Information cannot be unshared. Once a financial institution has our medical information, it becomes a permanent part of our consumer profile and it doesn't matter what passes later or what might offer more protections. So if the Congress has to err at all in this matter, let it be on the side of protecting patients and their private medical information; not codifying financial institutions' desire to use that information for marketing purposes.

I thank you for listening to the AMA's concerns and I am happy to answer your questions. Thanks.

[The prepared statement of Dr. Donald J. Palmisano M.D. can be found on page 524 in the appendix.]

Chairwoman ROUKEMA. Thank you.

Dr. Harding of the American Psychiatric Association.

**STATEMENT OF DR. RICHARD K. HARDING, M.D., VICE CHAIRMAN, CLINICAL AFFAIRS, PROFESSOR OF NEUROPSYCHIATRY AND PEDIATRICS, UNIVERSITY OF SOUTH CAROLINA SCHOOL OF MEDICINE**

Dr. HARDING. Madam Chairwoman, I am Richard Harding, M.D., Vice Chairman of Clinical Affairs and Clinical Professor of Neuropsychiatry and Pediatrics at the University of South Carolina, and Vice President of the American Psychiatric Association, and serve on the National Committee on Vital and Health Statistics which was charged by Congress to make legislative recommendations on protecting the privacy of medical records.

The views I am presenting today are my views and those of the American Psychiatric Association and not the National Committee on Vital and Health Statistics necessarily.

First let me thank you, Madam Chairwoman, for your outstanding support for non-discriminatory insurance coverage of mental illness and for your overall leadership on mental health issues and, indeed, health issues in general and for your attention to the serious patient privacy concerns raised in reference to Section 351 of H.R. 10.

Because these provisions would overturn the principle of patient consent before disclosure of medical records, and may overturn certain State privacy laws, it represents a significant step backward for patient privacy. Moreover, since doctor-patient confidentiality is an essential element of effective medical treatment, these provisions will also have significant ramifications for the quality of health, and particularly mental health care in our country.

Without a very high level of patient privacy, many patients will be reluctant to seek needed health care and for making a full and frank disclosure of information needed for their treatment. For these and other reasons, over forty physician and patient groups, including the American Lung Association, American Academy of Family Physicians and two major unions oppose these provisions.

Although we have very significant concerns about Section 351, the sponsor of these provisions has stated that it is his intention not to preempt State privacy laws. He also expressed his general support for the principle of patient consent before the disclosure of medical records. These are two critically important principles that we strongly support. When combined with other changes I outline in my written testimony, these principles offer some hope of a positive resolution of this issue.

However, we do urge Members of the subcommittee to err on the side of caution and, indeed, of protecting privacy when considering these provisions. Just as the first rule of medicine is to do no harm, we hope the subcommittee will adopt the same approach on medical records privacy issues.

If the Congress permits extensive use and disclosure of patients' medical records without informed voluntary consent of patients in H.R. 10, it will be enormously difficult, if not impossible, to undo the damage later. At least if we do no harm, States' efforts to address this issue can continue.

The safest approach may be to delete the medical records provision of H.R. 10—that is, Section 351—and address the issue subsequently through comprehensive legislation.

Finally, it is critically important to recognize the difference between medical records privacy and financial privacy. If financial information is disclosed, it can be an embarrassment and in some cases cause a financial loss. But it is not overly difficult to recover from any personal discomfort and one can win compensation for his financial losses.

But medical record information can include information on heart disease, terminal illness, domestic violence and other women's issues, and psychiatric treatment including alcoholism. As the U.S. Supreme Court recognized in its *Jaffee vs. Redmond* decision in 1996, I believe, disclosures of this information can cause "personal disgrace as well as discrimination." These disclosures can jeopardize our careers, our friendships, and even our marriages.

And if such disclosures occur, there are truly few meaningful remedies. Seeking redress will simply lead to further dissemination of the highly private information that the patient wished to keep secret, nor can a financial settlement do much to compensate the individual for these highly personal losses. For all of these reasons, very tight restrictions on access as well as disclosure of medical records information is essential.

Thank you for inviting me to testify, and I look forward to working with the subcommittee on these issues.

[The prepared statement of Dr. Richard K. Harding M.D. can be found on page 534 in the appendix.]

Chairwoman ROUKEMA. Thank you.

This panel has given me additional problems, especially the last two who are testifying on behalf of the medical community. I stated my own biases in my introduction. I have a bit more understanding of your perspective, but I am afraid that we have an honest difference of opinion on the strategies here. I am speaking now with respect to medical privacy. There is no contradiction here concerning the absolute need to do no harm and to go on for more comprehensive medical privacy.

Dr. Ganske would be one of the first to admit that his provision, Section 351, was not intended to be comprehensive medical privacy legislation. He attempted to deal, to the extent possible, with the fact that we are now permitting financial institutions that include insurance companies and enter into affiliations with banks, securities firms and other institutions.

So I am really perplexed here as to what the strategy should be as we are dealing with this problem.

Let me ask the insurance industry and maybe the banker, Mr. Fischer, how you respond to this question or this potential for violation of an individual's medical privacy. How do you protect yourself against a lot of lawsuits as a matter of fact that could come about? How do you feel that the legislation before us is either inadequate or can be improved, recognizing the legitimate concerns that the medical community has raised?

Ms. Meyer, would you like to be the first and then Mr. Fischer if you would, please. This is a very complex issue and we have got to deal with it.

Ms. MEYER. Exactly. And for better or for worse, this information and our ability to obtain it and to use it and to share it to—to do

what customers come to us to do is essential to our business. So it is very important to us.

I think it is important to state too that we recognize that these confidentiality provisions are not intended to be the comprehensive approach to medical records privacy and agree that they, in fact, are a first step.

We think that they are appropriate and that they do require consent to disclose information that our member companies have generally gotten either directly from the individual or with the individual's authorization. And the only circumstances that we are permitted to disclose it without their consent are for basic insurance functions that they came to us to do in the first place. In other words, we need to disclose to underwriters their applications and to pay their claims.

Chairwoman ROUKEMA. Ms. Meyer, forgive me, but that is discretionary on your part. That is not statutory requirement, as I understand it. That is discretionary and/or someone's interpretation of regulation that you have just described, although it is the common industry practice that you have just described.

Ms. MEYER. The practices that I described are permitted under existing privacy laws that are enacted in the States across the country, and I believe by virtue of the fact that they either require an individual's consent to disclose information or you have to be performing a legitimate insurance function.

And in addition to which, I believe that is in line with what is being proposed under the H.R. 10 medical privacy provisions. Am I responding to—

Chairwoman ROUKEMA. I think so, but we will have to go over it in a little more detail at another time. Did you finish? I interrupted you. Did you make your point?

Ms. MEYER. Yes, I think that I had, thank you.

Chairwoman ROUKEMA. I want to give time to Mr. Fischer.

Mr. FISCHER. Yes, Madam Chairwoman, we have looked at this issue. We recognize that a special standard applies to medical information. We acknowledge the particular sensitivity with respect to medical information. We have been supportive of the efforts to protect that information. We have left, frankly, the details of that protection to people who are much closer to it and much more directly affected than we are.

None of the banks, individual banks that I have talked with, have any interest in receiving medical information. The reports suggesting that, I think, are simply not true as I have seen it. We have left the details, we have been supportive of the approach.

Chairwoman ROUKEMA. You say, then, that we should move to improve this section of the bill. Changes should be consistent with what the medical representatives have said, and consistent with what I believe was Dr. Ganske's original intention. This would move us beyond just this first phase of medical privacy and perhaps institute some further protections?

Mr. FISCHER. Madam Chairwoman, we do not say that. What we do say is that Congress has recognized that there is a very narrow need for payment cards and other payment devices to pay for the medical service. Our only interest is making sure that people can continue to pay for those services. Once you look at the privacy pro-

tection and the information beyond that, what we frankly have said is that it does make sense to protect it. The details of that protection really should be left to those that are closer to that industry.

Chairwoman ROUKEMA. Would the doctors want to respond?

Dr. Harding.

Dr. HARDING. I think it is important to keep separate the issue of medical privacy and financial privacy. And in addressing Section 351, which is medical privacy, it has consent and then a series of issues that would not require consent, and that is where we start getting uneasy, because in this thing there are things such as in Section 2, research projects don't require consent. Well, what is a research project? Is that marketing and so forth?

So that the issue becomes one of when consent is followed clearly, there is very little problem. But this section is almost entirely the exceptions to that consent.

Chairwoman ROUKEMA. Dr. Palmisano.

Dr. PALMISANO. Yes, Madam Chairwoman, I echo what the doctor has said. And we have found this to be a very complex area. The American Medical Association has studied this area and we came out with a complex report that was approved by a house of delegates in June 1998, and then they said go into more detail in some areas, and we did. We formed a task force.

So part of the past year we have been talking to experts all over the Nation and we gave an interim report at this meeting that just ended in June of this year and we have found that patients will not disclose information if they think this information is going to go laterally.

For instance they come in, I treat somebody, a young woman is in an auto accident and I am a surgeon and she comes to me with a laceration on the forehead and I suture that laceration up. And I have a medical record that goes back ten years, and there is some information that she elects not to share with anyone else, and I understand that and keep it confidential.

I get a request from the insurance company because of a blanket consent that she gave that says we have the right to inspect all the records and so on and so on. All they really need is information for the laceration: what I did, what the charges are for payment purposes, to make sure there is no fraud. They can look at her and see if she has had a laceration. But they want history about a depression, separation from her husband. They want the entire record. These are just some of the issues that we face.

We also have patients who call and say, "I have been contacted by some third party saying there is a new medication. Why do they know that I have diabetes? Why do they know that I have HIV?" That is the problem we are facing now and we are concerned that 351 as written, as my colleague has pointed out, the exceptions eat up this particular rule. And research is under intense debate as to what constitutes research. Marketing research? Research to enhance the company's profitability? What is research? So we don't believe that is the answer.

And at the appropriate time, I will give you three options that the American Medical Association recommends to fix this. I alluded somewhat to it.

Chairwoman ROUKEMA. Yes, please submit that to me. We don't have time to go into that now.

Is there any final statement that anyone wants to make on this subject before I turn to Mr. Vento?

Ms. Meyer.

Ms. MEYER. I think the ACLI would like to make the point that we recognize that this is a first step, that this is a very complicated issue, and as you all know, the Congress has been working on the issue of medical records privacy for years, and that in fact we are supportive of a comprehensive approach to this very difficult issue. So we know that, in fact, there are concerns and that this does involve hard stuff.

Chairwoman ROUKEMA. All right. As you probably know, or if you don't know you should know, this issue of medical privacy is very important to me. Last week the Commerce Committee initiated hearings on this subject which, of course, we will be following closely. I am sure you will be.

I don't think that negates the necessity for doing something in H.R. 10. That is my conviction in terms of the strategy. By a strategy, I mean at least making the opening, given what is going to be happening to the merger and acquisition of financial institutions under H.R. 10.

Thank you.

Mr. Vento.

Mr. VENTO. Thank you, Madam Chairwoman. I regret that I couldn't be here to personally listen to the testimony. But I do have before me—I was reading a letter that was sent to our colleague or Chairman in the Commerce Committee, signed by the AMA and a whole group of other health care groups. It is called the Consumer Coalition for Health Privacy, and in it it says, "We believe, however, that so far as H.R. 10 authorizes the sharing of information between affiliates, it is appropriate to address the medical privacy in this specific context. In particular, there needs to be a specific prohibition on sharing of medical information without notice and consent."

Well, we got that, number one. We got that in the bill, I assume. We had this in the bill, I might say, Chairman Leach and myself, before our colleague from Iowa, Mr. Ganske—Dr. Ganske—put it in. And this is very similar to what we actually had added in the bill in the Banking Committee. And what we are trying to do is prohibit the misuse of this information as we merge insurance securities and banking companies together. I mean, there are all sorts of devious things that can happen. Someone might have a life insurance policy and we might have someone come to him with a structured payout where they take and give him or her the money and then pick it up at the end. So there are all sorts of misuses of this that could occur in the context of this new type of affiliate structure.

So that is all we are trying to do. We understand there is a bigger picture here in terms of the Health and Human Services and there is a larger picture in terms of medical privacy which is being circumvented by the Internet and by, you know, the accumulation of records and the necessity of those records being in place and pharmacists and, you know, it potentially is a very much a concern.

But I related to the committee yesterday my own experience some 30 years ago as a State legislator when we couldn't even get the information from the insurance companies to actually do a bid to, actually provide for bids on health insurance on a group. They held the information and would not release it for anticompetitive purposes. And so there are some serious problems.

So I think that the insurance companies and some of the provisions that you were referring to are basically included, because there is, obviously, a sharing. It really requires us not just to know the needs on the patient side in terms of privacy, but also to understand the transactions and the necessity of information in terms of how insurance works. Which is, you know—we are all laymen, I am a layman in this particular area, but I think that participating in research projects to me means medical research. But even there, maybe there should be consent. I grant you that some folks would want to have some consent in terms of information, but I think in a general sense that that is not—I mean, even if it was understood to be medical research I think you could probably find those that made quite an argument that that is in the public interest.

Dr. Palmisano.

Dr. PALMISANO. Yes, sir, the example you gave, deidentified information could be used to serve that purpose in order to get a bid, and that is one of the things we concluded in our extensive research at the American Medical Association dealing with the experts. So we think that could be solved and we know that research includes more than just medical research. And when people do things with other people's information, you should have the patient's consent.

Mr. VENTO. Well, I don't think that that is necessary if it doesn't have the personal identifier on there and you are trying to use it for a competitive issue.

Dr. PALMISANO. If it is deidentified, we don't have a problem with deidentified.

Mr. VENTO. I think that has been blown out of proportion in my view, and most people from a commonsense standpoint, having something in this bill that bars the information and doesn't do any harm—if I could use the pejorative term that is used by the medical profession, "do no harm," here is to have something positive. And I hope that the good intentions and work of the Commerce Committee and the Health and Human Services materializes into something.

But meanwhile, I think we should have—we should be working to at least put some sort of barrier here that addresses the merger of companies. That is what we are interested in. We are not interested in taking over the jurisdiction of other committees or of the Health and Human Services Secretary in terms of writing the rules. We couldn't do it even if we took the time. Probably it is beyond us.

So I hope that that is understood. And I will certainly study your testimony for other nuances; and this letter to Chairman Bliley in which you obviously endorse that particular policy path, I will put in the record. That is my assessment of the letter in any case. Without objection, Madam Chairwoman.

Chairwoman ROUKEMA. So moved.



[The information referred to can be found on page 363 in the appendix.]

Mr. VENTO. Beyond that, the testimony of others, of course, raises questions with regards to privacy. And I think one of the questions that stuck out here to me is, Mr. Fischer, could you give me an example or two of how information sharing restrictions would harm consumers by restricting availability of products and services they might want or request based on what is in the bill?

Mr. FISCHER. I would be happy to do that. For example, it is not uncommon at all for a retailer to effectively outsource their entire credit operation. It is called private label credit cards and in a situation like that, the core relationship is with the retailer, but the information that relates to the fact that somebody has purchased school clothing, for example—

Mr. VENTO. Excuse me; the presumption that they have opted-out? Is that the presumption? That they have opted-out under the provisions of that statute?

Mr. FISCHER. It is that they have opted-out.

Mr. VENTO. That is your presumption in terms of making the statement.

Mr. FISCHER. Or that they simply don't understand and they have seen a lot of information about privacy and the concerns about privacy, and if in fact they are told that here is an opportunity to protect their privacy and they opt-out under those circumstances.

Mr. VENTO. The exception in the opt-out section of the bill does not cover that? My interpretation is that it may.

Mr. FISCHER. Well, that as we have said earlier, we believe that there are a lot of clarifications that really still should be made in terms of the H.R. 10 provisions. That is one of them, sir.

Mr. VENTO. Madam Chairwoman, I know Mr. Inslee, if he has to go, I will yield back. I just have one additional question I wanted to raise and that was the issue of in terms of affiliates. It has been pointed out that there is some disparity between affiliates and non-affiliated types of structures. I don't think anyone intended for subsidiaries not to be covered, but that is another debate. But I think the basic issue is if it is a non-holding company, a smaller bank, a smaller financial institution, that they suggest that there is a disparity here and that people or individuals don't expect affiliates to in fact share any of the information that the parent holding company might have or that they will share with the parent company, and that there is some sort of disparity.

One of the suggestions made was that what we are dealing with generally, that there is not as much of a problem, and I think that that is correct. There is not as much of a problem in terms of information sharing when we are dealing with—unless we are dealing with unrelated services and/or products. Unrelated services and products.

Could you comment on that with regards to your viewpoint of changing or opting-out with regards to unrelated services or products and the issue in terms of whether it is an affiliate or non-affiliate status of the institution.

Mr. FISCHER. In most situations if you are talking about sharing information between two affiliated financial services companies,

the type of entity that we are looking at here under H.R. 10, the services that these entities are providing are by definition financial services. In one case they may be deposit accounts, in another case it may be loans, in another case it may be insurance or mutual funds, as Mr. Fink described. But in each case they are really financial services products.

Some of the press reports in terms of use of information for non-financial products really does not arise except in very unusual circumstances in an affiliate sharing context. The market reaction to disclosure of information to third parties, particularly for tele-market purposes, non-financial products and services, I think is what got the reaction.

Mr. VENTO. I think it is the list exchange. How about the size issue or the holding company versus non-holding company issue?

Mr. FISCHER. I think there was no intention in the legislation—I am being presumptive, obviously, in saying this—to create a disparity between big institutions and small. The fact of the matter is that there are as many large institutions that rely as heavily on outsource and service organizations as small. The legislation does, in fact, have an exemption for processing and servicing. It has an exemption for a use of agents to market your products, financial products. It has another exception for two financial institutions that are not related sharing information to meet their common needs.

The combination of those exceptions, I would expect, would level that playing field, if you will, as between large and small. There is no question but that there are issues with respect to the exceptions across the boards in terms of clarity that needs to be addressed.

Mr. VENTO. Thank you, Madam Chairwoman. Thank you, Congressman Inslee.

Chairwoman ROUKEMA. Mr. Inslee, please.

Mr. INSLEE. Thank you. I wanted to see if we could reach some agreement on this here so I want to ask an easy question to start with. I want to give you a scenario and I would like your thoughts on whether it should be or should not be allowed.

Assume we have got a person, Emma Smith, and she opens a checking and savings account at her bank. And she reads some of these articles in the newspaper and what Congress is up to and so she writes a letter to her bank and it says, "Dear Friendly Bank, I care about my privacy. Do not share my account information with your affiliates for marketing purposes. Thank you very much, Emma Smith."

Her bank then, in its incredibly powerful computers, profiles her bank account on a daily basis and one day they discover that she has \$10,000 cash she just got from some unknown source. In fact she inherited it, and they think that this is a good opportunity to sell a product, so the bank—or actually its computer, due to pre-ordained software—sends that information to the bank's affiliated securities company or brokerage house with the information that Emma Smith has \$10,000 cash; just got it in; we believe she is a good target to market some of your good, new, hot IPOs or some hot stock.

The question I want to ask, I think it is a yes or no answer if you can give it to me: Should the affiliated company of the bank under that circumstance be able to ignore Emma Smith's specific direction to the bank and use her account information to try to market to her a stock? And I want to ask that to the first four folks, if you can give me a yes or no answer or thoughts in that regard.

Mr. FISCHER. They shouldn't be able to use that information under those circumstances.

Mr. BECKER. No, they shouldn't.

Ms. MEYER. That is an interesting question from our perspective. I guess if she has given a specific request not to use the information, they shouldn't be able to use it.

Mr. FINK. I would agree.

Chairwoman ROUKEMA. Would the gentleman yield?

Mr. INSLEE. Certainly.

Chairwoman ROUKEMA. Have you asked the question in the context of statutory authority or regulatory prohibition or are they just responding in terms of their own feelings, not in terms of whether or not it could be done under the law?

Mr. INSLEE. I will give them a chance to answer that.

Chairwoman ROUKEMA. All right. Thank you.

Mr. INSLEE. We have agreement, the five of us on the answer to that question, I think.

Now, if that is the case, is it not appropriate for the U.S. Congress to incorporate in our unanimous opinion in this regard and find a way to draft a provision that would prevent such activities with affiliates as well as third parties? And I would ask all four of you to take a stab at that answer.

Mr. FISCHER. I will start it all. I don't believe, respectfully, that that is a parallel situation. Most financial institutions, hopefully all, but at least most financial institutions today do honor a "do not call" and "do not mail" list.

In other words, if a customer says I don't want to hear from you except to receive my statements, they honor that. You heard from the direct marketing association yesterday, that is their rules. Most banks, or at least large banks, are members of the association, they follow those rules. Once you start going beyond that to something that really looks at notifications and opt-out, and similar rules are talking about something that is far more complex.

Mr. INSLEE. Did anybody want to say anything significantly different than that?

Mr. BECKER. Only to underscore that I think that setting up the factual predicate really blows by the fundamental question which is whether or not there should be a Federal requirement for what the marketplace is already doing. I don't think as a business matter, businesses who ignore their customers' preferences stay in business for long. That is what our testimony said. We did not endorse Federal legislation to mandate good business practice in this area because we think it is unnecessary and could lead to very significant costs for consumers.

Mr. FINK. I think Mr. Fischer answered it. Under current law, people can and do provide "do not call," and I think that is just an

example of it. I think the bill, as I understand it, goes further and does not allow sharing, which is a much more difficult bar.

Chairwoman ROUKEMA. In connection with that, if the gentleman would yield for just one moment.

Mr. INSLEE. Certainly.

Chairwoman ROUKEMA. I had this question that came back to me as Mr. Becker spoke. Those legal protections, as you said and Mr. Becker alluded to in his testimony, said they already exist. But they have not existed in the context of what we see the future of financial modernization being out there in terms of much larger and diverse holding companies, affiliations and operating subsidiaries. So it would appear to add another facet or twist to the privacy issue; or does it not, in your opinion?

Mr. FINK. I don't think it is that black and white, because the industry I represent has been able from the beginning to be affiliated with securities firms, with insurance companies, and for the last twenty years with banks. Securities firms and banks for twenty years have been affiliated. So, there were never bars, or they have come down in the last twenty years.

So you are not going to go from night to day when you enact H.R. 10. It is a movement forward, but a lot has already happened. We are not moving from a world of no affiliations to complete affiliation. There are currently affiliations, as I said, of security firms/banks, mutual fund companies/banks and mutual fund/securities firms. Most of the pieces have already happened. I am not denying H.R. 10 doesn't do something, but it is not quite a whole brave new world.

Mr. INSLEE. I will just tell you that my perception is that banks, number one, are doing this; and number two, want to do this. And let me tell you where I get that perception. One is their great desire for these affiliations and therefore H.R. 10. And number two, in my discussions with bankers, I have repeatedly heard them say—these are individual bankers, these are not folks who are paid lobbyists, although there is nothing wrong with paid lobbyists—have said, you know, "All we are really doing here is we are trying to provide a service to our customers. That is all we are trying to do here." And I go, "What do you mean?" And they say, "All we are trying to do is if Emma Smith has \$10,000 in her bank account, we are trying to help her. We want the ability to try to help her to find the appropriate investment to make with that \$10,000."

And that is fine for the banks to have that motivation, but my belief—and I am going to ask you again to reiterate this—should not the consumer in these circumstances have the legal right to tell their banker not to use that information to try and market a product to them unless the consumer wants that service? Should not the consumer have that legal right?

Mr. Fischer.

Mr. FISCHER. Comptroller Hawke today talked about reasonable expectations and also statements from customers about certain types of activities that they found unacceptable. You also, sir, made a similar point in your example about telemarketing in that same panel. There is absolutely no question in my mind that under existing law today, and I said this earlier in my answer, if a consumer says "do not do this," then their expectation, which is enforceable

under law today, is that you will not do it and if you fail to do it you will be punished.

If you look at the situation, and I am not commenting on the underlying facts at all, in Minnesota where the allegation was that reasonable expectation was breached, in that case you didn't even have to say don't do it. The alleged activities were such, third parties, telemarketing information, that it was simply beyond the expectations and if that is not enforceable, I have never seen it.

In this particular situation when you are talking about affiliates, if you have someone say "do not use my information," as far as I am concerned—and this is how I advise financial institutions—you cannot use that information. I was going to say then, to go beyond that, though, and say that now we need to create a structure that not only says that you have to honor your customers' requests to not send things to them, which is existing law, but you have to put into place the sort of very broad initial annual and other disclosure requirements that are included in H.R. 10 and expand that to the affiliate relationship which is the core of the purpose of H.R. 10. That is where I say has crossed the line.

Mr. INSLEE. Would the Chair indulge me just for another minute or so?

Chairwoman ROUKEMA. We do have a vote, you understand. You can have the time. Go right ahead.

Mr. INSLEE. One more question. If in fact you believe, which I appreciate that consumers ought not to be violated in that sense, if they give a specific direction to a bank, what I hear you saying then is you think that prohibition already exists. And if that is true—many of us believe it does not, because of the transactional exception for the Fair Credit Reporting Act—why don't we make sure of that and incorporate that in some language that prevents that marketing activity and gives them a specific opt-out? Why not do that?

Mr. FISCHER. Obviously I wasn't clear in what I said. It is not that the practice is prohibited, it is that you must honor the request of your customer. That was the example. You must honor it.

Mr. INSLEE. If that is the case, then what you are telling me is that you must honor the consumer's statement not to share it, but we don't want to be obligated to tell the consumers we are doing it. So you can do it in the dark of night as long as they don't find out and we will go ahead and just sort of do this as long as they don't find out. Is that what I understand you are saying?

Mr. FISCHER. There is almost no financial institution of any size, which means anyone with any affiliates, that today does not tell their customers that they are sharing with their affiliate, not with respect to all information, but with respect to most information.

In other words today—and you heard that appropriately acknowledged in the regulatory panel this morning—today, customers are receiving notices that you are sharing information with affiliates as it relates to applications, credit reports and everything else, except experience information, and today they have the ability to opt-out. And as you have heard, that very few of them do.

And I would respectfully disagree with the Comptroller. It is not because the notices are poor. We are following their suggestions in that respect. It is that customers do recognize the difference be-

tween their affiliates, their bank's affiliates who they trust, and third-party marketers who they simply do not.

Mr. VENTO. If the gentleman would yield to me briefly. I think that it is a very important point. And as far as U.S. Bancorp, which is headquartered in Minneapolis, Minnesota, as the gentleman from Washington knows, the allegations that were made actually went to the fact that they had asked consumers whether they could market. That is the allegation. And then in spite of the fact that they had checked off that they didn't want to be marketed, they did market them. And so that is the allegation. Nobody has ever demonstrated it. In fact, I know that there are some pretty vociferous differences with regards to it.

But in any case, the point is that they have now, of course, adopted something that is called the opt-out, for whatever it works.

But one of my questions on that is do you happen to know, Mr. Fischer, if the U.S. banks, or other banks working with telemarketers to promote dental policies for their customers adopted uniform banking industry privacy principles as outlined in the attachments to your testimony?

Mr. FISCHER. Sir, I cannot comment on that specific case, but I can say that the vast majority of banks, particularly larger banks, have adopted those policies. The Comptroller indicated this morning that nearly 70 percent, when they looked at it, had adopted them in the online world. Undoubtedly there is more today and it applies much beyond that.

Mr. VENTO. Getting back to Mr. Inslee's question, we have to go quickly, but there is an honest difference about disclosure. I think the disclosure now that goes on under the Fair Credit Reporting Act is sort of convoluted, because institutions are bound to permit you to opt-out of certain provisions, but other provisions they are not bound to do and generally do not.

The message that you get into disclosure and fairness, which is, of course, the answer they should be giving me with regards to the fraction of percent here, one that I feel obligated to put on the record here, is a missed message. So it may actually go higher with clarification. So we know that, but since it wasn't on the record—I do think there is some merit in it, even if it isn't as effective as the advocates would assume. I thank the gentleman for yielding.

Chairwoman ROUKEMA. Mr. Inslee, we will have to leave for a vote now. Do you want to submit your further question in writing or do you want to return here?

Mr. INSLEE. I am going to defer to your judgment, which is to submit my question in writing.

Chairwoman ROUKEMA. That was the conference that Mr. Vento and I had earlier.

Mr. VENTO. I would ask unanimous consent to put in the record the statement by Mr. Robert Litan yesterday that did not get put in the record.

Chairwoman ROUKEMA. Absolutely. I thought I had already taken care of that, but yes that is approved.

[The prepared statement of Robert Litan can be found on page 125 in the appendix.]

Thank you. There are some remaining questions, we could probably be here the rest of the day, but I do want you to know how

seriously we are taking your testimony. We will be continuing these hearings at some time in the near future. I do invite you to please submit to us any final remarks that you have or additional comments based on these last two questions or any afterthoughts that you have had. We will distribute them. Thank you very much. We greatly appreciate it. Sorry we have to dash off.

This hearing is closed and the subcommittee is adjourned.

[Whereupon, at 2:07 p.m., the hearing was adjourned.]





# **A P P E N D I X**

July 20, 1999

Congresswoman

# Marge Roukema

Fifth District - New Jersey

---

2469 Rayburn House Office Building/Washington, D.C. 20515 (202) 225-4465

Contact:  
J. Craig Shearman  
(202) 225-4465

Release:  
July 20, 1999

## Roukema: Comprehensive Approach Needed for Financial Privacy

*Following is the opening statement of House Financial Institutions Subcommittee Chairwoman Marge Roukema, R-N.J.-5th, at today's hearing on financial privacy issues. The hearing will continue at 10 a.m. Wednesday in Room 2128 of the Rayburn House Office Building.*

Today, the Subcommittee is convening for several days of hearings regarding emerging privacy issues. Privacy touches all of our lives. There is no one here in this room that does not want to ensure that their personal information is secure. The issues relating to privacy are all encompassing and involve literally every aspect of our lives.

During consideration of H.R. 10, I worked with Mr. Vento, Ms. Pryce, Mr. Oxley, Mr. LaFalce and Mr. Frost to craft an amendment to enhance H.R. 10 with workable privacy protections. The House approved this amendment on a vote of 427-1, which requires banks, securities firms, and insurance companies to disclose their privacy policies and provide consumers with the ability to "opt-out" of the sharing of nonpublic personal information with nonaffiliated third parties. Furthermore, the amendment prohibits financial institutions from sharing customer account numbers for the purpose of third party marketing.

Does this amendment address all the concerns relating to privacy? Absolutely not. In fact, Congressman Inslee offered an amendment during the Banking Committee's mark up of H.R. 10, which was broader than the language contained in the amendment that we offered on the floor. I supported the Inslee amendment. However, I feel that, first, a comprehensive, rational discussion of how best to further proceed on the issues relating to privacy is in order. Such discussions are necessary to ensure that new legislation does not create unintended consequences, such as inhibiting an institution's daily operational needs. Our hearings this week largely will focus on privacy as it relates to the financial services industry in the off-line world. Our financial services industry is rapidly growing with services that are being offered over the Internet, which raises a host of privacy issues that this Subcommittee must address. This week is intended to be the beginning of several hearings that will be necessary in order to give due attention to all aspects of financial privacy.

The privacy debate has raised many questions regarding the extent to which we as consumers can "trust" that our financial, medical, and other personal information is maintained in a confidential manner. A breakdown in that trust would result in severe consequences for the business world and our economy. Consumers want to know who is collecting their financial information. What kind of information is being collected and who has access to it? For example, consumers may not object if their information is being shared so that they can be offered a product or service, but consumers may want to know under what circumstances such information is going to be shared. Furthermore, consumers want to know how they can maintain a reasonable degree of control over who collects and uses their personal information. The industry has expressed significant concerns about new legislation that could have "unintended

consequences" on their business operations. What are those consequences?

The industry received a wakeup call last month when the Minnesota Attorney General filed suit against U.S. Bancorp for practices related to sharing customer account information with third parties for the purpose of marketing nonfinancial products and services, such as low-cost medical and dental plans that could be paid for by automatic debits from consumers' checking accounts or automatic charges to their credit cards. Once aware of the practice, consumers expressed their outrage. Demonstrating the role of market discipline, many institutions reacted by revamping their privacy policies and committing to not engage in such third party information sharing practices.

Along with financial privacy issues, the Subcommittee will receive testimony on medical privacy. Concerns have been expressed by many groups that H.R. 10's medical privacy provisions will undermine the more comprehensive medical privacy initiatives currently being pursued on both sides of the Capitol. Such groups have suggested that the medical privacy provisions be stripped from the bill. I do not understand the logic of this suggestion. It would be irresponsible for H.R. 10 to be enacted without fundamental medical privacy protections for consumers. Let me emphasize that H.R. 10 is only a foundation. I, too, favor more comprehensive medical privacy legislation. However, stripping H.R. 10 of its medical privacy provisions in hopes that separate more comprehensive legislation will be enacted is unwise and irresponsible.

Over the course of today and tomorrow, we have invited witnesses from a broad range of perspectives, including government, academia, consumer advocacy, and industry. Witnesses will provide information on the categories of consumer financial information that are collected and how such information is used. Also, we will examine what Federal and State laws already cover financial privacy protections. Furthermore, our witnesses will offer their expert opinion on ways in which both consumers and businesses are affected by some of the policy approaches currently contemplated by Congress as well as what steps should be taken to strengthen the financial privacy of all consumers. I look forward to their testimony.

I would like to recognize our ranking member, Bruce Vento, who has played such a vital role in the privacy issue.

# Congressman Bruce F. Vento

## Minnesota, 4th District

Office of Congressman Bruce F. Vento • 2413 Rayburn House Office Building • Washington, D.C. 20515 • (202) 225-6631 • Fax: (202) 225-1968

For Immediate Release

Date: July 20, 1999  
 Contact: Erin Sermeus  
 Phone: (202) 225-6685

### STATEMENT OF CONGRESSMAN BRUCE F. VENTO AT THE FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE HEARING ON EMERGING FINANCIAL PRIVACY ISSUES

Thank you, Madame Chairwoman, for convening these two days of comprehensive hearings. We have a significant group of witnesses who should explore the full range of privacy issues in our economy. Privacy is increasingly on the minds of consumers as they see the technological advances eroding barriers, linking heretofore random data, shrinking the world and sharing their personal profiles with others.

In many respects, these two days of hearings are a continuation of our Subcommittee's look at consumer financial privacy which began in September of 1997. We took that look with a slight focus on the impact of the Internet on consumer privacy. But we also touched on many of the same issues we will have before us today: the adequacy of the Fair Credit Reporting Act (FCRA); data security; identity theft; and information sharing for marketing of products and services.

What may be different is that in these post-H.R. 10, post-Know Your Customer days, we have finally become a very sensitized Congress. With every day it becomes clearer that the American economy is running on data: customer data. We collect, disseminate, study, share and peddle profiles and preferences of people to run companies, enforce laws and sell products. But what voice and choice does any consumer have over their own personal and public data? What is the right balance of free information flow versus privacy protection? Should the only choice a consumer has be that she/he not do business with a company or a group of companies because she/he doesn't like their privacy policies?

Public concerns about personal information privacy are growing. Seemingly each week there are new reports of stolen identities and credit cards, selling of consumer financial data, "cookies" on Internet sites, false IRS returns and hijacked ATM cards and numbers. Bad actors are still stealing mail to divert your account statements. Companies are using old fashioned directories based on where you live to decide whether to interrupt your dinner with a phone call. Grocery stores are compiling your complete eating habits just because you sought to save a few bucks. Charitable groups are sharing or selling lists of their contributors. States are selling driver's

license numbers which are often your social security number. No matter what we do or do not do here, the modern consumer must be vigilant about the information that is out there about themselves. We are surrounded. Unwanted junk mail, spam and catalogues are the least of a person's worries.

With regard to financial privacy, Madame Chairwoman, I think we had a good product pass the House of Representatives as an amendment that we worked out to H.R. 10 earlier this month. This product affords consumers with new important safeguards for their financial privacy, putting banks, credit unions, securities and insurance firms at the forefront of many other U.S. sectors.

As passed by the House, H.R. 10 provides strong, affirmative provisions of law to respect and provide for a consumer's financial privacy with a privacy policy that meets federal standards to protect the security and confidentiality of the customer's personal information. Importantly, H.R. 10 prohibits the sharing of consumer account numbers for the purposes of third party marketing. This protection applies to all consumers and requires no action on their part. Consumers can "opt-out" of sharing of information with third parties in a workable fashion that protects consumers' privacy while allowing the processing of services they request. And importantly, regulatory and enforcement authority is provided to the specific regulators of each type of financial institutions.

H.R. 10 specifically prohibits the repackaging of consumer information. Data cannot be resold or shared by third parties or profiled or repackaged to avoid privacy protections. Further, consumers must be notified of the financial institution's privacy policy at the time that they open an account and at least annually thereafter.

Certainly, these are giant steps forward. These common sense hopefully workable provisions were added to the substantial protections already included in H.R. 10 that prohibit obtaining customer information through false pretenses and disclosing a consumer's health and medical information.

But because there are those that would have liked to have gone further, some who wanted to eliminate provisions like the medical privacy protections in the bill, and because the issue of financial privacy is certainly bigger than H.R. 10, I am hopeful that with these hearings we can begin to look at the big picture and then to act appropriately on the totality of privacy policy matters.

This Congress needs to step up to the plate and provide the legal framework across the board for protecting consumer privacy. While it is appropriate to insure that adequate privacy safeguards are in place to protect consumer privacy in our changing financial marketplace, we certainly need to look comprehensively at all the economic sectors, including the government, to understand how they all utilize information about people.

As many of my colleagues know, I have worked throughout my career on consumer rights and privacy. I have worked to protect consumer privacy through laws like Truth in Lending, Fair Credit Reporting Act and the Electronic Fund Transfer Act. I also introduced one of the first proposals to protect a consumer's privacy on the Internet, the Consumer Internet Privacy

Protection Act.

During the Banking Committee mark-up of H.R. 10, I initially introduced an amendment that would have provided an annual "opt-out" on affiliate sharing and beyond. I withdrew that amendment because I realized that it was unworkable and that there was much more to be shaped on financial privacy policies.

What is crystal clear is that a law that requires consumer action is appropriate, but third party and affiliate "opt-out" is hardly the first and last word in consumer rights. The fact is that a number of consumers have such a right today under FCRA or institution policies. Even with that authority, only a small fraction of individuals -- less than 1 percent -- exercise that option. Consumer choice may give us a warm feeling but what does it really accomplish? What is the bottom line? Does it really provide choice if a fraction of 1 percent responds to "opt out?"

Finally, the bottom line must be enforcement of such law. I note that we will have a witness from the Federal Trade Commission. Their testimony at the Commerce Committee last week promoting continued self-regulation for Internet privacy protection underscores for me the deficiency of some of the proposals for H.R. 10 which had superimposed the FTC as a privacy regulator. That approach would have given enforcement authority to the Federal Trade Commission as opposed to the appropriate functional regulator for each financial institution. I do not think we should turn over such an important enforcement authority to a non-financial institutions regulator. Indeed the functional regulators today show every sign of eagerness, awareness and the will to make financial privacy law work!

Madame Chairwoman, I would entreat my colleagues and our witnesses that as we go forward, to first look to the breadth of the personal privacy issues in our economy. Financial privacy is important, however, privacy concerns are not limited to banks, security firms and insurance companies.

Second, look to the basics for consumers and business. People want to know what information is being collected, how and why. People want to know how the data about them is being protected. People want to know how to correct false information. People want to know how the laws are enforced. Business wants a fair opportunity to provide options and use information to better serve their customers. Business wants a level playing field across economic sectors. Business wants to develop the means to keep data confidential and accurate.

There has to be a way to bring both sides together that does not violate the privacy of individuals nor jeopardize the flow of our economy built so much on information that the Internet is king on Wall Street and new telephone area codes are a dime a dozen.

Thank you, Madame Chairwoman. I want to thank our witnesses today for their time. I look forward to our hearings.

####



Questions in Writing of Congressman Bruce F. Vento  
For the Witnesses at the Financial Institutions and Consumer Credit Hearings  
on EMERGING FINANCIAL PRIVACY ISSUES:  
July 20, 1999

For Robert Barsness:

1. Could you describe the kinds of every day business activities through which customer data is provided to third parties now that would not be protected by the exceptions under H.R. 10?
2. You mention a "free" insurance policy that may be affected by the opt out limitation? Why would opting out be bad for such a program? If it is a good benefit for consumers, why would a great majority of consumers opt out?
3. Would you support "opt out" for all information sharing for marketing and other non-transactional reuses for third parties and affiliates?



Questions in Writing of Congressman Bruce F. Vento  
For the Witnesses at the Financial Institutions and Consumer Credit Hearings  
on EMERGING FINANCIAL PRIVACY ISSUES:  
July 20, 1999

for Richard Barton

1. In your experience, are abstracts of files used for data mining for marketing limited to financial institutions? Are other sectors participating in this as well? To what degree?
2. How does a consumer know who is not a member of the DMA?
3. How do we protect consumers from bad actors with self regulation in marketing and on the Internet?
4. Are there financial institutions that are members of the DMA?
5. Is e-mail marketing captured by the DMA policies for consumer to opt out of receiving solicitations?



A handwritten signature in black ink, appearing to read "B. Vento". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Questions in Writing of Congressman Bruce F. Vento  
For the Witnesses at the Financial Institutions and Consumer Credit Hearings  
on EMERGING FINANCIAL PRIVACY ISSUES:  
July 20, 1999

For Fred Cate

1. What state laws are in jeopardy of being preempted with regard to affiliate information sharing?
2. What kinds of tools are currently available for consumers to protect their privacy?
3. Your written testimony talks about the developments in on-line banking that give consumers greater ability to express preferences for how information about them is collected and used. Can you give me some examples of what you mean?
4. Does H.R. 10 as passed the House, or a future limitation on sharing of information among affiliates constrict competitiveness of financial industries vis a vis other non-covered industries?



Questions in Writing of Congressman Bruce F. Vento  
For the Witnesses at the Financial Institutions and Consumer Credit Hearings  
on EMERGING FINANCIAL PRIVACY ISSUES:  
July 20, 1999

For Barry Connelly

1. What kinds of information are your members using to profile consumer and sell to marketers? How do they market and sell this information? To whom do they sell it? Are most of the purchasers financial institutions? Or other industrial sectors?
2. On page 4 of your testimony, you suggest that some of your members develop high value information-based products such as fraud prevention and risk management systems. Could you give some examples?
3. In creating high value information-based products, what data do you use? From where do you obtain it?

Questions in Writing of Congressman Bruce F. Vento  
For the Witnesses at the Financial Institutions and Consumer Credit Hearings  
on EMERGING FINANCIAL PRIVACY ISSUES:  
July 20, 1999



For Mr. Mierzwinski

1. What is your best guesstimate of the percentage of people who would opt out of third party marketing? Affiliate information sharing? What do you think the percentage would be for opting in?
2. What concerns do you have, if any, about the operational or transactional concerns that the financial industries have raised with regard to complete prohibitions of data sharing? What besides "marketing" is a concern for you?
3. What are your views on the provisions placing an affirmative responsibility on institutions to respect and protect privacy in H.R. 10?
4. Do you support self regulation for privacy for any industry? The Internet? Financial institutions? Other companies?
5. What kinds of tools are available for consumers to protect their privacy today? Are the services offered by companies that suggest they will protect a consumer's privacy for a fee effective?



Questions in Writing of Congressman Bruce F. Vento  
For the Witnesses at the Financial Institutions and Consumer Credit Hearings  
on EMERGING FINANCIAL PRIVACY ISSUES:  
July 20, 1999

For Marc Rotenberg

1. How does existing technology that promotes seamless transitions -- back and forward features for example -- on Internet surfing, work for or against privacy of the individuals surfing? How can this be addressed? How is information, the cookie stream, being used to market or otherwise monitor consumers?
2. Do you support self regulation for privacy for any industry? The Internet? Financial institutions? Other companies?
3. Are there possibilities that e mail, e money accounts etc. . . are vulnerable to being intercepted or accessed at some routing computer or network storage of a company? What can consumers do? Is this a financial industry problem or multi industry problem?
4. Do you have any concerns regarding information compiled that may be inaccurate and that consumers would be unable to correct?

Testimony of Robert E. Litan<sup>1</sup>  
before the  
Subcommittee on Financial Institutions and Consumer Credit  
of the  
House Committee on Banking and Financial Services  
July 20, 1999

Madame Chairwoman. Thank you for inviting me to appear today to discuss issues relating to privacy in the financial services industry.

Several months ago I prepared a working paper on this subject for the AEI-Brookings Joint Center for Regulatory Studies, which I attach to this testimony.

I argued in that paper, and now outline for you briefly today, several propositions:

First, policy makers – including Congress – should be cautious about legislating in an area where markets and technology are moving rapidly. This couldn't be more true with respect to matters dealing with the Internet, where time is measured in weeks, if not days.

Second, at the same time, even on the Internet there can be market failures which call for government intervention, assuming the intervention itself does not create more problems than it cures.

Privacy is one area where the market appears to have failed, at least to some extent. Every survey I have seen indicates that strong majorities are concerned about their privacy on the Net. Yet many firms sell personal information without the subject's knowledge or consent. It is true that surveys also show an increasing number of web sites providing notice and to a lesser extent an opt out. But progress remains uneven.

Third, and this is the most important point I want to make in my opening remarks, U.S. law appropriately has never made privacy an absolute right that trumps everything else in all circumstances, as is broadly the case in Europe.

Instead, we have consistently *balanced* the benefits of privacy protection against the costs of providing it. There are objectives which often conflict with privacy –

---

<sup>1</sup> Vice President and Director, Economic Studies Program, The Brookings Institution and co-director, AEI-Brookings Joint Center for Regulatory Studies.

including the needs of law enforcement, the desire to ensure a continuing flow of information, and the First Amendment's guarantee of a free press, among others.

I urge the Congress to continue this balancing approach. This means, among other things, that the more sensitive the information and the less costly it is to protect it, the more protection it should have.

For example, this explains why Congress already has prohibited the sharing of data about individual's video rental or cable TV viewing habits. It also justifies provisions in HR 10 that restrict the sharing of medical information by insurance companies belonging to financial conglomerates. Indeed, medical information is so sensitive that it ought to be covered by more generic legislation, which I understand that Congress has been considering.

Personal financial data also is sensitive. But there are also competing reasons why much of it needs to be shared under some circumstances. For example, accurate credit ratings of individuals and businesses depend on the sharing of data through credit bureaus. If government prohibited data sharing of this type, credit would be far more expensive and less available than it now is. Similarly, banks share financial data with third parties that process it and to prevent fraud. These competing objectives demonstrate why an across-the-board opt-in requirement for financial data would be a major mistake in my view.

The heart of the complaints about financial privacy – indeed privacy on the Net more generally – center instead on the use of personal data for *marketing purposes*. Some consumers object to having their financial institutions provide sensitive personal information to retailers and other third parties. They ought to be given the opportunity to opt out of such information sharing, and H.R. 10 appropriately gives them that right.

As it is currently written, however, the opt out requirements of H.R. 10 do not apply to affiliates of financial institutions. Although I am aware that the financial industry strongly opposes extending those requirements to affiliates, I have come to believe that this opposition is short sighted.

One of the things that renders financial institutions – and especially banks – unique is the trust that consumers place in them. Banks that abuse that trust will be punished in the marketplace. For some, the debate over affiliate sharing of information stops there. Why not let individual institutions follow different policies and let the market decide the outcome?

The problem with that laissez-faire position is that banks that weaken customer trust in their individual institutions may weaken trust in the entire industry. Several “bad apples” can erode consumer trust in the whole barrel.

I therefore believe that a notice and opt out provision for marketing purposes ought to be extended to all affiliates of financial institutions and that such a provision is

in the institutions' own self-interest. Indeed, it would even save them money. Better that they know up front who is not likely to be receptive to a solicitation than to waste a bunch of money finding out.

More broadly, I am coming around to the view that there is no reason why financial institutions ought to be singled out in this regard. Why not require all retailers conducting interstate commerce – on or off the Internet -- to notify consumers of their privacy policies and offer them an opt out of having personal information transferred to third parties or affiliates for marketing purposes?

Extending such a requirement to the Internet in particular would strengthen customer confidence in the Net and encourage even faster growth in e-commerce, especially as data mining becomes ever more sophisticated (as was highlighted on the front page of yesterday's *Wall Street Journal*).<sup>2</sup> The analogy here is to \$50 liability limit that Congress placed on credit cards in the 1970s. Once the limit was in place, credit card use took off – in large part because people then have greater confidence in using their cards. I firmly believe a common policy on privacy on the Net would do the same thing for e-commerce, which although it is growing rapidly, still remains a tiny fraction of overall retail sales. A further benefit is that an across-the-board, but reasonable, privacy statute might go a long way toward defusing the continuing tension with the EU over its privacy directive.

I want to underscore the fact that my recommendation for an opt out is limited to marketing purposes. Indeed, if I were drafting the privacy provisions of HR 10 I would simply limit the opt out to marketing purposes rather than generically impose it and then provide a laundry list of exceptions to allow for legitimate uses of customer data. The problem with the "exceptions approach" is that there is a danger that the list will miss worthy uses of information sharing that may develop tomorrow but that would be prohibited by the current law today.

Finally, I recognize there are those who believe an opt out regime is too weak and that it should be replaced with an opt in requirement. As I've noted, there are important uses of financial information – fraud detection and third party processing, among others – that would be frustrated or effectively rendered impossible to carry out in an opt in regime.

But I also believe it is premature to be legislating an opt in associated with the transfer of financial information even if it were limited to marketing purposes. Many consumers learn of new products and services – and I count myself among this group -- only because information about them can be easily transferred from collectors to other parties. A significant cost of imposing an opt in is that marketers would find it much more difficult to target potential audiences for their products. The net result would be more rather than less junk mail and more mass advertising. This would aggravate some consumers and add to costs generally, which show up in higher prices of goods and services.

Many thanks again for inviting me to appear and I look forward to your questions.

---

<sup>2</sup>Alan Murray, "Net Effect: Is Service Getting Too Personal?", *Wall Street Journal*, July 19, 1999, p. A1.



**J O I N T   C E N T E R**  
AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

**The Regulatory Right-to-Know Act  
and  
The Congressional Office of Regulatory Analysis Act**

**Joint Testimony before the  
Committee on Governmental Affairs  
U.S. Senate**

**Robert W. Hahn and Robert E. Litan**

Testimony 99-1

April 1999

Mr. Hahn is Director of the AEI-Brookings Joint Center for Regulatory Studies, a Resident Scholar at AEI, and a Research Associate at Harvard University. Robert E. Litan is Director of Economic Studies at the Brookings Institution and Codirector of the AEI-Brookings Joint Center for Regulatory Studies. A copy of this testimony can be obtained from the Joint Center's web site: [www.aei.brookings.org](http://www.aei.brookings.org). The authors have benefited from the comments of Arlene Holen and Randy Lutter. The views expressed here represent those of the authors and do not necessarily reflect those of the institutions with which they are affiliated.



### **Executive Summary**

Regulation is becoming increasingly important in many aspects of our economy. Congress has traditionally paid much less attention to the benefits and costs of regulation than to directly budgeted expenditures. This imbalance needs to be rectified.

Congress is now holding hearings on the Regulatory Right-to-Know Act and the Congressional Office of Regulatory Analysis Act. Those acts, if passed, will highlight the impact of regulation on consumers and workers; help inform the process of designing new laws and regulations; and also help provide insight on how to improve existing regulations.

This testimony argues that both those bills are likely to improve regulatory accountability. We offer some specific suggestions for strengthening the Right-to-Know Act, for example, by encouraging the Office of Management and Budget regulatory oversight unit to make greater use of its expertise in evaluating the actual impacts of federal regulation on the general public. We also make some practical suggestions for implementing a congressional Office of Regulatory Analysis, including recommendations on which regulations to analyze, the scope of the analysis, and the timing of such analysis so that it can have an important impact on the regulatory process.

**The Regulatory Right-to-Know Act  
and the Congressional Office of Regulatory Analysis Act**

Robert W. Hahn and Robert E. Litan

I. **Introduction**

We are pleased to appear before the committee to provide our views on the Regulatory Right-to-Know Act (S. 59) introduced this session by Senators Thompson, Breaux, Lott, and Stevens and the Congressional Office of Regulatory Analysis Act introduced in the past congressional session by Senators Shelby and Bond.

The two of us have studied and written about regulatory issues for over two decades. Recently, we helped the two institutions with which we are affiliated—the American Enterprise Institute and the Brookings Institution—form a new Joint Center for Regulatory Studies which, among other things, is reviewing federal regulatory and legislative proposals.

We believe that both bills are good ideas and should be adopted, with minor modifications. Both would help ensure that regulators, lawmakers, and interested parties have better information on the benefits and costs of individual regulations as well as the cumulative impact of the entire federal regulatory effort. In that respect, the bills would help bring information disclosure about regulatory activity up to the standards long required for on-budget activity, thus enhancing regulatory accountability.

Indeed, one lesson the United States has been preaching to the rest of the world in the wake of financial crises in Southeast Asia and Russia is that activity in both the public and private sectors must be “transparent.” This simply is another way of saying that the public has a “right to know” information that is relevant to decisionmaking by both firms and governments. Both bills would apply that principle to regulation in this country. It is about time.

I. **The Regulatory Right-to-Know Act**

S. 59 would make permanent a requirement that Congress has imposed on the Office of Management and Budget (OMB) over the past two years: to prepare annually a report to Congress on the total benefits and costs of federal regulations.

Before those annual reports were required, the American people had no idea of the cumulative impact of federal regulatory activity. Now they know that federal regulations impose burdens on the private sector most likely in excess of \$200 billion a year, depending on how the costs are defined; and according to estimates supplied by federal agencies, federal regulations deliver total benefits of at least that magnitude and conceivably much more.

The OMB reports have been far from perfect, as we will explain. But that does not mean that they should be abandoned, especially now that the agency has gained experience preparing them. In making the reporting requirement permanent, Congress should be urging OMB to improve its estimates of benefits and costs and to expand its recommendations for legislative changes.

## 2. Responses to Possible Objections

Before outlining our suggestions for improving S. 59, we want to anticipate a number of possible criticisms of the bill and address each in turn.

### *General Concerns about Using Benefit-Cost Analysis*

Some interest groups object to the basic concept of collecting and reporting information on the benefits and costs of regulations for various reasons. For example, some claim that the numbers are too imprecise to be of much use. Others claim that the seeming precision of hard numbers drives out nonquantifiable considerations from regulatory decisions. And still others object on moral grounds—in particular, to the monetization of human health benefits. We do not believe that any of those objections defeats the usefulness of the kind of report that S. 59 would mandate and that OMB has already issued twice.

The broadest response to the critics is that the rear-guard battle over benefit-cost analysis, frankly, is over. Successive presidents from both parties for twenty-five years have issued and adhered to executive orders that require the executive branch agencies to analyze

the benefits and costs to the best of their ability before taking regulatory action. Those orders do not require the quantification or monetization of the impossible. But they do recognize that benefit-cost analysis provides a useful *framework* for making decisions: an organized and systematic version of a list of pros and cons. We strongly suspect that if any of those individuals who object to benefit-cost analysis were to become the head of a regulatory agency, he or she would use something that approximated that method of decisionmaking, even if only implicitly. The executive orders make the analysis explicit. And S. 59 simply asks that OMB report to Congress and the American people the cumulative impact of all those decisions.

We are not oblivious to the concerns of critics, however. It is true that the current state-of-the-art does not often permit precise numerical estimates of benefits and costs. For that reason, some agencies include ranges for the relevant figures as well as best estimates. There is nothing wrong with that; indeed, specifying reasonable ranges often can be far more illuminating than offering precise estimates that do not acknowledge key uncertainties.

Although benefit-cost analysis provides a useful framework for decisionmaking, there are times when policymakers may not wish to take the results literally. For example, the numbers generated in the exercise do not remove nonquantifiable factors from decision making. Instead, they can help policymakers put *implicit* price tags on those factors so that they better understand the implications of decisions.

For example, suppose that the best estimate of the economic impact of a water pollution rule is that it would cost \$500 million annually to implement while generating quantifiable social benefits of \$400 million. Regulatory officials may still choose to approve the rule, however. In some cases, they may not be permitted by the authorizing statute to balance benefits and costs, in which case Congress and the public would then at least know the consequences of such a statute. Alternatively, the officials may be allowed to balance, but they recognize other *nonquantifiable* benefits—such as the benefit to society of having clean bodies of water—that, in their view, tip the balance toward adopting the rule. In that case, the benefit-cost analysis will have revealed the *implicit* value of the nonquantifiable benefits to be at least \$100 million. That, too, is useful information for the public and Congress.

The critics of monetizing benefits, such as putting values on saving or extending lives and reducing the risk of injury—ignore one simple point. Whether one does it implicitly or explicitly, judgments are made all the time in both the public and private sectors about how

much to spend to achieve given levels of safety. The fact is that limitless resources are not spent in pursuit of that objective. We do not spend the whole gross domestic product (GDP) attempting to save lives, however much we would like to do that. If we did, there would no other activity taking place in our society—no recreation, no travel, and no education. Instead, we all make decisions about how to trade off some objectives against others. You, as legislators, do it when you decide how much to allocate to education, to transfer payments, and to various other activities that in their own ways help save lives—national defense, medical research, and crime prevention, to name a few. Juries put values on human lives and injuries; they do not place infinite values on either. When regulators place values on saving lives or avoiding injuries, they are simply making explicit judgments that can be used to help compare the benefits with the costs that the private sector and public will be asked to pay under different regulatory proposals. In the process, they help decide how and to what extent society should allocate its scarce resources toward given regulatory objectives.

Significantly, the executive orders instructing the agencies to conduct regulatory analyses do not mandate that all benefits be monetized in every case—only that this be done to the extent practicable. It is noteworthy that S. 59 does not even go so far, for it speaks only of “effects.” We believe that the bill should go further and follow the approach of current Executive Order 12886. Specifically, the bill should include additional language instructing OMB to estimate both benefits and cost in monetary terms, to the extent practicable. Furthermore, Section 6 of the bill—which instructs OMB (with advice from the Council of Economic Advisers) to issue guidelines to agencies to standardize their measurement of benefits and costs—should also instruct OMB to standardize the monetization of benefits and costs, when such estimates are available.

#### *Many Statutes Do Not Require Regulatory Balancing*

A second possible objection to S. 59 would question the usefulness of a regulatory accounting when a number of regulatory statutes do not allow the balancing of benefits and costs. We believe that the annual report is nonetheless useful.

As noted, executive orders have for over two decades required regulatory analyses to be conducted, even for regulations where balancing is not allowed. We believe that this is so

because regulators still find estimates of benefits and costs useful in rendering their decisions, if for no reason than to have a basic "reality check" before issuing their rules. Furthermore, whether or not the information is used to provide such a check, Congress and the public have a right to know the impact of the rules that are being promulgated under statutes that prohibit balancing. Such information could lead Congress to change its mind about the statutes, as in fact Congress has done in recent years by changing the Delaney Clause of the Food, Drug and Cosmetic Act and introducing some balancing language in the Safe Drinking Water Act.

The annual reports can also help Congress consider the overall "balance" of the regulatory effort: in particular, whether private sector resources might be reallocated so as to generate even larger benefits for the same aggregate cost. In that regard, one well-known study by researchers at Harvard found that a reallocation of mandated expenditures toward those regulations with the highest payoff to society could save as many as 60,000 more lives a year at no additional cost. Whether that is the right number is not the point. That kind of inquiry should be of central importance to Congress. But Congress cannot begin to address such issues without having the kind of information included in the OMB annual report, which under S. 59 must include not only total benefits and costs, but similar information by agency, agency program, and major rule.

#### *Official Estimates May Be Based on Unreliable Studies*

A third possible objection questions the value of the annual report to the extent that OMB and/or the agencies include estimates of questionable reliability. In particular, is it possible that OMB and/or the agencies can "game" Congress by displaying estimates strongly favoring existing regulations, so as to fend off possible criticism?

In fact, we are sympathetic to that concern. The most important difference between OMB's report of 1997 and the 1998 report is that the more recent one includes a new estimate of the benefits of the Clean Air Act from the so-called Section 812 study, which EPA estimated at over \$3 trillion annually (at the high end). That estimate alone pushed the upper bound of benefits of all federal regulation to \$3.5 trillion, compared with a total cost range of \$170-\$230 billion.

While we recognize that the EPA estimate was the product of a peer-reviewed study, even OMB highlighted the strong sensitivity of the estimate to a number of assumptions and

pointedly noted that other agencies held different views from EPA about those assumptions. That is hardly surprising. While we believe that the Clean Air Act may indeed produce benefits well in excess of its costs, we also believe that the EPA estimate, which OMB only indirectly questions in its report, on its face lacks credibility. Can one statute really generate benefits that are approximately 40 percent of the nation's annual GDP?

It is therefore understandable why some might question the usefulness of a report that accepts agency estimates without independent analysis. There is nothing in S. 59 that would prevent OMB from continuing to follow that practice in the future.

But that does not mean that the reports are useless. It is important to have the administration on record as to what it believes the values of its regulatory effort to be, just as the administration every year must defend its annual budget. But the buck does not stop there, so to speak. Congress can and should play a role in questioning the basis for regulatory estimates, just as it does now for budget requests. The annual regulatory report thus serves as the beginning of debate and thoughtful deliberation, not the end of them.

Over two decades ago, Congress recognized that it could not properly discharge its appropriations and budget responsibilities without having its own analytical arm to provide independent evaluations of the administration's budget request. Hence, in 1974, it created the Congressional Budget Office (CBO). We believe that the assessment of regulatory impacts deserves the same kind of independent consideration. Therefore, we will shortly discuss why we believe that the proposal to establish a counterpart to CBO for regulatory analysis is also meritorious.

Finally, we note that S. 59 can be implemented with few additional resources. In any event, to the extent additional resources are required, we believe that they are well worth the cost. There is the potential to save billions of dollars annually while ensuring that consumers get better regulatory results. And there is reason to believe that the government does not spend enough money analyzing the potential for improving regulations. An average homebuyer, for example, spends about ten times more per dollar actually invested in housing than regulators spend analyzing expenditures that are required by regulations.

## B Suggested Modifications

Having strongly defended the need for S. 59, we nonetheless believe that it could be improved in several respects, either in the body of the bill or in accompanying legislative history.

**First, OMB should be required in its report to recommend each year some minimum number (perhaps ten) of regulations, programs or program elements that should be reformed or eliminated.** Those recommendations should be based on a careful assessment of the likely economic benefits and costs of the regulation or program. We are concerned that without such a requirement OMB may choose not to recommend any regulations or programs for elimination or reform. Indeed, OMB chose not to make such recommendations in its first report to Congress and only briefly addressed the topic in its second report.

**Second, OMB should identify in each report some minimum number of regulations (such as five) where its assessment of the likely impact of a regulation substantially differs from that of the agency proposing the regulation.** The issues relating to the Section 812 Study provide perhaps the most dramatic illustration of what can happen when OMB adopts without change an agency estimate of benefits and costs: in that case, the estimate on its face raises more questions than it answers and thus can cast a cloud over the reliability of OMB's entire report. If OMB is critical of certain agency estimates, but unable or unwilling to provide its own estimates, then at least it ought clearly to indicate that to be the case.

**Third, Congress should develop mechanisms for better enforcement of the OMB guidelines.** OMB has already issued guidance to agencies on how to measure the benefits and costs of proposed regulations and formats for reporting that information. While there is room for improvement, the fundamental problem is one of enforcement. We suggest that OMB, in addition to providing guidance, issue an annual peer-reviewed statement about the extent to which agencies are complying with such guidance. That statement could be included in the associated report. In addition, when agencies are not complying, Congress should take the degree of agency compliance into account in setting appropriations for the agency and in instructing the agency how to proceed in the coming year.



Fourth, as noted above, the bill should make clear that the estimates of both benefits and costs should be stated in monetary terms, to the extent practicable or feasible. By estimating benefits in monetary terms to the extent feasible, they can be compared more easily. At the same time, the limitations of such comparisons need to be noted.

Fifth, the statute should require OMB to redo the regulatory analyses on a select number of existing rules. As it is now, OMB has been relying on estimates in the professional academic literature (to which we have contributed) to provide baseline estimates of existing regulations and has then buttressed those estimates with agency estimates of their most recently adopted rules. As some critics have rightly pointed out, the baseline estimates are getting dated. Firms have perhaps responded to mandates issued long ago in different ways from what was initially expected. In addition, scientists or other analysts may have learned more about the magnitude of the benefits of certain rules. As a result, it is important that OMB incrementally look back over the existing body of regulations and update the benefit and cost estimates.

Why not have the agencies do that? The major reason is to begin to develop some independence in the estimates. Where those estimates suggest a need for modification of some rules, then those results can help form the basis of the recommendations in changes in regulations that S. 59 would mandate. The agencies can then get to work considering those modifications based on the new estimates.

We recognize that our suggestions would require OMB to hire consultants in the same way that agencies now do this for the new rules they develop—and that this will cost some money. The amount, of course, will depend on the minimum number of such analyses Congress mandates. The total additional resources in any event should not exceed several million dollars. Given the fact that many existing rules now impose annual costs on the private sector in the billions of dollars, not to devote some small measure of added resources would be penny-wise and pound-foolish.

### 3. The Congressional Office of Regulatory Analysis Act

You have also asked to us to assess the Congressional Office of Regulatory Analysis Act, which Senator Shelby proposed last year (as did Representative McIntosh in the House). That act would create a CORA to provide Congress with “independent, timely, and reasoned analysis of existing and anticipated Federal rules.” As noted earlier, such an office would serve as the regulatory counterpart to CBO.

A. Why CORA Is Sound

We believe that the CORA proposal is sound for three reasons: first, because it is likely to serve as an independent check on the analysis done in the executive branch by OMB and the agencies; second, because it will help to make the regulatory process more transparent; and third, because Congress can use the independent analysis to help improve regulation and the regulatory process.

OMB’s Office of Regulatory and Information Affairs (OIRA) faces inherent limits in the scope of its review of individual regulatory proposals. OIRA is headed by a political appointee chosen by the same administration that appoints the heads of the regulatory agencies. There is likely, therefore, to be some implicit understanding that the head of OIRA is not to press the agencies “too hard” because he or she is on the same “team” as the agency heads. Even if the head of OIRA were given authority to challenge regulations, the basis for those challenges is rarely made public; and the scope of those challenges is likely to be limited. The constraints on OMB are manifested in its annual report, in which it has, so far, simply accepted the benefits and cost estimates compiled by the agencies instead of providing any of its own assessments. CORA would not face those constraints but instead would be able to provide its independent analysis, much as CBO has done in the budget arena.

CORA would also make the regulatory process more transparent by providing both a more independent and a more public voice than OIRA. As noted below, CORA could submit comments on proposals that would help the public and Congress gauge their accuracy.

Congress can use CORA to help implement its recent legislation. For example, Congress adopted legislation (the Small Business Regulatory Enforcement Fairness Act) giving itself the opportunity for at least sixty days after a regulation is finalized to disapprove it before it becomes effective. Congress has yet to exercise that responsibility. As it is now, if and when Congress chooses to do so, it will have to rely on the agency’s own estimates of the

impacts of a rule and on any other data that interested parties may or may not have submitted in the rulemaking record. Significantly, Congress now has no *credible, independent source of information* upon which to base such decisions. That is analogous to the pre-CBO Congress, which had to make budget and appropriations decisions based solely on the information developed by the executive branch. We doubt seriously that, whatever their day-to-day criticisms of CBO may be, few if any members of Congress would wish to return to the pre-CBO era for appropriations decisions. Analogously, Congress should want to create an office to provide information and assessments of the impacts of regulations that are independent of those of the agency.

CORA could also aid Congress in periodically assessing the need to modify its own regulatory statutes. The OMB annual report, mandated by S. 59, would assist in that effort, but again, it will be based solely on the information that OMB chooses to convey to Congress. CORA can and should provide an independent assessment of that report, a responsibility that should be added to the language of the bill.

#### B. Implementation Issues

The CORA proposal raises a number of practical questions that this committee should consider before deciding whether to recommend it to the full Senate. We examine those questions below and suggest the need for modifying the bill in some cases and providing guidance in the form of legislative history in others.

*What should be the scope of CORA's duties?*

The Shelby draft of last year would require CORA to perform its own regulatory impact analysis (RIA) for every "major rule." We do not believe that CORA has to go that far—in effect, replicating everything the agencies do, but without anywhere near the level of resources. Instead, Congress and the public would be better served if CORA reviewed the RIAs and the rules—both as they are proposed (see further comments below) and when they are issued—for their methodological and factual integrity and for whether they reflect a consideration of reasonable alternatives and whether they are consistent with the authorizing

statute. In other words, CORA should be doing the same kind of review that OIRA now performs, only without the political constraints.

In addition, as we have just suggested, CORA should also be required to provide Congress with an assessment of the OMB annual report, much as CBO now does with the annual budget.

*How many rules should CORA review?*

If it is required to analyze all major rules, CORA is likely to be doing thirty or so analyses a year (and maybe more, counting the rules of independent agencies). The Shelby draft also requires CORA to analyze nonmajor rules if they are so requested by a Senate or House committee.

The ability of CORA to carry out that full mandate depends on the level of resources Congress gives it. Our view that CORA should learn to walk before it runs, and therefore, should start on the small side—perhaps with fifteen to twenty senior-level analysts—and only ramp up in the number of personnel as it gains experience (by comparison, although OIRA has more employees, it has, to our knowledge, only about fifteen to twenty-five senior-level regulatory analysts).

If that view is sustained—indeed, if CORA is given even fewer resources at the outset—then serious attention should be given to limiting the number of rules analyzed. At a minimum, therefore, we would propose striking the requirement that CORA analyze nonmajor rules. In addition, for major rules, CORA should be able to devote more resources to reviewing very important rules with potentially large economic impacts than to major rules of lesser import.

*How much information should CORA get, and when should it get it?*

The Shelby draft (which closely tracks the McIntosh proposal in the House) would ensure that CORA gets the same information that OMB now gets when reviewing rules. As a practical matter, that means that CORA would get the regulatory impact analyses and underlying supporting materials that are placed in the rulemaking record, along with the notice of proposed rulemaking (NPRM), at the time the rule is proposed. CORA also should

have access to any other materials the agency used to help prepare its RIAs, so that it has the data and models necessary to replicate agency results on benefits and costs. And, of course, CORA should get all comments filed in the public record after the comment period closes.

We understand that the administration has previously objected to the CORA proposal for intruding excessively into the rulemaking process. There is a valid concern here. CORA should not be created to replicate everything the agencies do, just as CBO was not created to replicate everything that OMB does or that the budget offices of the individual agencies do. Instead, CBO was created to provide a “check”—an independent source of evaluation.

CORA can and should play the same role. It can do that, for example, by placing its own comments in the rulemaking record of the agencies during the comment periods, which typically last from 90–120 days. Indeed, we suggest that the language of the bill and/or its legislative history strongly encourage CORA to provide such comments, which should help give the agencies early warning of what CORA is likely to say in its report to Congress after the rules are issued. Where the RIAs, their supporting documents, and NPRMs have provided insufficient information for CORA to submit meaningful comments, CORA should say so in its comments and thus put the agency on notice of the need to do more homework before issuing the final rule (a circumstance Congress can and should take into account in deciding whether to review rules after they are issued). Knowing that CORA may file such comments would provide a powerful incentive for agencies to compile thorough records and analyses before proceeding with their NPRMs.

When should CORA get its information? In particular, should it get it when OMB does—which is often well before the NPRM, at the stage when the agencies are just scoping out their options and in the preliminary stages of their analysis? The administration’s objections to the proposal seem to center on the answer to this question being yes. But the proposal can be easily modified to clarify that CORA is to receive the information that OMB obtains only at the time when rules are proposed. That should alleviate the administration’s legitimate concern about excessive intrusion into the deliberations of the agencies, but at the same time leave enough time for CORA to do its work. As long as CORA is not doing its own RIA—which we have counseled against—the 90–120 day comment periods that are typical of agency rulemakings should allow sufficient time for CORA to carry out its functions. But just to be sure, Congress may want to add language in the bill allowing CORA to request the agency to hold open its comment period for an additional period—perhaps thirty to sixty days—

when CORA believes that additional time is warranted and when the agency has not otherwise claimed a need for issuing the rule on an “emergency basis” (an option that should be retained).

C. Staffing CORA

As noted above, we believe that it is appropriate for CORA to build up a staff over time with individuals from backgrounds similar to those of the analysts now working at OIRA. In addition, we believe that CORA should have a permanent set of well-known independent scientists, economists, and other technicians on peer-review panels. CORA can and should draw on those individuals for advice and, in appropriate cases, for help in preparing analyses. The members of the peer-review panels should be individuals of unquestioned expertise and of high standing in their academic or professional communities. No individual should be chosen to serve on a panel working on a particular rule if he or she works in an industry affected by that rule or could benefit financially from its adoption. The same conflict-of-interest considerations should apply to putting individuals on peer-review panels who work for public-interest organizations that have stated their views on the rule or related rules.

D. Alternatives to a CORA

We believe that it is best for the independent review function to be lodged in a separate congressional agency. Otherwise, if made a part of CBO or GAO, the office is likely to have less clout, and there is a greater chance that its activities will get lost amid the larger functions already performed by those agencies.

4. Conclusion

Regulation is becoming increasingly important in many aspects of our economy. It has an important effect on our quality of life and the costs of goods and services; it also affects the ability of firms to compete in an increasingly global economy.

The Regulatory Right-to-Know Act and the Congressional Office of Regulatory Analysis Act, if passed, will help enhance regulatory accountability. Those acts would help highlight the impact of regulation on consumers and workers. In addition, they would inform the process of designing new laws and regulations and could also help provide insights on how to improve existing regulations.

Congress has traditionally paid much less attention to the benefits and costs of regulation than to directly budgeted expenditures. That imbalance needs to be rectified.

Congress needs to have better information on the likely benefits and costs of regulations that flow from the laws it passes. In addition, American citizens have a right to know how regulations are likely to affect them in everyday life.

## Related Readings

- AEI-Brookings Joint Center for Regulatory Studies. 1998. *Conference Summary: Changing the Way We Think about Regulation*. [www.aei.brookings.org](http://www.aei.brookings.org).
- Arrow, Kenneth J., Maureen L. Cropper, George C. Eads, Robert W. Hahn, Lester B. Lave, Roger G. Noll, Paul R. Portney, Milton Russell, Richard Schmalensee, V. Kerry Smith, and Robert N. Stavins. 1996. *Benefit-Cost Analysis in Environmental, Health, and Safety Regulation: A Statement of Principles*. Washington, D.C.: AEI Press.
- Breyer, Stephen G. 1993. *Breaking the Vicious Circle*. Cambridge, Mass.: Harvard University Press.
- Crandall, Robert W., Christopher DeMuth, Robert W. Hahn, Robert E. Litan, Pietro S. Nivola, and Paul R. Portney. 1997. *An Agenda for Federal Regulatory Reform*. Washington, D.C.: AEI Press and Brookings Institution Press.
- Graham, John D., and Jonathan B. Wiener, eds. 1995. *Risk vs. Risk: Tradeoffs in Protecting Health and the Environment*. Cambridge, Mass.: Harvard University Press.
- Hahn, Robert W. 1998. "Government Analysis of the Benefits and Costs of Regulation." *Journal of Economic Perspectives* 12(4): 201–10.
- Hahn, Robert W., ed. 1996. *Risks, Costs, and Lives Saved: Getting Better Results from Regulation*. New York and Washington, D.C.: Oxford University Press and AEI Press.
- Hahn, Robert W., and Robert E. Litan. 1997. *Improving Regulatory Accountability*. Washington, D.C.: AEI Press and Brookings Institution Press.
- Lutter, Randall. 1998. *An Analysis of the Use of EPA's Clean Air Benefit Estimates in OMB's Draft Report on the Costs and Benefits of Regulation*. Regulatory Analysis 98-2. Washington, D.C.: AEI-Brookings Joint Center for Regulatory Studies.
- Morgenstern, Richard D., ed. 1997. *Economic Analysis at EPA: Assessing Regulatory Impact*. Washington, D.C.: Resources for the Future.
- Office of Management and Budget, Office of Information and Regulatory Affairs. 1998. *Report to Congress on the Costs and Benefits of Federal Regulations*. Washington, D.C.: Government Printing Office.
- Office of Management and Budget, Office of Information and Regulatory Affairs. 1997. *Report to Congress on the Costs and Benefits of Federal Regulations*. Washington, D.C.: Government Printing Office.
- U.S. General Accounting Office. 1999. *Regulatory Accounting: Analysis of OMB's Reports on the Cost and Benefits of Federal Rules*, Draft Report to Congressional Requesters. Washington, D.C.: Government Printing Office.



Answers of Robert E. Litan  
To Questions Posed By Rep. Bruce Vento

1. How might opt out affect fraudulent activities perpetrated on, and prevention of such fraud for financial institutions? Does limited sharing of information for other than marketing purposes affect these activities in your opinion?

In my view, the cleanest way to ensure that fraud is prevented while consumers are given choice is to limit any opt out requirement to marketing purposes only. That leaves the financial institution able to pass on information to third parties and law enforcement officials to detect and catch fraud. Alternatively, the law can – as HR 10 is currently drafted – provide a broad opt out with an exception for sharing designed to detect and prevent fraud. But a broad right riddled with exceptions is likely to require constant fine-tuning as other problems associated with an opt out are discovered. Better, in my view, to limit the opt out right away to marketing purposes and leave it at that.

2. Is it appropriate to put one set of privacy rules on financial institutions and another set of rules on the Microsofts, Lockheeds and Targets of the US economy?

Ideally, I believe an opt out for marketing purposes should apply across the board to all firms conducting interstate commerce. The same principles of choice apply to all firms in our economy. At the same, I believe a case can be made that some information held by financial institutions – account balances and debt accounts -- is more sensitive than, say, the customer purchases at a Microsoft, for example. Furthermore, medical information is in even more sensitive – and warrants an opt in – than financial information. So, the piecemeal legislative approach to privacy is not the worst outcome; indeed, it is consistent with the way privacy laws have been enacted by Congress over time. However, I would prefer in an ideal world to apply an opt out across the board – in the real and virtual worlds – to all information collected and passed on for marketing purposes.

3. I have stated that an opt in could disadvantage smaller firms, charitable organizations and the like. Could I expound on this?

A generic opt in requirement very likely would dramatically reduce the amount of information that could be passed on – even for marketing purposes – between parties. This is because far fewer consumers tend to opt in to anything than tend to opt out. If this continues to be true, and I think there is a substantial likelihood that it will be, then imposing an opt in across the board would very much reduce the value of customer-name data bases that are now sold. This would mean that new firms and charitable organizations – which depend on acquiring customer lists so they can refine their marketing or solicitations – would find it more costly to assemble those lists. Alternatively, they would have target their mailings, call-ins, or other forms of marketing much more widely – and in the process, have a much lower “yield”. In the process, consumers would end up getting bombarded by even more junk mail or junk

calls than they now do. So everyone would be worse off. There would be less competition from a reduced number of new firms and organizations, and at the same time more junk solicitations from existing firms.

4. Many argue that financial and medical data are especially sensitive. However, it is possible for companies to track your consumer purchases and use that information in an inappropriate manner. Should this information be protected as well?

In principle, consumer purchases could be tracked – whether by monitoring “cookies” placed on your PC, or through the trade in customer purchase information acquired by stores that consumers frequent. For example, medical insurers might want to know which consumers bought particular items (cigarettes, beer, and the like) as a way of screening for higher risk customers. For all I know, this may be going on now – something the Congress may want to look into.

I haven’t thought deeply about how best this problem might be solved (and it wouldn’t be solved by an across-the-board opt out for marketing purposes, as I have suggested). It is tempting to say that certain types of data acquirers – such as medical insurance firms – should not traffic in this data, rather than to put limits on the data itself. Indeed, there may be other types of acquirers who might be so limited. But I cannot confidently support a measure yet without knowing of the possible side-effects or unintended consequences such a federally mandated limitation might entail.

5. Does the FTC have adequate resources to be a super-regulator for privacy?

The FTC already is involved in regulating privacy to the extent that firms – whether individually or collectively in trade associations and the like – make privacy promises and then don’t keep them. To do so is to engage in an unfair trade practice, and the FTC has charged at least one company, to my knowledge, with having done precisely that.

I do not personally know the number of FTC personnel who are now monitoring the Net and the various self-regulatory efforts now under way in the private sector. My suspicion is that it does not have sufficient resources to adequately support a widespread system of “self-regulation”. But that is a determination that requires the expert judgment of both the FTC and the Congress.

6. Would disclosure of privacy policies by financial institutions be prohibitively expensive?

Of course not. Most large banks already post their privacy notices on the web. They could easily do so in their bank lobbies, if they are not doing so already. There are standard notices that have been developed and they can be readily copied and posted.

7. Does an opt restrict information flow within companies and in our economy?

To a small extent it would, but the benefit is to ensure widespread consumer choice. The benefits greatly outweigh the small costs, in my view.

**PREPARED STATEMENT OF DR. MARY J. CULNAN**

Professor

The McDonough School of Business

Georgetown University

Washington, D.C.

Hearing on

**Emerging Financial Privacy Issues**

Before the

U.S. House of Representatives

Committee on Banking and Financial Services

Subcommittee on Financial Institutions & Consumer Credit

Washington, D.C.

Tuesday, July 20, 1999

Chairwoman Roukema and members of the Subcommittee, thank you for inviting me to testify. I also want commend you for scheduling these important hearings so quickly after the floor debate on H.R. 10, the "Financial Services Act of 1999." My name is Mary Culnan. I am a professor at the McDonough School of Business, Georgetown University where I teach electronic commerce. I have been conducting research on the impact of technology on consumer privacy for more than a decade. I have also been employed in the information systems field for more than thirty years, first as a systems analyst for a Fortune 500 company, and as a professor of information systems since earning my doctorate in 1980. This is the seventh time I have testified before Congress on information privacy issues, and the second time I have testified before the House Banking Committee<sup>1</sup>.

In the United States today consumers benefit from a robust information economy. Because most of us are not from very small towns but instead live in a "society of strangers," we also enjoy a large measure of personal privacy. The price we pay for that privacy is "surveillance" in the form of information systems.<sup>2</sup> Because the majority of organizations can no longer personally know their customers, the need for information to support decisions involving risk and to serve customers as individuals have fueled the growth of vast databases of personal information. These systems create benefits for both consumers and organizations such as lower costs, targeted offerings, personalized customer service and instant access to credit. However, their use also raises privacy concerns when consumer expectations of privacy come into conflict with what organizations believe is a legitimate commercial use of personal information.

My statement will be organized as follows. I will begin by providing some context for the discussion of financial privacy. Next, I will address two emerging issues related to financial privacy. First I will discuss the privacy issues raised by secondary use of personal information, that is the use of information collected for one purpose for other unrelated purposes. This section will include a discussion of the privacy issues related to secondary use of public records. I will conclude with a discussion of the new privacy

---

<sup>1</sup> See Statement and Testimony of Mary J. Culnan on Legislation to Amend the Fair Credit Reporting Act, Subcommittee on Consumer Affairs and Coinage, House Committee on Banking, Finance & Urban Affairs, June 6, 1991.

<sup>2</sup> See Steven Nock, *The Cost of Privacy*, New York, Aldine de Gruyter, 1993.

issues raised by the Internet. Many of my comments will address the use of financial information for marketing as that is my primary area of expertise.

### **The Context for Privacy**

Information privacy is the ability of individuals to control the terms under which their personal information is acquired by others and used. Underlying this definition is an implicit understanding that privacy is not absolute; rather the individual's privacy interests are balanced with those of society at large. Information privacy concerns can arise in three different contexts, all of which are relevant to work of the Banking Committee<sup>3</sup>:

- Organizational reuse or sharing of the information gathered about consumers in the course of routine consumer transactions, e.g. marketing;
- Authorized access to personal information about one individual contained in public records, credit reports and other databases, e.g. credit or hiring decisions;
- Unauthorized access to an individual's personal information either through a security breach or because the custodian of the information has not implemented appropriate internal controls, e.g. pretext calling, identity theft or having one's credit card number stolen online by hackers.

Prior research on privacy found that people are willing to disclose personal information in exchange for some economic or social benefit subject to the "privacy calculus," an assessment that their personal information will subsequently be used fairly and they will not suffer negative consequences in the future.<sup>4</sup> People disclose personal information to gain the benefits of a relationship; the benefits of disclosure are balanced with an assessment of the risks of disclosure. This hearing, then is as much about disclosure as it is about privacy. The information economy depends on consumers being willing to disclose personal information and to have that information used by business for legitimate commercial purposes including marketing. From the perspective of the financial services industry, privacy should be about making consumers confident that disclosing their personal information is a low risk proposition<sup>5</sup>.

<sup>3</sup> My testimony addresses the first type of use.

<sup>4</sup> R.S. Laufer and M. Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, Vol 33, No. 3, p. 22-42, 1977.

<sup>5</sup> See for example Mary J. Culnan and Sandra J. Milberg, "The Second Exchange: Managing Customer Information in Marketing Relationships," 1998, available at [www.msb.edu/faculty/culnanm](http://www.msb.edu/faculty/culnanm).

Organizations can minimize the perceived risks of disclosing personal information by observing fair information practices. Fair information practices are global norms that serve as the basis for U.S. privacy laws and self-regulatory programs as well as international privacy laws. At the heart of fair information practices are the following principles:

- Notice about what personal information is collected and how it will be used,
- Choice (e.g. opt out) about subsequent uses of personal information for other unrelated purposes,
- Access to their personal information and ability to correct any errors,
- Data Stewardship including integrity and security for data during both transmission and storage, and
- Enforcement and redress to ensure that organizations “do what they say.”

Fair information practices mediate the privacy concerns raised by disclosure and subsequent use of personal information by empowering individuals with control over their personal information, even if people do not choose to invoke the procedures. They also signal to consumers that the firm will not behave opportunistically with their personal information, and that the risks of disclosure are therefore minimal.<sup>6</sup> As a result, protecting privacy by observing fair information practices is good for business because doing so promotes consumer confidence and trust. I will now turn to a discussion of some of the privacy issues facing the financial services industry and the Subcommittee.

### **Secondary Use of Personal Information**

#### Commercial Financial Information

Consumers understand that they need to disclose personal information in order to qualify for automobile insurance, a mortgage or a credit card or to open a bank or a brokerage account. Surveys also show that people do not object to having other relevant sources of information such as their credit history or driving record checked as part of the

---

<sup>6</sup> For empirical evidence, see for example the Harris surveys conducted for Equifax Inc. and *Privacy & American Business*; Mary J. Culnan & Pamela J. Armstrong, “Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation,” *Organization Science*, Vol. 10, No. 1, p. 104-115, 1999; Mary J. Culnan, “Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing,” *Journal of Direct Marketing*, Vol. 9, No. 2, p. 10-19, 1995.

application process as long as the information is relevant to the transaction. It is secondary use of the information provided that raises privacy concerns.

Secondary use refers to collecting information for one purpose and subsequently using the information for other purposes. Privacy concerns are raised when this reuse is unrelated to or incompatible with the purpose for which the information was originally collected, and the firm does not offer the consumer the opportunity to object to this reuse. Secondary use includes unrelated use by the organization that collected the information as well as sharing the information with third parties. One of Washington's most prominent privacy attorneys stated that when the use of information is not compatible with the purpose for which it was collected, "the prospect of misinterpretation or crass exploitation usually follows."<sup>7</sup> The most common form of secondary use is targeted marketing.

Privacy concerns raised by secondary use are potentially greater in the financial services industry because along with medical information, personal financial information is viewed as highly sensitive by consumers. Anyone who examines their monthly credit card statement knows that a profile based on credit card or ATM transactions can provide a detailed picture of an individual's life. Further, technology now enables firms to analyze large databases of transaction data and to draw inferences that promote subsequent unrelated uses by the organization with which the consumer has a relationship, the organization's business partners, and unrelated third parties.

Public opinion surveys and my own research have shown that firms can balance these privacy concerns with their legitimate business need for the information by observing fair information practices. When consumers are offered notice and choice (e.g. opt out), privacy concerns are no longer significant and a majority of consumers do not object to secondary use of personal information.<sup>8</sup>

The provisions in the H.R. 10 which require banks, securities firms, and insurance companies disclose their privacy policies and provide consumers with the ability to opt

<sup>7</sup> Ronald L. Plesser, formerly General Counsel of the Privacy Protection Study Commission, quoted in Charles Piller, "Privacy in Peril," *Macworld*, July 1991, p. 8-14.

<sup>8</sup> See for example the 1990 & 1996 Harris-Equifax surveys; Harris-Westin survey *Commerce Communication and Privacy Online*, 1997; Culnan and Armstrong, "Information Privacy Concerns, Procedural Fairness and Impersonal Trust," *Organization Science*, Vol. 10, No. 1, p. 104-115, 1999;

out of the sharing of nonpublic personal information with nonaffiliated third parties is an important first step. However, I do not believe they are adequate for two reasons.

First, the disclosures are not required to reflect the core elements fair information practices. The principles that the disclosure must incorporate should be specified.<sup>9</sup> As discussed above, fair information practices are established norms that have been embraced in the United States and worldwide<sup>10</sup>. Individual financial institutions would retain the freedom and flexibility to create the language that they feel communicates these principles most effectively to their customers.

Second, consumers should also be offered a chance to opt out of having their personal information shared with affiliates for marketing purposes. While some have argued that by providing notice to consumers, those who object to the sharing of personal information with affiliates can choose to do business with financial institutions that do not engage in this practice. However, if large financial conglomerates become the norm as expected, consumers lose even this limited opportunity for choice. Further, there has recently emerged evidence that not all of these affiliate relationships are in the best interest of the consumer<sup>11</sup>.

It should also be noted that the failure to offer an opt out for affiliate sharing is at odds with the self-regulatory programs that America's best companies have embraced<sup>12</sup>. Consider the following examples:

- The Direct Marketing Association's "Privacy Promise" which took effect on July 1, 1999, requires all of its members who market to consumers to give notice and choice if personal information is shared with third parties and to respect consumer requests not to receive solicitations from the company or its affiliates.<sup>13</sup>

Culnan, "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing*, Vol. 9, No. 2, p. 10-19, 1995.

<sup>9</sup> See for example the language proposed by Representative Markey in his motion to recommit H.R. 10.

<sup>10</sup> See Online Privacy Alliance, "Guidelines for Online Privacy Policies," available at [www.privacyalliance.org](http://www.privacyalliance.org). The OPA is a voluntary association of approximately 80 companies and associations. See also the Federal Trade Commission's two reports to Congress, *Privacy Online: A Report to Congress*, June 1998, and *Self-Regulation and Privacy Online: A Report to Congress*, July 1999, both available at [www.ftc.gov](http://www.ftc.gov).

<sup>11</sup> See for example Robert O'Harrow Jr., Telemarketer Deals Challenged in Suit: Sale of Consumer Financial Data Assailed, *Washington Post*, July 17, 1999, p. E1.

<sup>12</sup> See for example the privacy policies for American Express ([www.americanexpress.com](http://www.americanexpress.com)) and Bank of America ([www.nationsbank.com](http://www.nationsbank.com)) which describe policies governing their information offline and online.

<sup>13</sup> Direct Marketing Association, Privacy Promise Member Compliance Guide, September 1998.



- The Online Privacy Alliance's Guidelines for Online Privacy Policies states that individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use, including the vast majority of circumstances where there is third party distribution of the information<sup>14</sup>.
- To qualify for the BBBOnline Privacy Seal, organizations must disclose the choices they provide to consumers with regard to information that is shared with affiliates or third party agents.<sup>15</sup>
- American Express has long offered its customers an easy opt out from receiving American Express offers, offers from its business partners and telemarketing solicitations. They have reported that a very small number of customers actually opt out, but by providing this opportunity, trust in the American Express brand is enhanced.

Providing an opportunity to opt out of affiliate sharing will not restrict the free flows of information so important to our economy. Information about consumer choices and behavior can still be analyzed and shared in the aggregate, minus only the information that identifies the customer. Affiliates and other third parties will also save money by not contacting people who have no interest in the products or services they are offering.

One final point needs to be made about the distinction between "public" and "nonpublic" personal information that is made in H.R. 10. The telephone book, one of the most widely available sources of public information, is a good example that people value the ability to make choices about disclosing even their name and address, and when offered choices, will exercise them. Bell Atlantic provides its customers with a range of choices about how they will be listed in its directory. These choices include not being listed at all, listing only your name and phone number, not listing your first name, being listed under a "pseudonym" (e.g. the name of your pet), or listing full name, address and telephone number. Selecting any page at random from the local directory will include listings that reflect a variety of these preferences. Consumers should be able to opt out of having their names and addresses shared for marketing purposes, even when this information is considered "public."

---

<sup>14</sup> See [www.privacyalliance.org](http://www.privacyalliance.org)

<sup>15</sup> See [www.bbbonline.org](http://www.bbbonline.org)

## Public Records

Technology has redefined the public record. Public records formerly existed as "puddles of data," manual record systems or small files or databases contained on standalone computer systems. Privacy was often protected by the effort required to access to these records. Today, advances in technology and the growth of the Internet have promoted the merging of puddles into readily accessible lakes or even oceans of personal information<sup>16</sup>. The time has come to have a national discussion about the many ways public records are used in our information society, and to examine the current balance between individual privacy and the public interest.

Similar to commercial information, public records raise the same privacy issue of unrelated secondary use that may not be governed to fair information practices<sup>17</sup>. While the Drivers Privacy Protection Act mandated notice and choice for motor vehicle records if the state elects to make the information available for incompatible purposes as defined by the law, secondary use of other types of public records are not governed by such protections.

Public opinion supports the distinction between compatible and incompatible use of public record information. The 1992 Harris-Quifax Consumer Privacy Survey asked how the public feels about individual consumer data being available in public records. The majority of the public feels that private sector use of public record information is acceptable when public is used for a compatible purpose, such as relevance to the individual's application for employment or a consumer benefit such as automobile insurance, but not when it is used for unrelated purposes. These results are shown in the table below.

---

<sup>16</sup> See *Personal Privacy in an Information Society*, the Report of the Privacy Protection Study Commission, 1977 and Willis H. Ware, "The New Faces of Privacy," *The Information Society*, Vol. 9, No. 3, p. 195-212, 1994. Ware was Vice Chairman of the PPSC and has recently argued for the need to revisit the privacy issues resulting from the automation and aggregation of public records. He stated that the PPSC never extended its dialogue to "stress the totality of public records" because public record laws and practice at that time did not reflect today's high level of automation.

<sup>17</sup> See for example, Mary J. Culnan, Prepared Statement on H.R. 3365, Driver's Privacy Protection Act of 1993, House Judiciary Committee, Subcommittee on Civil and Constitutional Rights, February 3, 1994. For example, motor vehicle records may be used for targeted marketing by drawing inferences about an individual's lifestyle based on the type of automobile they driver, whether or not they wear glasses or their height/weight ratio. None of these inferences are related to driving. Property records and court records have also been used to draw inferences for direct marketing. The Supreme Court will hear arguments on the Drivers Privacy Protection Act during its upcoming session.

Question (Base = 1254 respondents)	Generally All Right
Auto insurance companies checking the accident and driving record of a consumer applying to them for a policy	77%
Employers checking for criminal convictions when a person applies for a job	75%
Businesses checking bankruptcy and other financial records when a consumer applies to them for credit	71%
Private investigators obtaining public record information on individuals for clients	34%
Companies obtaining public record lists in order to mail people information about products and services	32%
The media obtaining and publishing public record information about people in public life or in the news	28%
A private individual obtaining public record information about another person	19%

Second, a key difference between commercial information and public records is that public record information is not collected voluntarily. For example, few adults can survive without a driver's license or an automobile, and a condition of having either is to register with the state. When the state makes this information available for unrelated uses such as marketing without an opportunity to opt out, the state is essentially placing an unfair burden on the public. This is in direct contrast to marketing use of commercial data where the individual has voluntarily "raised their hand" in the marketplace by responding to an offer of some type. No such claim may be made for all of those listed in the public records.<sup>18</sup>

Public records play an important legitimate role in our society. Providing enhanced access to public records through technology can mean more efficient government and improved service for its citizens. However, these benefits need to be balanced with privacy concerns. For example, a 1997 Harris survey found that 75% of the public see a problem with state and local governments putting public records on the Internet for easier access by all interested parties. Because different types of public records are used in different ways and raise different privacy issues, the policy discussion should proceed on a case by case basis.

<sup>18</sup> For legal arguments related to this point for motor vehicle records, see Marc Rotenberg, Brief Amicus Curiae of the Electronic Privacy Center in Support of Petitioners, *Reno v. Condon*, U.S. Supreme Court 98-1464, July 15, 1999, available at [www.epic.org](http://www.epic.org).

### Privacy and the Internet

When financial services move onto the Internet, they potentially raise a new set of privacy issues due to the interactive nature of the medium. This in addition to the privacy concerns raised by unrelated secondary use discussed above.

In the offline world, consumers leave a data trail only when they engage in a transaction: withdraw money from an ATM, use a credit card, file an insurance claim, trade securities or apply for a mortgage. On the Internet, not only can transactions be recorded, but consumers can also be tracked when they browse online, but do not engage in any transactions. When we visit a Web site, our browser provides the Web site with the URL of the previous page we visited. Cookies can be used to identify a returning visitor to a web site, even if surfers do not explicitly identify themselves.

Privacy concerns about disclosing personal information online threaten electronic commerce from reaching its full potential. As in the offline world, these concerns can be addressed if financial services firms observe fair information practices: post a comprehensive privacy policy on their Web site and subsequently ensure that their information practices conform to the policy. For example, a 1997 Harris survey found that 87% of the Internet users they surveyed had declined or had lied when asked by a Web site to provide personal information. Sixty-three percent said they would have supplied the information if the site had clearly informed them in advance how the information would be used and the consumer was comfortable with these uses. The semi-annual Georgia Tech surveys of Internet users have consistently reported similar results. It is, therefore, clearly in the self-interest of the financial services industry to observe fair information practices online.<sup>19</sup> However, if recent evidence for commercial Web sites can be extrapolated to the financial services industry, it is unlikely that the majority of financial Web sites have posted comprehensive privacy policies that reflect the core elements of fair information practices.<sup>20</sup> This situation needs to be remedied.

---

<sup>19</sup> See for example E-Loan which is a member of the Online Privacy Alliance ([www.eloan.com](http://www.eloan.com)).

<sup>20</sup>The Georgetown Internet Privacy Policy Survey found that while nearly two-thirds of consumer-oriented .com Web sites posted some form of privacy disclosure, less than 10% posted a comprehensive statement that included all core elements of fair information practices. For the full report, see [www.msb.edu/faculty/culnanm/gippshome.html](http://www.msb.edu/faculty/culnanm/gippshome.html). I am the director of the Georgetown study.

### Conclusion

Privacy concerns arise primarily when personal information collected for one purpose is reused for unrelated purposes. Privacy concerns may be addressed by observing fair information practices. This represents a win-win solution for consumers and the financial services industry as it promotes disclosure by reducing the perceived risk to the consumer while consumers retain control over their personal information. The policy question is whether this can be accomplished through self-regulation or whether legislation is be required. In either case, the same principles should apply to information gathered offline and over the Internet. However, care needs to be exercised to ensure that any regulatory solution does not threaten electronic commerce by prohibiting new Internet business models such as those where an intermediary searches on behalf of a consumer for a favorable rate for a loan.

The current Federal Trade Commission process has worked well for promoting online privacy. The FTC has convened workshops where participants represent a wide range of stakeholders, conducted research and issued periodic progress reports to Congress on the need for new privacy legislation. As a result, the private sector has mobilized and initiated several promising self-regulatory initiatives. While similar efforts may be underway in the financial services industry, I am not aware of any with the exception of the practices of a small numbers of firms who have a long-time commitment to privacy.

I recommend the Subcommittee charge the financial regulators to implement a similar process for financial services. The OCC is a promising candidate as it has held at least one workshop on financial privacy and appears to have an ongoing interest in the issue.

This concludes my statement. I would be happy to work with the Subcommittee as you address this important issue.

Responses in Writing to the Questions of Congressman Bruce F. Vento  
 by Professor Mary J. Culnan  
 [Emerging Financial Privacy Issues Hearing, July 20, 1999]

1. **What is your view of the affirmative responsibility provisions in H.R. 10 that require an institution to protect the security and privacy of consumer information? Given that the rates of consumers “opting out” are quite low, isn’t this provision more powerful in some ways as it takes no consumer action at all to be put to employ?**

Sec. 501 (a) of H.R. 10 states the policy of the Congress that all financial institutions have an affirmative responsibility to “respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” Fair Information Practices operationalize these protections. The core elements of fair information practices include the following:

- Notice about what personal information is collected and how it is used,
- Choice about how the information will be subsequently used,
- Access to the personal information they have provided
- Assurances that the organization will insure the security and integrity of personal information
- Procedures to enforce the policy and provide redress to consumers in the event the policy is violated.

As fair information practices are simply principles, alternatives exist for their implementation. For example, “opt out” and “opt in” are two approaches for implementing choice. Both provide consumers with an opportunity to exercise control over the ways their personal information is used beyond the original transaction.

H.R. 10 provides consumers with limited choices about subsequent uses of their personal information. It only requires financial institutions to provide an opt out when nonpublic personal information is to be disclosed to unaffiliated third parties. It does not require any form of choice before personal information is shared with affiliated third parties, and does not provide an opt-out for other uses of nonpublic personal information. A major shortcoming of H.R. 10 is that it does not require financial institutions to offer choice when personal information is shared with affiliates for purposes that are unrelated to completing the original transaction (e.g. cross-marketing). This is a violation of fair information practices, and is also at odds with the self-regulatory programs that have been implemented by other industries.

Prior research on privacy found that consumers are willing to disclose personal information when the benefits of disclosure exceed the risks. Observing fair information practices is good for business because it builds trust by minimizing the risks of disclosure, even when consumers choose not to invoke the choices that are offered to them (e.g. opt out). This may explain the low opt out rates: people primarily want to be assured the organization plays by rules they consider to be acceptable and will not behave in an opportunistic fashion. My own research has found that observing fair information

practices promotes disclosure, builds trust and reduces privacy concerns; my research is available at: <http://www.msb.edu/faculty/culnanm/home.html>.

Finally, should choice be implemented using “opt in” or “opt out”? Opt in requires affirmative consent while opt out allows information to be used if the consumer does not object. It is my view that a good “opt out” is an appropriate method for implementing choice when personal information is going to be used for marketing because it fairly balances the consumer’s interest in controlling how their personal information is used with the business interests that make a substantial contribution to our economy. Central to my position is the concept of a “good” opt out. In the offline world, a good opt out is easy to find, easy to understand and easy to use. It does not require the consumer to write a letter.

As an example of a good opt out, I am enclosing the “opt out” notice American Express mails to its customers and ask that it be included in the hearing record. Its strengths are the following:

- The notice is easy to find and easy to use
- It provides a detailed description of how personal information is used
- It explains how the customer benefits from these uses
- It provides multiple choices
- It allows the customer to respond by mailing back the form (American Express pays the postage) or by calling a 800-number.

In the online world, there is little difference between “opt in” and “opt out,” assuming the notice is easy to find and easy to understand. Here it is just a matter of clicking a box to reflect one’s preference. Privacy policies online should be linked from the home page and should also be accessible on all Web pages where consumers are asked to provide personal information. The FTC’s views on online privacy are available in its 1998 and 1999 reports to Congress.

**2. What (besides marketing) are other secondary or reuse applications of consumer data?**

For the purposes of this answer, I will define “marketing uses” as using consumer data to contact or solicit a consumer about products or services by any means. In addition to marketing, customer data may be used to support activities all across an organization’s value chain such as improving the operational efficiency of an organization (e.g. ensuring adequate staffing at peak periods), planning for expansion and identifying the need for additional facilities (e.g. location of new ATM machines or branches based on demand) and identifying problems or errors that need to be corrected based on customer feedback. On the Internet, clickstream data generated by customers can be used to improve the organization’s Web site. Many of these uses involve aggregated data to measure trends rather than focusing on individual or identifiable customers.

**3. Will smaller institutions, like community banks and credit unions, market on their smallness and their “better” privacy policies as a response to the**

**consolidated mega companies who would have dozens or hundreds of affiliates to share with?**

It is important that H.R. 10 does not create a playing field that disadvantages the smaller institutions. Further all financial institutions should observe fair information practices including notice about all the types or organizations with which they share personal information and choice before information is shared if the sharing is not related to completing the original transaction. The main way the smaller institutions can gain a competitive advantage from privacy is if they are required to offer choice before information is shared because they do not have affiliates while the larger firms do not have such a requirement. As I have stated previously, I believe this is bad public policy.

Smaller institutions can know their customers better, provide more personalized service and potentially have a strong trust-based relationship with their customers. However, in my opinion, this does not mean that their customers will not want the convenience of one-stop shopping for financial services that they could find at a larger financial conglomerate. Congress should ensure that the competitive playing field is level for all types of organizations including the rules for handling personal information. Fair information practices should apply uniformly across institutions independent of their size.

**4. Are there particular public records that are a problem because of their availability? Particular public information practices that are a problem? Any negative interfaces with financial data?**

Technology has increased the availability of all types of public records. Two types of public records, motor vehicle records (drivers license and automobile registration) and property records are the most problematic because of the type of personal information these records contain. For example, a drivers license includes height, weight and corrective vision information which some consider to be medical information.

Public records raise the following privacy issues.

- They are often used in ways that are incompatible with the reason for originally collecting the information. In many cases, the information (e.g. make of automobile or dwelling characteristics) is used to draw inferences about an individual's lifestyle or financial situation that serve as the basis of a marketing campaign. Individuals cannot opt out of these uses. The Drivers Privacy Protection Act provides an opt out for incompatible use of motor vehicle records, but this law was overturned. The Supreme Court will hear the case during the current session.
- Individuals often have little or no choice about having their personal information included in public records. For example, it is difficult to survive in our society without being able to drive. Further, a government I.D., typically a drivers license, is required to travel by air. For most people, a drivers license is key to being able to move freely. However, there is no public safety or "open



government” argument in favor of the marketing uses and other unrelated uses of this information described above.

Public records play important, legitimate roles in our society. When they are used for other purposes that are unrelated to the original purpose for collecting the information, fair information practices should apply. Consumers should be able to opt out of these incompatible uses.

**5. What would be an appropriate transition or phase-in period for applying new privacy policy disclosures and new restrictions on sharing of customer data?**

I have no first-hand knowledge of what would be required to implement these new procedures. I assume it would be reasonable to allow a few months at a minimum for financial institutions to develop and send disclosures to their customers, if all affected institutions have already adopted a privacy policy. Because these institutions already communicate regularly with their customers, implementation of the notice provision would involve documenting their procedures and including this notice with one of their regular mailings. The institutions would also need to insure they have posted the required disclosures on their Web sites.

More time should be allowed to implement any rules that will require changes to an organization’s information systems, particularly since the majority the information systems staff in financial institutions are currently working to address the Y2K issue.

To ensure that any new requirements are implemented in a timely fashion but at the same time do not unreasonably burden financial institutions of all types, I strongly recommend that the appropriate regulatory agency convene a workshop with industry and consumer representatives to discuss these implementation issues and to gather feedback before any rules are finalized. The workshop could be modeled after the workshop the FTC held to discuss procedures for gaining parental consent required by the Children’s Online Privacy Protection Act.

No Postage  
Necessary  
If Mailed in the  
United States



## BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 5595 GREENSBORO, NC

Postage will be paid by Addressee:

American Express  
Cardmember Mailing List Services  
PO Box 27000  
Greensboro, NC 27499-3234

PLEASE  
CONTACT  
TRAVEL  
RELATED  
SERVICES  
At American Express Company



# An Important Notice



Concerning  
Cardmember  
Privacy,  
Mailing,  
and  
Telemarketing  
Options

At American Express, we want you to understand all that the Card affords you, including the offers you receive through the mail and by telephone.

At American Express, we want you to understand all that the Card affords you, including the offers you receive through the mail and by telephone.

These offers come directly from us, from our affiliates, from establishments that accept the Card, or from other well-established companies. Each offer is carefully developed to ensure that it meets our standards. Additionally, we try to make sure that these offers reach only those Cardmembers most likely to take advantage of them.

To do this, we develop lists for use by us and our affiliates based on information you provided on your initial application and in surveys, information derived from how you use the Card that may indicate purchasing preferences and lifestyle, as well as information available from external sources including consumer reports.

We may also use that information, along with non-credit information from external sources, to develop lists which are used by the companies with whom we work.

These lists are developed under strict conditions designed to safeguard the privacy of Cardmember information.

Many Cardmembers tell us they appreciate these offers, as well as information on Cardmember benefits. However, if you no longer wish to receive these offers and information about benefits, please select one or more of the following options:

- Please exclude me from American Express mailings, including new benefits and American Express Merchandise Services catalogs.
- Please exclude me from mailings by other companies, including offers in cooperation with American Express provided by establishments that accept the Card.
- Please exclude me from lists used for telemarketing.

If you have previously informed us of your preferences, you do not need to complete this form unless you have new accounts to add, or wish to change your selections.

Please enter all of your American Express and Optima™ Card account numbers for which you would like the above options to apply:


Check here if you also wish these selections to apply to Additional Cardmembers on your account(s).

**Please note:**

- 8 to 10 weeks are generally required for your request to become effective.
- So that you receive important information about the Card, we may continue to enclose notices in your monthly account statement, and on a very limited basis, we may send you other notices from American Express.

**Please return this postage-paid mailer or call us at 800-528-4800.**

Cardmember Name *please print*

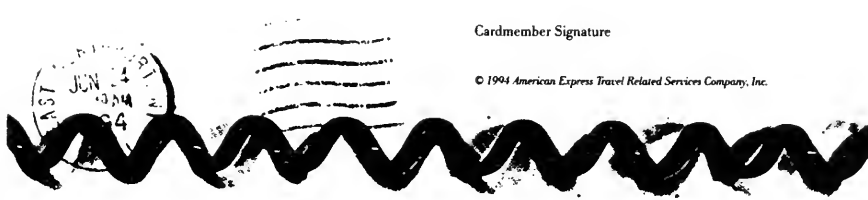
Street Address

City State Zip

Cardmember Signature

© 1994 American Express Travel Related Services Company, Inc.

model: 300 in half, rear and mail



Statement By

**Mr. Gary E. Clayton**  
President and Chief Executive Officer  
The Privacy Council

on  
**Financial Privacy**

Before the  
**Financial Institutions and  
Consumer Credit Subcommittee**  
**House Banking and Financial Services Committee**

July 20, 1999

**GARY E. CLAYTON TESTIMONY TO THE  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE  
HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES  
JULY 20, 1999**

Madam Chairwoman and members of the Committee, my name is Gary Clayton and I am the President and CEO of the Privacy Council. We are a Dallas based organization that provides legal and technical counsel regarding the complex privacy issues encountered when businesses use personally identifiable information in the course of their operations. The explosive growth of e-commerce has greatly enhanced the complexity and importance of these issues and I commend this Committee and Congress for its leadership as we search for an appropriate response. I would like to briefly discuss with you why I believe the privacy provisions of the Financial Services Act of 1999 (H.R. 10) are helpful, and what I believe the Federal government can do in the near future to protect privacy while also protecting other interests of citizens.

In the quarter century since the Department of Health and Human Services released its seminal report on privacy protections in the age of data collection, certain guiding principles have gained wide acceptance both here in the United States and around the globe. They are: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. These principles have been incorporated into a number of guidelines adopted during the last two decades, including the following: (a) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1981; (b) 1981 Council of Europe Convention No. 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data; (c) Council of Europe Recommendations on Protection of Personal Data Used for Employment Purposes, 1989; (d) UNCHR Guidelines for Regulation of Computerized Personal Data Files, 1990; and (e) International Labor Office Code of Practice for Protection of Workers' Personal Data, 1997 and (f) the European Union's Data Protection Directive 95/46/EC.

GARY E. CLAYTON TESTIMONY TO THE  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE  
HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES  
JULY 20, 1999

In my view, these principles are sound because they reflect the paramount importance of the individual freedoms and choice in American society. A privacy policy to protect our citizens should empower our citizens. Furthermore, these principles permit balance between privacy and other important societal interests, such as broad access to information, affordable quality services and the prevention of fraud and other crimes. Information and technology are fueling the growth of a dynamic new economy. The Internet is literally giving the average citizen access to information that was formerly available to only a few, thus empowering individuals to take advantage of information on investments that would not have been possible just a few years ago. Indeed, this is one of the fundamental reasons for the phenomenal growth of the U.S. economy over the last few years. Privacy policies must be cautiously crafted and implemented in a manner that does not choke off this growth and innovation.

Finally, these principles provide a framework within which we can craft a number of specific policies that differentiate between government custodians of information versus private sector custodians of information, and between the unique uses of information in one industry as opposed to another.

The privacy protections in Title V of the Financial Services Act of 1999 reflect these principles and yield a balanced initiative. Consumers are assured of both notice and choice. Notice makes it possible to evaluate whether a bank's privacy policies are aligned with their own hierarchy of interests--which include not only privacy but also cost, quality, service and security. If the bank's policies are not satisfactory, the consumer has market choice. He or she can choose a bank with policies that match their preferences. If a consumer likes everything about a bank except its policy of sharing information with third parties, he has the choice to "opt out"--and forbid the bank from sharing his personal information.

I believe these two protections give consumers the power and leverage they need in the financial services marketplace. In a different market or industry where there is little or no choice, additional regulations might be considered. But in this case, industry self-regulation, followed by observation and study, is appropriate and sufficient.

GARY E. CLAYTON TESTIMONY TO THE  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE  
HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES  
JULY 20, 1999

Section 508 of the Financial Services Act essentially adopts an observation and study approach by calling for the Secretary of the Treasury, in conjunction with the Federal functional regulators and the Federal Trade Commission, to conduct a study of information sharing among financial institutions and their affiliates. This is an important "fail-safe" mechanism. I encourage the Congress to use the study to determine whether the innovative protections in the Financial Services Act and the accompanying industry self-regulation do indeed successfully balance the several interests I have enumerated.

Section 351 of the Financial Services Act includes a right of confidentiality in medical records. It also follows the "observe and study" approach by calling for consultation between State insurance regulatory authorities and the Secretary of Health and Human Services. This consultation should serve as a conduit of information to Congress on the effectiveness or lack of effectiveness of Section 351 as implemented.

The work of the Federal Trade Commission with the on-line industry concerning privacy issues provides an example of acceptance of industry self-regulation accompanied by government observation and study. In the summer of 1998 the Commission reported to Congress that effective on-line industry self-regulation had not yet taken hold. The Commission recommended and Congress enacted limited legislation to set standards for the collection of information from children. This year the Commission has continued to monitor the on-line industry and last week issued a report noting the on-line industry's commitment to and progress toward fair information practices.

In summary, I believe the Federal government should use its resources to be a cooperative party with the private sector in the development of new and dynamic best practices regarding privacy. I wish to invite the Committee's attention to a place where only the Federal government has the resources to lead us to a satisfactory resolution. The Federal government, through the Department of Commerce, is in continuing negotiations with the European Union over the EU's Data Protection Directive. That directive threatens to diminish the role of American business and remove the European Community from the world market through the creation of a "Fortress Europe."

**GARY E. CLAYTON TESTIMONY TO THE  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE  
HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES  
JULY 20, 1999**

Under the plan, the EU would prohibit the sharing of any information relating to an identified or identifiable natural person unless certain criteria are met. The Directive also prohibits the transfer of personally identifiable data to non-EU countries that do not provide an adequate level of data protection as determined by the European Union. The European Union does not consider the United States to provide an adequate level of privacy protection.

Under the EU approach, for example, an American multinational corporation with its headquarters in New York may not be able to access data on its own employees in making management decisions on personnel. This will also mean that a company wanting to export such data to the United States will have to notify the appropriate privacy official - a privacy czar if you will - in the country where they are doing business that it intends to process personal data. The U.S. will have to adopt the EU's government-centric approach in order for the Europeans to deem our protections "adequate." Were the EU to compel U.S. businesses to meet costly and burdensome EU privacy standards, the cost to U.S. companies of compliance would run into many billions of dollars. The EU regulations do not reflect the principles of individual empowerment, balance of interests or flexibility in the face of complexity that I have suggested should govern our actions in the United States.

I encourage Congress to actively monitor negotiations with the EU to ensure that the agreement finally reached thoroughly reflects these principles.

I thank the Committee for this opportunity to testify. This concludes my prepared remarks. I look forward to your questions.





STONE INVESTMENTS, INC.

## GARY E. CLAYTON



Gary E. Clayton is the vice president, general counsel and senior privacy analyst for Stone Investments, a technology investment firm based in Dallas, Texas. Presently, Gary is responsible for Stone Investment's international and domestic advocacy efforts on initiatives for the Internet and privacy issues.

Gary is a frequent speaker on Internet issues to corporate executives and law firms. He has also participated as a faculty member for dozens of conferences on privacy and Internet issues for commercial and legal organizations. Gary has spoken on domestic and international technology and privacy issues at seminars and conferences all over the world,

including the International and National Conference Boards in Dallas, Los Angeles, Geneva and London, the Council of International Investigators in Boston, the Justice Management Institute in Phoenix, the Association of American Matrimonial Lawyers in San Juan, Puerto Rico, Richardson Technology Forum in Dallas, the Texas Bar Association convention, and numerous other conferences and councils around the world.

Articles authored by Gary have been published in *The Wall Street Journal*, *The Texas Tech Law Review* and *The Texas Lawyer* and he has been quoted by *The New York Times*, *The Financial Times of London*, *U.S. News & World Report*, *The Journal of Commerce*, *Computer Reseller News* and many other publications.

Gary received a B.S. in History and Political Science and a law degree at Louisiana State University, an M.A. in public international law and organizations at American University's School of International Service and an LL.M. in international and European business law at University of Exeter, England where he attended on a International Rotary Foundation scholarship.

For most of the past two decades, Gary has had an active commercial litigation practice focusing on commercial, technology and intellectual property disputes in Texas, Louisiana, District of Columbia and other jurisdictions. Prior to private practice, Gary served as counsel for the U.S. Army Judge Advocate General's Corp. where he was the chief trial counsel for the U.S. Southern European Task Force in Italy, Greece, Turkey and the Sinai. During that time, he was appointed as legal advisor for the United Nation's Peacekeeping Force for the Israeli-Egyptian accords.

He lives in Dallas, Texas with his wife Marsha and their three young children.

8150 N. CENTRAL EXPRESSWAY

SUITE 1901

DALLAS, TEXAS 75206

(214) 365-1900

1. Is the self-regulatory approach of the FTC satisfactory for protecting Internet privacy? Would such a framework work for financial institutions?

The Federal Trade Commission has taken the correct approach by giving industry and the market sufficient time to develop ways of protecting the privacy of individuals on the Internet. I believe that it is too early in the game for the government to rush to judgment and set rules. Europe and a number of other nations have done so and have established bureaucracies to control and regulate the gathering and use of personal information on the Internet. I do not believe that such an approach is necessary nor do I believe that in the long run it will protect individuals' privacy any better than self-regulatory efforts.

Banks have every reason to protect their customers' data. As demonstrated in the recent U.S. Bancorp case in Minnesota, failure to do so results in a public outcry and ultimately, a loss of customers. In a competitive industry like banking, financial institutions are certain to respond to the market's demand for privacy. Those that do not will lose customers.

The Federal Trade Commission's conclusion that "legislation to address online privacy is not appropriate at this time" is the right approach. The FTC has recommended instead "effective self-regulation is the best way to protect consumer privacy."

The issue of privacy is clearly growing among Americans. A recent survey by Professor Alan Westin of the Center for Social & Legal Research indicates that 94% of American consumers surveyed were concerned about a "possible misuse" of their personal information. In the United Kingdom the number was 72% and in Germany 78%. Both Germany and the United Kingdom are subject to the privacy provisions of the European Data Protection Directive.

Professor Westin's survey also revealed that 65% of Americans believe that most businesses handle customer personal information in a proper and confidential way. The highest level of confidence in the United States was for the banking industry. 77% of Americans believed that consumer banks handled their information properly. By far the lowest level of trust was for companies selling over the Internet. Of the 1,000 Americans surveyed, only 21% believed that e-commerce companies handled their personal information properly.

The simple conclusion is to say that legislation is needed or that new bureaucracies must be established to protect consumer privacy. I disagree. In Europe, the costs to businesses and consumers to implement the regulatory protection schemes are very high. Those engaged in providing privacy audits and assisting businesses have publicly stated that the financial costs are many times anything that had been projected when the legislation was enacted. Yet, as Dr. Westin's survey indicates, European consumers continue to express the

same sorts of concerns as consumers in the United States. The difference is that consumers in the European Union will have to pay for the costs of implementing the legislation whether or not they are concerned with privacy issues or not. Additionally, restrictions on data flows in Europe will almost certainly hamper such customer services as instant credit, overdraft protection, debit cards and other services that depend on the ready availability of consumer information.

In the United States and around the globe, the financial industry is experiencing rapid technological change and indeed may be one of the most beneficial areas of development for consumers. Banks have an incentive to move to online banking: the costs are considerably lower than that of traditional banking. Online banking also is providing consumers with new and more convenient ways of accessing financial services and of participating in financial markets. Almost of these new developments, however, depend upon the availability of information on the parties to the transactions. Imposing new restrictions on financial institutions at this critical juncture of development will threaten online banking activities and ultimately harm consumers.

There are serious ramifications of regulations in this area. During the Subcommittee's hearings on H.R. 10, numerous witnesses spoke of the danger of unintended consequences if Congress legislates in this area. In an area that is developing so quickly and in which market forces are driving the development of new technologies and mechanisms for protecting privacy, it is premature to implement federal legislation at this time.

There is so little consensus on how to proceed in this area because so much has yet to be determined and the technologies are changing so quickly. Unfortunately for Congress, the fact is that it will become increasingly more difficult for legislation to keep pace with the rapid change of new technology or the market. This does not mean that Congress should do nothing, however. Congress should adopt the approach of the Federal Trade Commission and continue to monitor developments in the market place. Consumers have an incredibly high level of faith in the way financial institutions handle their personal information. Congress should defer further legislation until it has been clearly demonstrated that such faith is unjustified or that financial institutions fail to provide the privacy protections demanded by the public.

Congress should encourage financial institutions to adopt privacy policies. Many financial institutions already have done so and several have appointed senior officers who will monitor the bank's compliance with good privacy practices. Congress should also encourage financial institutions to make their customers fully aware of their privacy policies. Many of these policies will operate under the numerous laws and regulations that already protect the privacy of a bank's customers. By making these policies public, customers who are

concerned with the privacy of their personal data can choose which financial institutions have acceptable privacy policies.

2. Is it appropriate to put one set of rules on financial institutions and another set of privacy rules on the Microsofts, Lockheeds and Targets of the U.S. economy?

Yes. The appropriateness of regulations is not a question of the size of the company holding the information. The issue of regulations should be determined by considerations of the sensitivity of the personal information involved, the sensitivity of the market in responding to consumer demands for privacy, and the ability of lawmakers to pass legislation without inflicting unintentional consequences that stifle new services and technologies and end up harming consumers.

One of the major criticisms of the European Union's approach to data protection is that Europe has a "one-size-fits-all" approach. They have one set of rules to be applied regardless of the economic sector involved. The United States has traditionally taken a different approach and has attempted to enact rules that govern particular market segments. This reflects recognition of the reality that information is used differently among various sectors of our economy.

One thing is common among the various companies you have listed in the question: information is and will increasingly be an essential element of the way they do business. This is particularly true as more and more American companies engage in electronic commerce. Availability of data will enhance business efficiency, reduce costs, prevent fraud and allow businesses to provide consumers with the services they will demand. Privacy rules and regulations will impede the free flow of data and potentially limit the benefits that would otherwise be available to customers.

As the Internet becomes the preferred way of doing businesses for many Americans, companies will have to face the fact that they will lose customers if they fail to respond to privacy demands. Customers who lose confidence in the way a business uses his or her personal data, whether it be a financial institution or Microsoft, will increasingly have the ability to choose other companies. In competitive industries, businesses will have to compete to provide customers with as much control over their personal data as they demand. Those that do not will lose business to those who do.

Congress should refrain from further legislation until a need is clearly demonstrated. In areas where the market fails to meet consumer demands for privacy protections, Congress may have to act but only after a consensus has formed that emerging market mechanisms are insufficient to protect consumers and their personal data.

Subcommittee on Financial Institutions and Consumer Credit  
 Committee on Banking and Financial Services  
 U.S. House of Representatives

FINANCIAL PRIVACY

Professor Fred H. Cate

July 20, 1999

Madam Chairwoman and members of the Subcommittee:

My name is Fred Cate. I am a professor of law, Harry T. Ice Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington, and senior counsel for information law at Ice Miller Donadio & Ryan in Indianapolis. I am testifying today on my own behalf, as someone who has researched, taught, and written about information law issues generally, and information privacy issues specifically, for more than a decade.<sup>1</sup>

"Privacy" is capturing legislative attention in Washington and state capitals as never before. Congress has a number of significant privacy bills—including H.R. 10<sup>2</sup>— under consideration. State legislatures are being no less attentive: in 1998, 2,367 privacy bills were introduced or carried over in U.S. state legislatures; 42 states enacted a total of 786 bills. This year has seen extensive action at the state level; New York alone has already enacted 14 new privacy laws.

These laws respond to dramatic changes in technologies which make it easier and more profitable to collect, process, and use information about individuals. And they respond to reports of mounting consumer fears about privacy. They are often popular laws. Nonetheless, I encourage you to defer additional legislation intended to protect further the privacy of financial information.

Information as Essential Infrastructure

---

<sup>1</sup>I am the author of *Privacy in the Information Age* (Brookings Institution Press, 1997); *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (Coalition for Sensible Public Records Access, 1999) (with Richard J. Varn); "The Changing Face of Privacy Protection in the European Union and the United States," forthcoming in the *Indiana Law Review*; "The European Data Protection Directive and European-U.S. Trade," *Currents*, vol. vii, no. 1, at 61 (1998); "Privacy and Telecommunications," 33 *Wake Forest Law Review* 1 (1998); "The EU Data Protection Directive, Information Privacy, and the Public Interest," 80 *Iowa Law Review* 431 (1995); and "The Right to Privacy and the Public's Right to Know: The 'Central Purpose' of the Freedom of Information Act," 46 *Administrative Law Review* 41 (1994) (with D. Annette Fields and James K. McBain). A biographical statement is attached. In compliance with House Rule XI, clause 2(g)(4), I certify that I have received no federal grant, contract, or subcontract in the preceding two fiscal years.

<sup>2</sup>Financial Services Act of 1999, H.R. 10, 106<sup>th</sup> Cong., 1<sup>st</sup> Sess. (1999).

Historically, the United States has placed extraordinary importance on the open flow of information, for good reason. As the Federal Reserve Board reported to you in 1997 in its examination of data protection in financial institutions, "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."<sup>3</sup>

My colleague, Richard Varn, Chief Information Officer of the State of Iowa, and I have just completed a report that highlights the critical roles played by just one segment of information—public record information—in our economy and society. In that report, which will be released next week at the annual meeting of the National Conference of State Legislatures, we conclude that such information constitutes part of this nation's "essential infrastructure," the benefits of which are "so numerous and diverse that they impact virtually every facet of American life. . . ." The ready availability of public record data "facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."<sup>4</sup>

I attach a draft copy of our report, which offers specific examples of the value of that information, but it is clear that, however essential the infrastructure of public record information in our society, it is only one part of the much larger infrastructure that includes the vast array of information held by financial institutions. To close off part of that infrastructure is likely to be as disruptive of our economy as closing off an interstate on-ramp or off-ramp is to traffic.

The late Anne Branscomb, author of *Who Owns Information?*, wrote: "Information is the lifeblood that sustains political, social, and business decisions."<sup>5</sup> Given the central importance of information in our economy, Congress has long hesitated before interfering with its availability. Protecting privacy inevitably impedes the availability of information and free-flow of data.

#### The Unanticipated Consequences of Restricting Information Flows

The cost of such restrictions is further magnified by the inevitable unanticipated consequences of regulating information flows in an effort to protect privacy.

---

<sup>3</sup>Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997).

<sup>4</sup>Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (Coalition for Sensible Public Records Access, 1999).

<sup>5</sup>Anne W. Branscomb, "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition," 36 *Vanderbilt Law Review* 985, 987 (1983).

This was the painful lesson of the State of Maine when it enacted legislation to protect the privacy of health records, a subject that I know is also before this Congress. The legislation, passed after two years of debate, took effect on January 1, but the legislature had to rescind this well-intentioned law 14 days later because it had the effect of keeping family members from learning whether their loved ones were in the hospital, blocking deliveries of flowers and balloons to patient rooms, and even interfering with the access of clergy to their hospitalized parishioners.

Other states have experienced similar results: it is extraordinarily difficult to close off information flows, even for the best of reasons, without imposing wide-ranging costs on individuals and institutions alike.

The likely scope and impact of unintended consequences is even greater in the context of financial information. The substantive privacy provisions of H.R. 10, which are far more moderate than some would have liked, create definitions and distinctions that are often difficult to follow, particularly when compared with federal regulation of related areas of commerce such as credit reporting. It is far from clear how the bill would apply in practice. For example, how does "personally identifiable financial information," a term that H.R. 10 uses but does not define, relate to the information regulated by the Fair Credit Reporting Act?

Similarly, H.R. 10 forbids a bank from disclosing financial information to nonaffiliated third parties unless the bank provides customers with an opportunity to "opt out" of such use, and forbids nonaffiliated third parties from redisclosing such information to other nonaffiliated third parties. The bill expressly exempts credit reporting agencies from the first limitation (on receiving information), but it is silent on whether they are subject to the second limitation (on redisclosing that information), despite the fact that only three years ago, in the 1996 amendments to the FCRA, Congress expressly exempted experience and transaction information from the scope of that law. Should H.R. 10 be enacted into law, which of these two statutes would control?

Because the privacy provisions of H.R. 10 were adopted quickly and without public hearings, there is no sense of those provisions' likely impact on the cost of financial services. That cost may be measured in terms of both lost revenue and decreased opportunities for customers. Moreover, H.R. 10 is silent on affiliate information sharing and on whether the bill would pre-empt state laws that regulate affiliate information sharing.

If the bill had gone further, as some proposed, and prohibited the sharing of financial information among affiliates, the potential ramifications would have been far greater, especially as banks increasingly rely on affiliates to provide key services to their customers. I applaud the restraint that this committee has already demonstrated. I urge you to wait before enacting additional restrictions until you and federal regulators have an opportunity to measure the impact—intended and unintended—of H.R. 10, should it be enacted into law.

#### Market Responses to Protect Privacy

In addition to the vital role played by information, and the virtual impossibility of restricting information flows to protect privacy without imposing other, unanticipated costs, I encourage you to defer further regulation because of the widespread and escalating response of financial institutions and

associations to customer privacy concerns, and the increasing availability of technological and other forms of self-help.

In this, I concur fully with the Federal Trade Commission's recommendation last week in the context of online privacy. Despite finding that "the implementation of fair information practices is not [yet] widespread among commercial Web sites," the Commission concluded that "legislation to address online privacy is not appropriate at this time,"<sup>6</sup> recommending instead that "effective self-regulation is the best way to protect consumer privacy."<sup>7</sup> The principle reflected in Chairman Pitofsky's statement—that market responses offer more tailored and effective privacy protection and impose fewer costs than legal restrictions—certainly applies to financial privacy.

In recent years we have witnessed not only an increase in concerns about privacy, but also a parallel increase in the tools available to consumers to protect their privacy and in the self-regulatory actions of industries responding to consumer demands. Moreover, there are exciting developments that are just coming into reality that promise to give consumers greater ability than ever before to express meaningful preferences for how information about them is collected and used. This is especially true in the rapidly expanding arena of online banking.

Many companies are actively competing for customers by promoting their privacy policies and practices, and with good reason: in a trust-based industry such as consumer financial services, companies cannot survive if they lose their customers' confidence. Banks have every reason to provide the privacy protections that their customers desire, because if customers don't trust banks' handling of their data, they aren't likely to trust banks' handling of their money. Moreover, in such a competitive industry, giving customers as much control over their information as they desire is likely to be an effective competitive tool. This was the calculation made by Bank of America, when it announced that it would not share customer information with nonaffiliated entities.

Ultimately, of course, if enough consumers are concerned about better privacy protection and back-up their concerns, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much we really value privacy.

---

<sup>6</sup>Federal Trade Commission, *Self-Regulation and Privacy Online* 12 (1999).

<sup>7</sup>"Self-Regulation and Privacy Online," FTC Report to Congress, Federal Trade Commission news release, July 13, 1999 (quoting Chairman Robert Pitofsky).



Clearly, these extra-legal measures for protecting privacy do not exist in a legal vacuum. Federal and state law already provides important protections and rights, ranging from those that address privacy issues explicitly, such as the Fair Credit Reporting Act, to broader legal rights that empower courts to enforce contractual promises and the Federal Trade Commission to investigate "unfair or deceptive acts or practices in or affecting commerce."<sup>8</sup>

The privacy provisions in H.R. 10 are, therefore, consistent with past legal measures and commendable in carrying out this important principle of "say what you are going to do, and do what you say you will." This requirement for disclosure and for behavior consistent with that disclosure is a fundamental underpinning of American contract and consumer law. And it is essential if consumers are to be able to make intelligent choices about the level of privacy protection they desire.

At the same time, I believe that H.R. 10 goes too far in not merely requiring financial institutions to provide customers with notice of their privacy policies and to act consistent with that notice, but by imposing certain substantive terms that must be included in those policies themselves, rather than letting consumers choose in this competitive market how much privacy protection they want and how much they are willing to pay for it.

It is not an answer to say that all the bill requires is an opportunity for individuals to opt out of nonaffiliate information sharing. Substantive legal restrictions to protect privacy impose costs on everyone, even those who not desire the heightened level of privacy protection. Moreover, those restrictions are likely to conflict with the interest of the persons whose privacy is being protected. Customer services such as instant credit in a retail store, overdraft protection on checking accounts, debit cards, and online banking all depend on the ready availability of information, often collected and maintained in advance. Substantive legal restrictions (including the opt-out provisions) may make it untenable to provide instant access to credit histories, to market overdraft protection and debit cards to appropriate customers, or to verify the identity and creditworthiness of the online shopper. When that happens, the customer is harmed, even though he or she may be willing at that moment and for that purpose, to consent to the disclosure of his or her credit information. Restrictions on information to protect privacy inevitably restrict the range of opportunities to which consumers will be given the chance to consent in the first place.

Legislation in the Face of Rapid Change

---

<sup>8</sup>15 U.S.C. § 45(a)(1) (1997).

However great the impact of H.R. 10—or any other privacy legislation—today, we should be even more concerned about its likely impact on our future. Electronic commerce is finally beginning to take off in the United States. A recent University of Texas study calculates that the Internet generated \$301 billion in revenue in the United States last year, including \$102 billion in on-line sales.<sup>9</sup> Financial services promise to be the central component of e-commerce, both because of the need to find secure ways to pay for goods and services purchased online, and because of the dramatic cost savings available when banking online. A Booz-Allen Hamilton study found that a single banking transaction costs \$1.08 at a bank branch, 60 cents at an ATM machine, 26 cents with PC banking, but only 13 cents on the Internet.<sup>10</sup>

Online financial services require reliable and accurate means for identifying the parties engaging in the transaction, verifying their consent to the deal, and transferring funds from the purchaser to the seller. Financial services and technology companies alike are racing to develop the tools to do this, but it seems unthinkable that e-commerce and online banking will work without ready access to information, just as check clearance and credit authorization services today require such access. Restricting the collection and accessing of information, as H.R. 10 and proposals for other financial privacy legislation do, threatens online banking activities in more ways than we can imagine.

Crafting clear, effective legislation in the face of such rapid change in an area as central to our economy as financial services is a daunting task. It is made even more so by the complexity of and controversy surrounding privacy issues. I know you have just lived through this with H.R. 10, which, as I have already indicated, is subject to a variety of interpretations and serious concerns about its scope and effectiveness from both sides of the free flow debate. The inclusion of medical privacy provisions in a financial services bill only magnifies those concerns. While you are often forced to take on daunting tasks, I query whether you should choose to in the face of such rapid change, so little consensus on how to proceed, and the serious and likely, even if unintended, ramifications of regulating in this area. In short, why impose a legislative solution if there is still a reasonable likelihood (and I believe there is far more than that) that industry action, self-interest, and self-regulation, existing laws, and new technologies may eliminate the need for further regulation? This is especially true given the difficulty of using legislation to keep pace with rapid technological and market changes.

The importance of our information infrastructure, the virtual impossibility of restricting information flows to protect privacy without imposing unanticipated costs, the expanding range of more sensitive and effective mechanisms for protecting privacy that are emerging in competitive markets, and the rapid change in the contexts in which financial services and products are delivered all justify a high degree of caution before creating new restrictions on information flows to protect privacy. There is certainly need for continued enforcement of existing laws to protect against inaccurate or misleading disclosures to customers, information practices that are inconsistent with an institution's agreements with its customers, or other activities that violate existing laws. Moreover, this is certainly an

---

<sup>9</sup>See <http://www.InternetIndicators.com>.

<sup>10</sup>Sharon Reier, "Battlelines Are Forming For Next 'War of Wires'," *International Herald Tribune*, Sept. 30, 1996.

area, like so many others, that requires close and continuing scrutiny to determine whether new laws are necessary.

I am not suggesting that there may never be a need for additional privacy legislation, but rather that there should be no new legislation until that need is clearly demonstrated. That would require showing that both existing laws and regulations and emerging market mechanisms are insufficient to protect consumers from clearly identified harms resulting from financial institutions' use of information about those consumers. I do not yet see evidence of such a need. Given the significant consequences of regulating information, further legislation should be deferred until that need is clearly demonstrated.

Thank you.

Attachments

## Biographical Statement

Fred H. Cate is a professor of law, Harry T. Ice Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington, and senior counsel for information law in the Indianapolis law firm of Ice Miller Donadio & Ryan.

He specializes in information law and is the author of many articles and books in this area, including *Privacy in the Information Age*, which received Honorable Mention as the Association of American Publishers Professional/Scholarly Publishing Division Best New Book in Law 1997, and *The Internet and the First Amendment: Schools, and Sexually Explicit Expression*, both of which were selected for the 35th annual *Choice Outstanding Academic Books* list by the Association of College and Research Libraries. He is the editor of *Visions of the First Amendment for a New Millennium*.

A frequent speaker before professional and industry groups on matters relating to privacy and the ownership and control of information, Professor Cate is vice chair of the American Bar Association Section on Health Law's Electronic Communications and Privacy Interest Group and a member of the Privacy Exchange Advisory Board. He has testified before Congress on privacy in electronic communications, directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the Department of Health and Human Services' Working Group on Intellectual Property in Networked Health Information, chaired the American Association of University Professors' Intellectual Property Committee, and served as a member of Indiana Governor Frank O'Bannon's Public Access Task Force and of the U.S. Congress Office of Technology Assessment's panel of experts on Global Communications Issues and Technology and panel of reviewers on International Money Laundering. He served as a senior fellow and director of research and projects of The Annenberg Washington Program in Communications Policy Studies; he directed the Program's project on Privacy and the Public Interest, among other initiatives.

Professor Cate writes widely for the popular press and has appeared on CNN, PBS, and many local television and radio programs. In 1998 he hosted WTU's congressional candidate debates. He received his J.D. and his A.B. with Honors and Distinction from Stanford University. Prior to joining the faculty at Indiana University, he practiced in the Washington, D.C. office of Debevoise & Plimpton. A member of the board of trustees of Phi Beta Kappa Associates, Professor Cate is listed in *Who's Who in American Law*.

Professor Cate can be reached at the Indiana University School of Law—Bloomington, 211 South Indiana Avenue, Bloomington, IN 47405, telephone (812) 855-1161, facsimile (812) 855-0555, e-mail [fcate@indiana.edu](mailto:fcate@indiana.edu).

# **The Public Record:** Information Privacy and Access

---

*A New Framework  
for Finding the Balance*

Fred H. Cate and Richard J. Varn

Copyright © 1999 Fred H. Cate and Richard J. Varn

*Printed in the United States of America*

Permission is granted for reproduction of all or part of this document, provided that appropriate attribution is given.

Recommended citation: Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (1999).

Additional copies of *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* are available without charge from the Coalition for Sensible Public Records (CSPRA):

CSPRA  
1200 New Hampshire Avenue, NW  
Suite 440  
Washington, DC 20036  
[www.cspra.org](http://www.cspra.org)

# **The Public Record:** Information Privacy and Access

---

*A New Framework  
for Finding the Balance*

Fred H. Cate and Richard J. Varn

## About the Authors

Fred H. Cate is Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute at the Indiana University School of Law–Bloomington, and Senior Counsel for Information Law in the Indianapolis law firm of Ice Miller Donadio & Ryan.

Richard J. Varn is Chief Information Officer of the State of Iowa, on leave from the University of Northern Iowa, and President of RJV Consulting.

The development and distribution of this paper was funded by the Coalition for Sensible Public Records Access (CSPRA). The members of the Coalition are: Acxion Corporation, Donnelley Marketing, The Dun & Bradstreet Corporation, Equifax Inc., Experian, First American Real Estate Solutions, Lexis Nexis, The Polk Company, and Trans Union.

The authors alone are responsible for its contents.



## Executive Summary

The open public record system has been the mainstay of the U.S. democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports. The American open public record allows citizens to oversee their government, facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want. As the Federal Reserve Board reported to Congress in the context of financial information: *"[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."*

The public record also raises concerns about information privacy. It is no exaggeration to say that access to and privacy of public records about individuals are virtually always in tension. Recently, however, pressures from European regulators and growing concern over the computerization of data have heightened both the importance and the difficulty of balancing access and information privacy. The very technologies, such as the Internet, that expand opportunities for easy, inexpensive access to public records also increase the ability of the government and citizens to search and collect disparate pieces of data to "profile" individuals, thereby heightening concerns about personal privacy.

The number and complexity of the issues surrounding public records make impossible the implementation of bright-line rules for balancing access and information privacy. Instead, policymakers need a framework to evaluate when and how the law should protect privacy and access interests and how to balance the maintenance of the essential public records infrastructure with legitimate concerns about harms that may result from inappropriate use. Balance is the key.

Decades of legislative, administrative, and judicial experience suggest that the following twelve principles should help guide the process of balancing access and information privacy:

**"Open access to public records is a cornerstone of American democracy. Such access is central to electing and monitoring public officials, evaluating government operations, and protecting against secret government activities. Open access recognizes that citizens have a right to obtain data that their tax dollars have been spent to create or collect."**

"More than a century ago Supreme Court Justice Louis Brandeis, perhaps best known for his ardent defense of the 'right to be let alone,' also argued that '[i]f the broad light of day could be let in upon men's actions, it would purify them as the sun disinfects.' He proposed a 'companion piece' to his influential *Harvard Law Review* article, 'The Right to Privacy,' on 'The Duty of Publicity.'"

1. **Policymakers Should Identify and Evaluate Conflicting Interests**—Decisions regarding privacy and access inevitably affect and are affected by other important interests. It is therefore essential that any policymaking process identify and examine those interests carefully to determine how they are implicated by a proposed law or regulation and to what extent they can—and should—be accommodated.
2. **Privacy Solutions Must Respond Reasonably to Defined Problems**—Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy.
3. **Limits on Access to Protect Privacy Should be Effective and No More Restrictive Than Necessary**—The accommodation between access and privacy needs to be carefully crafted, so that we continue to permit as much access as possible without unnecessarily invading privacy. In no event should limits be imposed on access to, or use of, public record information to protect privacy if those limits will not in fact be effective in solving identified problems. Moreover, the government should not impose broad limits on access to protect information privacy where effective, extra-legal mechanisms exist that permit a more sensitive and individualized balancing of access and privacy interests.
4. **Privacy Interests are Limited to Personally Identifiable Records**—Access to government records that do not identify individuals should not be restricted on the basis of protecting privacy. Anonymous and pseudonymous records pose no meaningful privacy threat.
5. **Enhancing State Revenue is Not a Privacy Problem**—The government should not use privacy claims as a pretense for raising revenue, enhancing the competitive position of state-published information products, or restricting access to information for other purposes.
6. **Public Information Policy Should Promote Robust Access**—Information policy should facilitate as much access as possible without harming privacy interests.
7. **There Should Be No Secret Public Records**—The public should be able to easily discover the existence and the nature of public records and the existence to which data are

accessible to persons outside of the government. In many cases, it may be desirable and appropriate for the government to inform citizens about who is using their public records and for what purposes. Obviously, access to records is not appropriate in all cases, but this principle recognizes that access serves broad and important purposes.

8. **Not Every Privacy/Access Issue Can be Balanced—** Despite the importance of balancing, it is not appropriate in every case. The courts have established that there are some instances where the societal interest in access is so great that it trumps all privacy concerns. Similarly, the privacy of some types of records is of such importance to our society that it outweighs access interests.
9. **Systems For Accessing Public Records and, Where Appropriate, Controlling Their Use Should Not Be Burdensome—** The mechanisms for accessing the public records and for allowing individuals to protect the privacy of records concerning them should be easily accessible and no more burdensome than necessary.
10. **Information Policy Must Ensure the Security of the Public Record Infrastructure—** The government must ensure that public records are protected from unauthorized access, corruption, and destruction.
11. **Education is Key—** An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions. Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues.
12. **The Process for Balancing Access and Information Privacy Should Be Sound—** Government should have a process for balancing access and information privacy issues that is informed, consistent, and trusted. This process should be in place before one evaluates any new access or privacy issues. The process should draw heavily on expertise and existing data, involve as many of the affected parties as possible, apply these principles faithfully, focus on real and effective solutions, and provide for the automatic termination and/or frequent re-examination of those solutions to ensure their effectiveness and precision in the face of fast-changing technologies.

**“What is needed today more than ever is a meaningful way of thinking sensitively and practically about ways of better protecting the privacy interests of citizens, without unnecessarily compromising access to public record information and the broad benefits such access brings. Balance is the key.”**

Neither information privacy nor access is an absolute. The goal of policymaking should be to create and apply rational privacy and access policies as efficiently and fairly as possible. This is, of course, not always possible. There are times when the society will reject a perceived intrusion that has great benefit and accept a substantial intrusion that has little benefit. The difficult challenge for policymakers is to pay attention to the concerns of constituents while at the same time seeking to educate them about the costs and benefits and the intended and possible unintended consequences of proposed regulations. This challenge is made all the harder and all the more necessary by the rapid evolution of information technologies and societal attitudes.

We must think clearly and precisely about the values served by access and privacy. We must consider the extent to which the public actually and reasonably expects that given information in the public record will be or should be kept private. Finally, we must determine whether targeted and effective protections for privacy can be constructed without denying completely the public's access to information. The cost of doing any less is real, considerable, and will be borne by us all.

**“The law has traditionally balanced access and data privacy by providing for disclosure of all information held by the government, except where such disclosure would offend a specific, enumerated privacy interest.”**

## Introduction

The open public record system has been the mainstay of our democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports. Over the past 35 years, however, the increasing computerization and expanding volume of, and ease of access to, public records have raised fears about their misuse. The number and complexity of the issues surrounding public records make impossible the implementation of bright-line rules for balancing access and information privacy. Instead, policymakers need a framework to evaluate when and how the law should protect privacy and access interests and how to balance those interests when they conflict.

This paper suggests such a framework for policymaking that balances the maintenance of the essential public records infrastructure with legitimate concerns about harms that may result from inappropriate use. (For possible ways of categorizing public records, see the Public Records Classification Options in Appendix A.) The paper draws on an extensive review of information privacy and access literature, economic and legal research, interviews, and the diverse experience of the co-authors. In the three sections that follow, we discuss (1) the value of public records and why accessibility must be balanced with legitimate privacy concerns, (2) the principles that should guide that balancing process, and (3) the elements of that process itself.

This discussion focuses exclusively on *public* policymaking. Many of the substantive and procedural principles that follow would also apply to policymaking by private organizations; in fact, many businesses and not-for-profit organizations recognize the necessity for balancing access and information privacy interests and reflect that recognition in self-regulatory codes and internal policies. Many private institutions have in place processes, similar to those that we recommend below for government policymakers, for reconciling access and information privacy interests.

Despite these similarities, there are critical distinctions between government and private policymakers: Only the government exercises the constitutional power to compel

**“It is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy.”**

**—Federal Reserve Board**

disclosure of information and to impose civil and criminal penalties for noncompliance, only the government collects and uses information free from market competition and consumer preferences, and only the government is constitutionally obligated to avoid obstructing information flows and to facilitate the participation of all citizens in democratic self-governance. Therefore, we confine our analysis to balancing access and information privacy issues in the public arena.

## Access and Privacy

While the value of information privacy is widely accepted and is the subject of numerous recent articles and books, there has been virtually no attention to the value of an open public record. A balance between demands for privacy and the need for access to public records is impossible to achieve without a better understanding of the important role that accessible public information fills. This section, therefore, discusses the value of the public record infrastructure and the tension between access and data privacy. Later sections address the principles that should guide efforts to resolve that tension and the process for policymaking in this area.

### The Essential Infrastructure of Public Records

An essential infrastructure, when effective, is often ignored. We take it for granted. We assume it will work and it disappears from our thoughts. Yet when it is missing or unavailable, only then do we begin to realize how much we depended on it and how it is integrated into many of the things we need and do daily. Anyone who has experienced an extended power outage has had this kind of realization. Similarly, the overarching value of an open records infrastructure is that people and systems assume it will be there and depend on it for a wide variety of activities.

Open access to public records is a cornerstone of American democracy. Such access is central to electing and monitoring public officials, evaluating government operations, and protecting against secret government activities. Open access recognizes that citizens have a right to obtain data that their tax dollars have been spent to create or collect.

The value of this essential infrastructure, however, extends far beyond the government. Its benefits are so numerous and diverse that they impact virtually every facet of American life, to

**In 1998 public record information “assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.”**

**—FBI Director Louis Freeh**

the extent that we frequently take the benefits for granted. Consider just a few of the essential roles that open public records play:

- Access to public record information provides an important foundation for U.S. capital markets, the most vibrant in the world. The ability to grant credit speedily and appropriately depends on ready access to information about consumers collected in part from the public record. As a result, even major financial decisions are often made in a matter of minutes or hours, instead of weeks or months, as is the case in most other countries.<sup>1</sup> Finally, public records have helped democratize finance in America, meaning that many economic opportunities are based on what you have done and can do instead of who you are and who you know.
- This country's open public record system significantly reduces the cost of credit because the information that credit decisions depend upon, drawn in part from the public record, is assembled routinely and efficiently, rather than being recreated for each credit decision. As a result, American consumers save \$100 billion a year because of the efficiency and liquidity that information makes possible.<sup>2</sup>
- Journalists rely on the public record every day to gather information and inform the public about crimes, judicial decisions, legislative proposals, government fraud, waste, and abuse, and countless other issues.
- Law enforcement relies on public record information to prevent, detect, and solve crimes. In 1998 the FBI alone made more than 53,000 inquiries to commercial on-line databases to obtain a wide variety of "public source information." According to Director Louis Frech, "Information from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."<sup>3</sup>
- Public record information is used to locate missing family members, heirs to estates, pension fund beneficiaries, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought.<sup>4</sup>

**“Commercial users and resellers of public record data improve upon that information by updating it, correcting inaccuracies, and then providing it back to the governmental custodians of the public record.”**

**“Reducing access to public information poses specific and grave risks to the U.S. economy and to the provision of services and products that the public values and has come to expect.”**

- Open public records help identify victims of fraud or environmental hazards; save lives by locating owners of recalled automobiles and blood, organ, and bone marrow donors; and protect consumers from unlicensed professionals and sham businesses.
- Businesses rely on public records to choose facility locations, clean up or avoid environmental hazards, schedule the manufacture of consumer durable goods, reduce costly inventory, and prepare economic forecasts.
- Researchers use public information for thousands of studies each year concerning public health, traffic safety, environmental quality, crime, prisons, governance, and a vast array of other subjects.
- Some check verification services use state motor vehicle records to help combat the 1.2 million worthless checks passed every day. One such service used that public record data to verify or warranty \$19 billion worth of consumer checks paid to more than 200,000 businesses last year, improving the speed and accuracy of check acceptances, fighting identity theft, and reducing check fraud.
- Cable companies and public utilities also use motor vehicle records to verify information about new customers, thereby helping people who have yet to develop credit histories establish new service.
- Our entire system of real property ownership and nearly all real estate transactions have long depended on public records.<sup>5</sup> These records are used to confirm that the property exists, its location, and its defined boundaries. Buyers, lenders, title insurers, and others use these records to verify the title owner. Mortgages, many legal judgments, and other claims against real property cannot be collected without reference to public records.
- Commercial users and resellers of public record data often update them, correct inaccuracies, and then provide the improved version back to the governmental record custodians. They also greatly reduce the volume of inquiries that could otherwise overwhelm a government agency by providing services, Internet sites, and other means to access public records.<sup>6</sup>
- More than two-thirds of U.S. consumers—132 million



adults—take advantage of direct marketing opportunities each year.<sup>7</sup> Public record information helps sellers accurately and efficiently identify consumers likely to be interested in a given product or service.

In sum, the American open public record allows citizens to oversee their government, facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want. As the Federal Reserve Board reported to Congress in the context of financial information: “[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy.”<sup>8</sup> Yet, it is in the creation of these benefits that many information privacy concerns arise.

### The Tension Between Access and Information Privacy

“Privacy” is the subject of many varied definitions and valuations, but it is clear that privacy of information—the interest of individuals in controlling access to and use of data about themselves—serves many essential roles in the growth and development of us as individuals and in our participation in government, commerce, and society. Much of the value of information privacy is abstract. As a result, it is often difficult for political and judicial processes to examine that value, because it varies so greatly according to the individual, the situation, and the benefit received for the privacy lost. Nevertheless, in balancing privacy and access, these intangibles must be considered.

There is also a demonstrable value to data privacy. The free flow of information and the value it represents is dependent in part on privacy policies that engender the necessary level of trust on the part of the citizenry. People must believe that their best interests or those of the society are being promoted by the use of public records. If not, they will avoid or subvert the public records systems whenever possible. Moreover, they may succeed in advocating for restrictive information privacy laws without regard for the value that access provides. It is only in the balancing of privacy and access that we can determine their net value and thereby identify the best policies and processes.

It is no exaggeration to say that access to and privacy of public records about individuals are virtually always in tension. That tension is not new. More than a century ago Supreme Court Justice Louis Brandeis, perhaps best known for his ardent defense of the “right to be let alone,” also argued that “[i]f the

**“American consumers save \$100 billion a year in mortgage payments because of the efficiency and liquidity that public record information makes possible.”**

broad light of day could be let in upon men's actions, it would purify them as the sun disinfects." He proposed a "companion piece" to his influential *Harvard Law Review* article, "The Right to Privacy," on "The Duty of Publicity."<sup>9</sup> The tension between access and privacy is particularly acute in the United States because of the critical role that both access and information play in our system of government and in our markets. As noted above, the issue is especially important because of the power of the government to compel disclosure of information and the fact that individuals have few alternatives but to comply: The market, which can reflect consumer demand for privacy protection, does not apply to most information processing by the government.

Lawmakers have recognized in cases such as medical records that the important privacy interests of individuals must on occasion temper the constitutional commitment to the free flow of information. Disclosure of some information possessed by the government may reveal intimate details of individuals' private lives without providing any significant public benefit. In such situations, the government appropriately restricts access or requires that identifying details be removed from the information before it is released.

The law has traditionally balanced access and data privacy by providing for disclosure of all information held by the government, except where such disclosure would offend a specific, enumerated privacy interest. This is true of virtually all state and federal public records laws. The federal Freedom of Information Act, for example, requires disclosure of all records other than (1) "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," and (2) records compiled for law enforcement purposes "to the extent that the production of such [information] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."<sup>10</sup> Under the FOIA, these records may be withheld if the agency believes that the privacy risk justifies it. The laws of the states and the District of Columbia follow a similar pattern: *disclosure is the rule, privacy is an exception.*

Laws applicable to the private sector reflect a similar balance. The Fair Credit Reporting Act, which for almost three decades has established the regulatory framework according to which consumer information is collected and used in the United States, permits the broadest possible access and use of public record information, subject to specific but vital protections for consumer privacy.<sup>11</sup>

**"The very technologies, such as the Internet, that expand opportunities for easy, inexpensive access to public records also increase the ability of the government and citizens to search and collect disparate pieces of data to 'profile' individuals, thereby heightening concerns about personal privacy."**

To respond to privacy concerns, many private organizations that use public information offer important privacy protections of their own. For example, the Direct Marketing Association operates the Mail Preference Service and the Telephone Preference Service. With a single request to each, it is possible to be removed from DMA-member company mailing and telephone solicitation lists.<sup>12</sup> Similarly, many of the major companies that provide information on individuals, much of which is drawn from public records, have agreed to abide by Individual Reference Services Group Principles. These principles not only establish privacy protection standards, but also require annual compliance audits by third parties and a commitment not to provide information to entities whose practices are inconsistent with the IRSG Principles.<sup>13</sup>

Today, however, pressures from European regulators and growing concern over the computerization of data have heightened both the importance and the difficulty of balancing access and information privacy. The very technologies, such as the Internet, that expand opportunities for easy, inexpensive access to public records also increase the ability of the government and citizens to search and collect disparate pieces of data to "profile" individuals, thereby heightening concerns about personal privacy. While there are a growing number of concerns related to actual uses and abuses of public records (*e.g.*, identity theft), many privacy concerns are hypothetical or mythical. They reflect fear of the unknown rather than specific harms, or are about privacy in general and only nominally related to public records. Such fears cannot be dismissed out of hand, but care must be taken not to overvalue them in the balancing process.

What is needed today more than ever is a meaningful way of thinking sensitively and practically about ways of better protecting the privacy interests of citizens, without unnecessarily compromising access to public record information and the broad benefits such access brings. Balance is the key.

**"The goal of policymaking should be to create and apply rational privacy and access policies as efficiently and fairly as possible."**

## Principles for Policymaking

What principles should guide the process of balancing public access with information privacy? Decades of legislative, administrative, and judicial experience suggest that the following twelve principles should help guide the process of balancing access and information privacy:

1. Policymakers Should Identify and Evaluate Conflicting Interests

Decisions regarding privacy and access inevitably affect and are affected by other important interests. These interests are often socially valuable and deeply held. It is therefore essential that any policymaking process identify and examine those interests carefully to determine how they are implicated by a proposed law or regulation and to what extent they can—and should—be accommodated.

In addition to the broad concepts of “privacy” and “access,” those interests often include, but are not limited to, concerns about:

- **Equality**—Equal and open access to public records helps level the playing field in such endeavors as issue advocacy, lobbying, and elections. It also gives small and start-up businesses access to some of the same databases as large and established players.
- **Freedom**—Public records about the functioning of government, private individuals, and companies can be used to keep them in check so they do not impinge on the rights of others.
- **Participation**—The more people know about their world and about government in particular, the greater the likelihood that they will increase the quantity and quality of their contributions to participatory and representative democracy.
- **Security**—Public record security and integrity systems must be adequate to the task or their failure will defeat the goals of both privacy and access, cause explosive public reactions, and create governmental liability.
- **Economic Opportunity**—A substantial portion of the current economy is in part dependent on the free flow of public records and limiting their use or availability will have economic consequences. Moreover, public and private records are the raw materials for the emerging economy and for the knowledge revolution of the Information Age.

**“Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy.”**

- **Quality of Life**—The use of information systems can free people from rote tasks and greatly speed transactions. Getting the amount of privacy one needs, however, also may affect quality of life.
- **Intangible Values and Uncertain Fears**—A catchall value for things people like and dislike. Often we dress up our likes and dislikes in more eloquent terms, but often decisions and opinions are really based on this simple amalgamation of our feelings.
- **Efficiency**—Efficient access to public records saves time, resources, and money. Without complete and reliable information, much of the benefit of information technology cannot be realized. However, we can also be so efficient as to impinge on individual freedoms.
- **Fairness**—Is the process by which a law or rule is enacted, or by which a decision is reached, fair, and is the outcome fair to all of the parties involved?

As this list suggests, identifying and evaluating the interests at stake when balancing privacy and access are not easy tasks, but they are essential if the outcome of the process is to be effective, efficient, in the public's interest, and fair.

## 2. Privacy Solutions Must Respond Reasonably to Defined Problems

Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy. The Supreme Court has long asked in the context of various constitutional issues, such as Fourth Amendment challenges to government searches and/or seizures: What expectation of privacy is implicated by access and how reasonable is that expectation? When evaluating wiretaps and other seizures of private information, the Court has inquired into whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experience and widely shared community values.<sup>14</sup>

The inquiry regarding the reasonableness of the privacy concern should take into account three specific issues: (1) the sensitivity of the information disclosed; (2) the use to which the information is to be put; and (3) privacy

**“American consumers save \$100 billion a year in mortgage payments because of the efficiency and liquidity that public record information makes possible.”**

protection afforded similar information in the past. These inquiries help prospectively arrive at a common-sense value on the privacy side of the access-privacy balance.

Furthermore, the solution should go no further than is necessary to solve the problem: Access should be limited no longer and to no more data than necessary to protect privacy. Laws that purport to stop a harm to privacy but are ineffective harm both privacy and access. Such laws at once constitute an empty promise and a restraint on openness and freedom of information.

### 3. Limits on Access to Protect Privacy Should be Effective and No More Restrictive Than Necessary

The accommodation between access and privacy needs to be carefully crafted, so that we continue to permit as much access as possible without unnecessarily invading privacy. For example, both access and privacy interests might be served by delaying access to certain law enforcement records until a pending investigation is completed. In other cases, removing (known as "redacting") particularly sensitive information from documents otherwise made public might protect the individual's privacy interests and be preferable to denying access altogether. In no event should limits be imposed on access to, or use of, public record information to protect privacy if those limits will not in fact be effective in solving identified problems.

Government should not impose broad limits on access to protect information privacy where effective, extra-legal mechanisms exist that permit a more sensitive and individualized balancing of access and privacy interests. The development of privacy seals and certification programs, anonymizing software, user-determined browser privacy settings, prominent privacy policies, industry codes of conduct, and technologies that allow persons to opt out of specified uses of some types of government records are examples of market responses to privacy concerns generally that diminish the need for government action by allowing individuals to protect effectively the privacy of data about them. Clearly, these and similar developments will not eliminate the need for government attention to information privacy, but the number and variety of these initiatives, and the speed with which they are emerging, suggest that they may supplant the need for at least some government actions to protect information privacy.

**"While there are a growing number of concerns related to actual uses and abuses of public records, many privacy concerns are hypothetical or mythical . . . . Such fears cannot be dismissed out of hand, but care must be taken not to overvalue them in the balancing process."**

#### 4. Privacy Interests are Limited to Personally Identifiable Records

Access to government records that do not identify individuals should not be restricted on the basis of protecting privacy. Anonymous and pseudonymous records pose no meaningful privacy threat. Aggregate data can be used in ways offensive to the privacy concerns of some, but by far these concerns have been best addressed by market-based solutions and private sector codes of conduct. If government action is considered, it should be aimed at the behavior of the offenders and not the records themselves.

#### 5. Enhancing State Revenue is Not a Privacy Problem

The government should not use privacy claims as a pretense for raising revenue or enhancing the competitive position of state-published information products. This principle does not suggest that the government cannot seek to recoup the marginal or even the operational cost of providing records. But levying excessive charges on citizens to use a public infrastructure that is already paid for with tax dollars is wrong. Moreover, the government should not use claims of protecting privacy as a justification for restricting access to information for other purposes. This principle would seem to many so obvious as to not warrant stating, but many calls for privacy protection today are in fact seeking protection from other harms or are unrelated schemes for generating revenue.

#### 6. Public Information Policy Should Promote Robust Access

Information policy should facilitate as much access as possible without harming privacy interests. The more robust the flow of data, the more robust the information infrastructure that supports both democratic processes as well as growth of our economy. This reflects the constitutional importance of open public records and the law in most U.S. jurisdictions today: access is presumed unless a specific privacy exemption applies. It also reflects the importance of the public record infrastructure to our polity and our economy. As noted above, it is often possible to target specific privacy harms and leave the public record infrastructure largely intact.

**“The development of privacy seals and certification programs, anonymizing software, user-determined browser privacy settings, prominent privacy policies, industry codes of conduct, and technologies that allow persons to opt out of specified uses of some types of government records are examples of market responses to privacy concerns generally that diminish the need for government action by allowing individuals to protect effectively the privacy of data about them.”**

## 7. There Should Be No Secret Public Records

An informed citizenry is essential to all checks and balances systems and that includes public record systems. The public should be able to easily discover the existence and the nature of public records and the existence to which data are accessible to persons outside of the government. In many cases, it may be desirable and appropriate for the government to inform citizens about who is using their public records and for what purposes.

Obviously, access to records is not appropriate in all cases (one notable exception in many jurisdictions is investigative files before a criminal case is brought), nor will it always be feasible or advisable to provide information to citizens about the uses made of their records. But this principle recognizes that access not only serves broad social purposes, but also helps build citizen confidence in the public record system, improve the accuracy of public records, helps sharpen citizen understanding of privacy and access implications of the uses of their records so that they may respond appropriately, and contributes to educating all of us about the actual costs and benefits of public record access.

## 8. Not Every Privacy/Access Issue Can be Balanced

Despite the importance of balancing, it is not appropriate in every case. The courts have established that there are some instances where the societal interest in access is so great that it trumps all privacy concerns. For example, Congress recognized the overriding importance of access, irrespective of the significant privacy interests at stake, when it passed Megan's Law, requiring states to make publicly available the records of convicted child sex offenders for at least ten years after their release from prison.<sup>15</sup> Congress believed that the societal interest in access to the record overwhelmingly outweighed the privacy interests, however great, of the convicted sex offenders. In other cases, information must be public to effectuate the public policy reasons for collecting it in the first place. One example of such a record is bankruptcy filings so that creditors have the opportunity to protect their interests and future creditors can accurately assess risk.

Similarly, the privacy of some types of records is of such importance to our society that it outweighs access interests. Use of certain types of records, such as medical or individual tax records, causes such significant demonstrable

**“Information policy should facilitate as much access as possible without harming privacy interests. The more robust the flow of data, the more robust the information infrastructure that supports both democratic processes as well as growth of our economy.”**



harms that our society rejects that use even when there is a substantial desirable benefit. Productive use of other types of records causes such a visceral reaction that we restrict that use, as demonstrated by the recent outcry over digital driver's license photos. However, one must exercise caution in the application of this principle, as there are many false positives of this kind of reaction caused by sensationalistic journalism and unscientific or biased polling. It is also true that in most cases where a visceral reaction, rather than evidence of specific harms, prompts legislative action, that reaction precedes any understanding of the benefit of the use of the record so no true balancing process was used. Ultimately, policymakers must decide whether the harms are sufficiently clear and severe or the reaction sufficiently genuine and widespread to conclude that it is in the best interests of state or nation to close access to the public record.

9. Systems For Accessing Public Records and, Where Appropriate, Controlling Their Use Should Not Be Burdensome

The mechanisms for accessing the public records and for allowing individuals to protect the privacy of records concerning them should be easily accessible and no more burdensome than necessary. Information technology systems are emerging that may allow persons to opt out of specified uses of some of their government records. These important systems should not be exempt from the process of balancing the range of interests in the record against the privacy interests of the individual. Moreover, these systems can be costly to run and government must account for this as a spending priority *and* a societal concern. It must balance the cost of such privacy and who benefits against the other priorities of the government, the public, and of those parties directly affected by the loss of access. In using this test it is rarely, if ever, feasible or justifiable to require a person to affirmatively determine the uses of their non-confidential records (known as opting in). This would involve permissions from each of person in the 100 million households in America for each record and/or for each use. The process of responding to countless requests for permission would make the solution worse than the problem.

**Drivers' Privacy Protection Act**

**Federal law currently requires states to restrict access to drivers' information, although this law has been struck down by the U.S. Court of Appeals for the Fourth Circuit on constitutional grounds. Application of this framework calls into question why Congress singled out drivers' information to withdraw from the public record. Motor vehicle registrations reveal little, if any, sensitive information and no more than property tax records, which are presumptively accessible to the public. Moreover, the law was enacted in response to the stalking and murder of actress Rebecca Schaeffer, and its stated purpose was to prevent stalking—an activity already prohibited in most states. And the law permits broad exceptions, including one for private investigators, the very source of the reports used to track down and kill Schaeffer.**

#### 10. Information Policy Must Ensure the Security of the Public Record Infrastructure

The government must ensure that public records are protected from unauthorized access, corruption, and destruction. Public record security and integrity systems must be adequate to the task or their failure will defeat the goals of both information privacy and access.

#### 11. Education is Key

An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions. Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues. The more policymakers and the citizenry know about this issue, the more accurate and satisfying the balancing process will become.

#### 12. The Process for Balancing Access and Information Privacy Should Be Sound

Government should have a process for balancing access and information privacy issues that is informed, consistent, and trusted by all parties. This process should be in place before one evaluates any new access or privacy issues.

Neither information privacy nor access is an absolute. The goal of policymaking should be to create and apply rational privacy and access policies as efficiently and fairly as possible. This is, of course, not always possible. There are times when the society will reject a perceived intrusion that has great benefit and accept a substantial intrusion that has little benefit. There are those who will fight against the secondary use of a government record and will give the same information away on a warranty card or in exchange for a “free” service or product. The difficult challenge for policymakers is to pay attention to the concerns of constituents while at the same time seeking to educate them about the costs and benefits and the intended and possible unintended consequences of proposed regulations. This challenge is made all the harder and all the more necessary by the rapid evolution of information technologies and societal attitudes.

**“An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions.”**

## The Policymaking Process

We have thus far discussed why we should be concerned with balancing access and privacy and what principles should guide that balancing process. Now, we turn to the process itself by which we seek to accommodate privacy and access.

Information policy committees, agencies, and officers that have the benefit of experience and training in this field should exist at each level of government. Moreover, these persons and entities need to be structured to provide the opportunity to balance privacy and access concerns. Where individuals or offices cannot represent both sides of this equation, the policymaking process should be modified to reflect the values of both privacy and access to give the decision-makers the context for striking the balance between them. If, for example, it is considered necessary to have a Privacy Advocate, then there should also be an Access Advocate. Preferably their respective contributions are shared with other neutral experts who seek the proper balance between the two perspectives.

Once established, information policy entities can begin to choose their decision-making models to sort through these complicated issues. This should begin with the steps in the process. Each step in this process can determine whether a record is completely public for any uses, public in whole or in part and limited in its uses, or confidential.

### A Proactive Policymaking Model

This suggested model, which focuses on proactively balancing the promotion of access and the protection of privacy at the many stages of the decision-making process, begins with specialized information policy officers or entities applying the basics of good public policy. Within the steps described below, these actors will arrange the values on the access and privacy balance. They can then determine the worth of these weights to strike a proper balance. The steps outlined below complete the recommended model in that it brings together the necessary information, the parties in interest, and the desire to make balanced and effective policy in a deliberative process.

#### 1. Gather Existing Data

Consider what is needed to make sound decisions in this field. If the necessary data do not exist in compiled form, it must be gathered. If a means to gather it does not exist,

**“The government’s process for balancing access and information privacy should draw heavily on expertise and existing data, involve as many of the affected parties as possible, apply these principles faithfully, focus on real and effective solutions, provide for the automatic termination and/or frequent re-examination of those solutions to ensure their effectiveness and precision in the face of fast-changing technologies.”**

those means must be invented. Here is a short, non-exhaustive list of data sources:

- Existing laws and policies in the local jurisdiction, examples of proposed model laws and provisions, and laws and policies from other jurisdictions.
- Existing surveys, opinion polls, and personal knowledge to determine the salient privacy and access issues and the general level of concern. Get a sense as to the percentage of people who are:

Privacy Purists  
 Privacy Pragmatists  
 Indifferent  
 Access Pragmatists  
 Access Advocates

In this case, being a pragmatist simply means that one's opinion depends on the costs and benefits of each encroachment on privacy or increase in access.

**“Most reactions to a notorious occurrence or crisis produce ill-conceived, poorly targeted, and ineffective laws.”**

- Information policy impact statements because, as noted above, there are often substantial (sometimes unintended) economic effects of public record use. Policymakers should use these impact statements in the same way as fiscal notes, small business and environmental impact statements, and economic multiplier analyses.
- Data, to the extent available, on each of the previously mentioned values relevant to any particular issue under consideration.

## 2. Educate

Information policymaking requires multidisciplinary resources. Ideally, academic, government, industry, and public interest groups should work together to create and acquire information privacy and access resources for the policy specialists, the decision-makers, and the public.

## 3. Identify and Involve the Affected Parties

In many jurisdictions, privacy advocates, the information industry, and other users of government records are not organized to express their interests. Moreover, many of these entities and associations are naturally myopic in their

interests and cannot be relied upon as a sole source of feedback on policy matters. Consider creating a task force representing industry, government, citizens, and advocates to help sort through and respond to these issues.

4. Use the Principles for Policymaking to Perform the Balancing Process

With the necessary data and parties at the table, one can now apply the relevant principles to complete the balancing process and decide whether access or privacy interests should prevail or whether both can be accommodated.

5. Choose a Solution

There are a variety of statutory and market-based solutions to implement a balancing decision.

6. Until This Area Matures, Require Reauthorization of All New Policies

Unlike mature industries such as transportation, finance, and utilities, the information industry does not have time-tested, high quality economic models or policy creation and review models and processes. The information industry changes so rapidly, in fact, that assumptions and policies can be outdated before policymaking bodies can react. To keep information policies flexible, revisable, and modern it is recommended that sunset and reauthorization clauses be applied to each new access, privacy, and information technology law, policy, or rule.

7. Assess Outcomes

Policymakers need to assess the effect of their decisions on privacy protection and access concerns to adequately gauge the success of the process.

**“Information policy committees, agencies, and officers that have the benefit of experience and training in this field should exist at each level of government.”**

### A Reactive Policymaking Model

There are times when an event or political crisis causes policymakers to react and try to immediately address privacy or access issues. While this is ill advised, the following steps will help guide this type of policymaking process. Most reactions to a notorious occurrence or crisis produce ill-conceived, poorly targeted, and ineffective laws. If possible, delay the policymaking process until the issue can be fully considered.

However, if political realities will not allow such a waiting period, proceed with the following steps:

### Information Futures

**Information is the raw material for the knowledge revolution of the Information Age. Without complete and reliable information, much of the benefit of information technology cannot be realized. Data warehousing and relational databases, geographic information and visualization systems, and extraordinary technological developments help us better understand our world and behavior of chaotic and complex systems that otherwise defy comprehensive human understanding. In such a technological environment, information is the fuel of our future. The benefits of the Information Age can only be realized if we have the raw materials on which it's essential systems depend: complete and accurate information used within the reasonable expectations of privacy.**

#### 1. Determine the Cause of the Privacy Harm or Access Limitation

What, in short, is really causing the problem? Is it a public record or bad behavior? If it is both, would it be more effective and fair to attack the behavior or place limits on public records?

#### 2. Determine the Direct and Indirect Impact on Persons and Entities

Despite a perception of a need for swift action, this step is crucial. The information age economy and systems are so interconnected, it is nearly impossible to make a substantial change in one part without affecting many others. It is incumbent on policymakers to find out these effects before enactment. An Information Policy Impact Statement would help force this step in the process and assure that the cure is not worse than the perceived problem.

#### 3. Use the Principles for Policymaking to Perform the Balancing Process

With as much data and as many of the concerned parties at the table as time will allow, one can now complete the balancing process, deciding whether access or privacy interests should prevail, or whether both can be accommodated.

#### 4. Choose a Solution

There are a variety of statutory and market-based solutions to implement a balancing decision.

#### 5. Evaluate the Likely Effectiveness

In the heat of a controversy, it is sometimes politically expedient to just pass a new law to quell the debate, without fully considering its likely effectiveness. While recognizing how difficult it can be to preserve time for thoughtful reflection in the midst of a fast-moving political process, policymakers should strive to evaluate carefully proposed policies to ensure that they will in fact solve the problem, not create unintended problems, and, if such a policy cannot be identified, to wait until an effective

solution can be found and adopted. Ineffective solutions are worse than no solution in the long run, even in politics.

#### 6. Delay Enactment and Require Reauthorization

To allow time to assess the impact and complete a more thorough policy process, policymakers should require a delay in the effective date and require reauthorization.

## Conclusion

The unparalleled openness and accessibility of public records in the United States is not an accident or an historical anomaly. It reflects an understanding that public information is critical for democratic self-governance; that public records belong to the public; and that the widespread availability of public data facilitates opportunity, competition, and prosperity.

Of course, not all information collected by the government is or should be made public. There are important legal protections for confidential financial and health information, trade secrets, and other data which if disclosed publicly would violate a widely shared, objectively reasonable expectation of privacy. This accommodation between information privacy and access is appropriate and necessary in a society that respects the rights of individuals.

Recent efforts to dramatically reduce access to the public record, to close off sources of public information, and to deny the public access to information it has paid to have created or collected threaten the fine-tuned balance between access and privacy. Such a significant shift highlights important issues about the role of the public in the democracy and the right of the public to access its information—information that belongs to the public, not to the government. Equally important, and often ignored in the current debate over the public record, is the understanding that reducing access to public information also poses specific and grave risks to the U.S. economy and to the provision of services and products that the public values and has come to expect.

In terms of policymaking, this area is immature and requires substantial development. Information bears a complex and yet uncharted relationship to the economy and the quality of our lives. Its use and misuse has great potential for good and harm. Great care must be taken in its regulation as each action is likely

**“Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues.”**

to have unintended consequences, positive or negative. Balance, deliberateness, careful review, and caution should form the core of our policymaking efforts.

We must think clearly and precisely about the values served by access and privacy. We must consider the extent to which the public actually and reasonably expects that given information in the public record will be or should be kept private. Finally, we must determine whether targeted and effective protections for privacy can be constructed without denying completely the public's access to information. The cost of doing any less is real, considerable, and will be borne by us all.

**“The difficult challenge for policymakers is to pay attention to the concerns of constituents while at the same time seeking to educate them about the costs and benefits and the intended and possible unintended consequences of proposed regulations. This challenge is made all the harder and all the more necessary by the rapid evolution of information technologies and societal attitudes.”**



## Endnotes

<sup>1</sup> The nation's economic boom and the public's standard of living depends in large part on the availability of more than \$6.5 trillion in outstanding installment and mortgage credit. Credit reporting agencies and other information compilers collect information on property ownership, outstanding liens and other encumbrances, criminal records, corporate filings, and from hundreds of other public records to maintain the reliable, up-to-date data necessary to support rapid and appropriate credit decisions. Associated Credit Bureaus, Inc., *The U.S. Market at a Glance*, 1998. Although the public record constitutes only one of many sources of credit data, information gathered from public records is often particularly relevant. Public record data includes, for example, information about bankruptcies.

<sup>2</sup> Diogo Teixeira and Walter F. Kitchenman, "Bureaus Do a Credible Job," *The Banker*, May 1998, at 104. Reliable, centralized, and standardized consumer credit information makes it possible to pool consumer loans and then sell them to investors. As a result, mortgage rates in the United States are estimated to be as much as two full points lower. With outstanding mortgage rates approaching \$5 trillion, American consumers save \$100 billion a year because of the efficiency and liquidity that information makes possible.

<sup>3</sup> Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 24, 1999. According to Director Freeh the FBI consulted commercial on-line databases to obtain "credit records, real property and tax records; boat, plane, and motor vehicle registration records; business records, including filings with the Securities and Exchange Commission and bankruptcy filings; articles of incorporation; financial information; rental records; news articles; concealed weapons permits; and hunting/fishing licenses" and other "public source information regarding individuals, businesses, and organizations that are subjects of investigations." Access to commercial providers of public record information "allows FBI investigative personnel to perform searches from computer workstations and eliminates the need to perform more time consuming manual searches of federal, state, and local records systems, libraries, and other information sources. Information obtained is used to support all categories of FBI investigations, from terrorism to violent crimes, and from health care fraud to organized crime."

<sup>4</sup> Statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis, before the House Committee on Banking and Financial Services, July 28, 1998.

**"The open public record system has been the mainstay of the U.S. democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports."**

<sup>5</sup> The U.S. real property system also depends on companies that assemble diverse data from diverse sources around the country, verify its accuracy, and make it readily and affordably accessible to purchasers, sellers, lenders, insurers, and others.

<sup>6</sup> Consumer credit bureaus purchase property tax records in bulk from cities and counties. Those bureaus then respond to more than 600 million requests for credit reports each year. As a result, the cities and counties are relieved of the obligation of responding to those requests individually, thereby dramatically reducing their operating costs. Associated Credit Bureaus, Inc., *The U.S. Market at a Glance*, 1998.

<sup>7</sup> In 1998, direct marketing accounted for \$912 billion in sales—12.4% of all consumer sales or an average of \$3,378 for every U.S. citizen—and 24.6 million jobs. The \$429.8 billion spent on direct mail in 1998 is the largest single contributor to the operation of the U.S. Post Office. Direct Marketing Association, *Economic Impact: U.S. Direct Marketing Today* (4<sup>th</sup> ed.), 1998.

<sup>8</sup> Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997) (emphasis added).

<sup>9</sup> Letter from Louis Brandeis to Alice Goldmark (Feb. 26, 1891), in *1 Letters of Louis D. Brandeis* 100 (Melvin I. Urofsky & David W. Levy eds., 1971); Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193, 193 (1890); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

<sup>10</sup> 5 U.S.C. §§ 552(b)(6), (b)(7)(C).

<sup>11</sup> 15 U.S.C. §§ 1681-1681t.

<sup>12</sup> Direct Marketing Association, *Name Removal Services* (available at: [http://www.the-dma.org/home\\_pages/consumer/dmasahic.html#removal](http://www.the-dma.org/home_pages/consumer/dmasahic.html#removal)).

<sup>13</sup> Federal Trade Commission, *Individual Reference Services: A Report to Congress* (1997).

<sup>14</sup> *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Terry v. Ohio*, 392 U.S. 1, 9 (1968); *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

<sup>15</sup> 42 U.S.C. § 14071(a).

**“While recognizing how difficult it can be to preserve time for thoughtful reflection in the midst of a fast-moving political process, policymakers should strive to evaluate carefully proposed policies to ensure that they will in fact solve the problem, not create unintended problems, and, if such a policy cannot be identified, to wait until an effective solution can be found and adopted. Ineffective solutions are worse than no solution in the long run . . . .”**

## Appendix A

### Public Records Classification Options

Public records come in many forms, are collected by many different government agencies, include diverse information, and are used for a wide variety of purposes. In the debate over access and information privacy, there have been many proposals for how to classify public records and the expectations of privacy that may be reasonable for each category. Some of those proposals seeks to classify public records as they exist today; others provide recommendations for how public records might be categorized in the future. Many of those proposals overlap, yet none is entirely comprehensive or satisfactory. However, given the importance of this topic, we include some of the many possible classification options below.

- Unlimited

Simply put, an "unlimited" public record is one that can be used for any legal purpose. This means any legal government or private primary, secondary, or downstream use and it can be packaged, linked, disseminated, re-disseminated, sold, resold, and reused without limit.

- User-Dependent Limits

The first distinction in limited use is whether the limit is on governmental or private users. For example private citizens cannot extract data from personal tax records and use other governmental records to analyze it. However, government can do just that. Several states have tax records in data warehouses where data from individual returns and other government and private data is used to determine such things and under-reporting, non-filing, overstating exemptions, and non-payment of student loans while claiming a refund. There are also exceptions for researchers and other special circumstances. Therefore, it is critical to determine if the limited or confidential classification applies to the public, a special private group, or the government.

- Limited Public Records

Use can be limited to the primary use that is the reason for its collection. If use is allowed beyond the primary use, then the question is whether secondary use (use unrelated to the purpose of collection) is restricted in any way. Finally, if use is allowed beyond secondary use, the question is whether such downstream use (use by third parties after a permissible secondary use) is restricted in any way.

- Transactional Use Only

Where a record is collected and used only for completing a transaction. Such records may be destroyed after the or transaction is completed. An example would be a credit card number given to get a license. These records are usually kept confidential from the public and have only limited use allowed by the government.

- A Gatekeeper Determines the Use

A gatekeeper is a trusted public or private official who limits access to public records to protect the subject of the information. A gatekeeper facilitates communications and transactions otherwise impossible if the subject's record is destroyed or made confidential. One way this approach is used is in selected exceptional circumstances to shield a person from an unacceptable harm that would occur if normal procedures and protections were in place. Some examples include witness protection programs, battered spouses, and stalking victims. Another way it can be used is when a non-governmental gatekeeper holds the public records to ensure that they are only used for their proscribed purposes. This is used only where there is extreme concern, fear, paranoia about government misuse or protection of the record. Some examples of this approach that have been used, discussed, or proposed include lists of AIDS victims, gun registration data, and encryption keys.

- An Infomediary Determines the Use

An "infomediary" is a "a trusted third party, one who connects information supply with information demand and helps determine the value of that information" (<http://www.privaseek.com/>). Infomediaries would be used where there is a desire to allow for a greater range changeable choices and decisions about how records are used. They could also be used where a person and/or the government want to control the choice process and possibly profit from sale and use of the record.

- Third Party Use Only

This is where government collects, but does not use the information. Instead, government merely facilitates its use, storage, and transfer. Some examples include bone marrow donor matching programs and medical records in some adoption cases.

- Confidential Records

Confidential records are those for which there is no public access except for aggregate data in which individual identifiers have been removed. A good example is Medicare records. Government officials or their designees can review them for fraud, waste, and abuse and approve them for payment. However, the only public access to such records is in the aggregate. In other cases, neither the public nor the government is permitted access to a confidential record. An example of this is a sealed court record.

**Testimony of**

**Robert N. Barsness  
Chairman and President  
Prior Lake State Bank  
Prior Lake, Minnesota**

**on behalf of the**

**Independent Community Bankers of America**

**Before the**

**Financial Institutions and Consumer Credit Subcommittee  
Banking and Financial Services Committee  
U.S. House of Representatives**

**on**

**Emerging Privacy Issues**

**July 20, 1999**

**Testimony of Robert N. Barsness**

Madam Chairwoman, Members of the Committee, my name is Robert N. Barsness, and I am chairman and president of Prior Lake State Bank, a community bank located in Prior Lake, Minnesota. I am honored to also serve as president of the Independent Community Bankers of America,<sup>1</sup> and it is on behalf of ICBA's 5,300 community bank members that I appear before you today. Thank you for inviting me to share with you the views of our nation's community bankers on financial privacy issues.

My bank is located in a community of 14,000 people just outside the Twin Cities. We have \$95 million in assets, \$84 million in deposits, and hold \$57 million in loans. We have been in business serving the small business, agricultural and consumer needs of our community since 1909, and have about 35 full time employees.

**Privacy Issues Not Fully Vetted, Could Have Unintended Consequences**

Madam Chairwoman, we are pleased to address the issue of financial privacy from the small bank perspective. In your letter of invitation, you note that "The floor debate [on H.R. 10] regarding privacy reinforced the need to carefully explore the many issues involved in protecting personal financial information in order to avoid unintended consequences such as reduced availability of affordable credit and financial products because of limits on the flow of information." You are absolutely on target, Madam Chairwoman. While the financial privacy legislation horse might not yet have galloped out of the barn, she is saddled-up and moving towards the barn door, which was opened wide by House passage of H.R. 10. And no one is quite sure what will happen when she breaks free. This hearing could not be more timely in terms of outlining the consequences, both intended and unintended, of the privacy provisions contained in H.R. 10.

Indeed, we would much prefer the Congress withholding adoption of new privacy protections until the overall issue can be more fully vetted through the hearing process. At this point, even if privacy policy changes were suggested as a result of these hearings, with H.R. 10 scheduled to go to conference with the Senate imminently, there frankly are few legislative options left to make such changes if they fall outside the privacy parameters of H.R. 10.

---

<sup>1</sup> The ICBA is the primary voice for the nation's community banks, representing some 5,300 institutions at nearly 16,200 locations nationwide. Community banks are independently owned and operated and are characterized by attention to customer service, lower fees and small business, agricultural and consumer lending. ICBA's members hold nearly \$439 billion in insured deposits, \$526 billion in assets and more than \$314 billion in loans for consumers, small businesses and farms in the communities we serve.

### Community Banks Have No Tolerance For Breaches of Privacy

Community banks have a long tradition of carefully safeguarding the confidentiality of their customers' information. In a small community like mine, the consequences of breaching customer privacy are felt immediately. If my bank employees who have access to confidential customer information were to start spreading information around town about how much a customer had in his or her account, or to whom he or she is writing checks, there would be a line of people waiting outside my bank the next day to close their accounts. There are a lot of competitive options in the marketplace, and customers will not stay with a financial institution that does not put a premium on their privacy.

This was in full evidence recently in my state of Minnesota. On June 9, Minnesota Attorney General Mike Hatch filed suit against Minneapolis-based U.S. Bancorp for allegedly selling its customers' private information to a telemarketer. U.S. Bancorp immediately denied any wrongdoing and informed its customers in a letter that the Attorney General "distorted the nature of our marketing partnerships, implying that we sell customer information without regard for confidentiality." The case has since been settled.

Well, Madam Chairwoman, I can tell you that even before the dust was settled on the initial complaint filed by the Attorney General, U.S. Bancorp customers were looking for new places to conduct their banking business. A number came to my small bank in Prior Lake seeking to open accounts, and asking whether we would fully protect the privacy of their accounts.

I am fully confident that my bank enjoys and deserves the full trust of our customers, and know that the community bankers in our nation place the highest value on customer privacy. And we must communicate this to our customers and assure them that their confidential information will be safeguarded.

### Banks Should Adopt Privacy Policies

Simply put, Madam Chairwoman, it is in the self interest of community financial institutions to avoid the misuse of private customer information. The result of such misuse would be the loss of consumer confidence in the institution, and eventually, the loss of customers. That is why voluntary customer privacy practices have worked well. Community banks cannot long survive if they gain a reputation for abusing customer confidentiality.

In September 1997 -- well before privacy became a public policy buzzword in the H.R. 10 debate -- the banking industry adopted a set of industry guidelines, or Privacy Principles, to govern voluntary privacy practices. Since that time, ICBA has continually encouraged its members to formalize their privacy policies and communicate them to their customers. In September 1998, then-ICBA president Bill McQuillan sent a letter to all ICBA members urging them to do just that. President McQuillan noted that, "*With the growth of technology, including*

*electronic commerce, has come increased concerns about privacy of financial information. It's both good public policy and good customer service to assure customers by telling them -- early and often -- what you do to safeguard their financial records. Effective self-regulation is always preferable to external regulation."*

President McQuillan went on: *"Whether or not you handle customer transactions electronically, nothing can strengthen the trust your customers have in your institution more than knowing that you have policies in place for safeguarding confidentiality. Technology makes the world seem like an increasingly impersonal and unfriendly place. If you haven't already made your customers aware of and comfortable with your handling of their records, we strongly urge you to take steps immediately."*

### **Privacy Policy Key to Public Trust**

The point is that privacy is not a new issue for community banks. The protection of our customer's confidential information is central to maintaining the public trust and is key to long-term customer retention. Indeed, the financial services industry as a whole operates under an existing framework of state and federal laws and regulations that provide comprehensive privacy protection for our customers. There are at least sixteen different federal laws that provide privacy protections, not to mention the myriad of rules and regulations that have been written to implement these laws. This Committee and this Congress must decide whether or not these laws are adequate and have been properly enforced, or whether a new set of laws and regulations on top of those already in place are warranted.

### **Competitive Effects of H.R. 10**

The enactment of H.R. 10 will repeal the laws that have historically prevented affiliations among banks, insurance companies and securities firms. The result will be the formation of new financial conglomerates that, in the final analysis, will reduce choices for consumers and further concentrate our nation's financial and economic system.

The prototype conglomerate has already taken shape (and jumped the gun, in our opinion). Citigroup, representing the merger of Citibank and Travelers Group, will be able to offer traditional banking products, underwrite and sell insurance, and provide brokerage services and securities underwriting for its customers, activities that current law generally prohibits from being offered under one roof.

The \$750 billion Citibank-Travelers merger was pulled together under a combination of legal loopholes and anticipated legislative changes. But once all the barriers are removed, cross-industry mergers are expected to proliferate. This will inevitably result in fewer and fewer companies controlling a larger and larger share of the financial market.

To compete effectively in the future and provide a competitive alternative in this



landscape, many community banks will also have to offer products and services beyond traditional banking services. Given that many community banks do not have affiliates -- and are not expected to become affiliated with broker-dealers, and securities or insurance underwriters -- their ability to compete and provide the panoply of financial products and services to their customers depends on their ability to partner with third party providers.

It is for this reason that, as the debate on the privacy provisions of H.R. 10 ensued, we urged -- and continue to urge -- that Congress not pass any proposal that would discriminate against information sharing activities between community banks and third parties for legitimate purposes, or discriminate against institutions based on size or organizational structure.

Madam Chairwoman, this underscores the need to develop a privacy policy that will protect customer's privacy in the new world of financial conglomerates, while recognizing the legitimate differences between those conglomerates and the smaller community banks serving Main Street America. The privacy language in H.R. 10 doesn't accomplish this.

### **H.R. 10 Privacy Provisions**

Madam Chairwoman, in addressing the specific questions posed in your letter, I would like to discuss the first three together, dealing with the purposes of collecting and sharing customer information with affiliates and nonaffiliates, addressing the specific privacy provisions contained in H.R. 10, and discussing the effect more stringent privacy laws would have on our member institutions.

The notice and opt-out requirement of H.R. 10 requires financial institutions to provide clear and conspicuous notice of the bank's information sharing practices, and an opportunity for customers to "opt out" before disclosure of nonpublic personal information to any nonaffiliated third party. However, the bill does not apply the same requirements to those institutions which share the same information in an affiliate relationship. Given that most community banks do not have affiliates, but operate as agents or through joint agreements, this special carve out would reduce the ability of community banks to compete with larger institutions that do have affiliates. We believe that this is inequitable, is competitively harmful, and imposes a disproportionately heavy new regulatory burden on community banks.

### **Community Banks and Third Party Information Sharing**

Community banks provide customer information to a variety of third parties through contractual relationships in order to conduct their everyday business activities. Requiring an opt-out procedure for such routine, ongoing and necessary transactions would impose significant new regulatory and data processing burdens and costs on community banks. Given that these institutions are generally smaller in size and have fewer resources available to them than those institutions with corporate affiliates, singling them out for new restrictions would be even more detrimental and anti-competitive.

From the perspective of a customer of a community bank, this discriminatory restriction also would be harmful. Because of the costs of implementing an opt-out procedure, a small community bank may have to limit the availability of other related products and services to its customers.

For example, my bank now offers each of our consumer deposit customers a free \$1,000 accidental death benefit underwritten by a third party provider. Customers may purchase higher levels of insurance coverage, but are not required to. In order to provide this customer service, I must provide the name, address and account number of our customers to the third party provider. It appears that if H.R. 10 is enacted, I will be prohibited from offering this free benefit, unless I first notify each customer and give them the right to opt out. I will have to weigh the cost of implementing such a notice and opt-out policy, against the good will that my bank receives for providing this free benefit to our customers.

Madam Chairwoman, you asked for examples of the information sharing activities that community banks engage in on a routine basis. As noted, most community banks do not have affiliates; therefore, most do not share information with affiliates. However, because of their limited resources and to maintain efficiency, community banks rely on a variety of third party providers, so-called "outsourcers" to provide services for the bank, such as the insurance underwriter that provides the free accidental death benefit for our customers. As part of this relationship, customer information must be shared as part of the task being undertaken. For example: data processing (outside service bureaus); check clearing and processing; check printers; credit card processing; ATM/EFT networks and ATM/EFT data processors; appraisers, title insurers, electronic banking vendors/service providers, etc. This list could be practically endless.

Community banks also share information with outside parties in order to make quick, efficient credit decisions, manage and control risk, and prevent fraud. The most typical examples in this category are credit bureaus and similar consumer reporting agencies that provide information for credit underwriting, identity authentication, risk management and fraud protection (e.g., agencies that maintain databases on fraudulent or unsatisfactory check writers).

Similarly, certain customer information is made available to outside auditors and other community bank consultants that need access to bank records and files, such as loan files for financial and compliance audits and reviews.

Community banks also must by necessity disclose or share certain customer information with third parties when they sell assets, e.g., secondary market loan sales, loan participations, sale of loan servicing, loan securitizations, and branch sales (may include both deposit accounts and loans). They also must disclose or share customer information as part of mortgage activities such as mortgage banking, mortgage brokering, and origination of loans closed in the name of another lender.

Customer information may be shared or disclosed to third parties in a number of instances in order to provide a full array of additional financial products and services to customers. Typical examples include:

- Joint agreements/ third party networking arrangements with unaffiliated broker/dealers to provide securities sales/investment product services to bank customers. Frequently, these arrangements use dual/common employees that are employed both by the bank and broker/dealer.
- Joint ventures/networking arrangements with insurance agents to sell insurance products to bank customers. These as well may involve dual or common employees.
- Credit card agent bank programs. Many smaller banks want to issue credit cards to their customers, but do not want to undertake the credit risk or the administrative/processing responsibilities. These banks can contract with larger card issuers to become an agent bank of that issuer and issue credit cards to their customers.
- A variety of other joint ventures, cobranding, networking arrangements to provide products and services to customers (e.g., credit life insurance sales, frequent flyer programs, club accounts, etc.).

The foregoing examples are not meant to be exhaustive, but rather illustrative of the types of legitimate business activities community banks engage in where customer information may be shared or disclosed to third parties.

Importantly, it should be noted that community banks do not undertake these activities cavalierly. They carefully select reputable outsourcers and third party partners. They also carefully review, ascertain and limit what particular customer information will be shared. As part of the contractual relationship, the third parties are required to maintain the confidentiality of the customer information that they have access to. A typical confidentiality agreement provides that: the customer information remains the property of the disclosing party; the third party may not use the information in any way not permitted by the agreement; and access to the information must be restricted only to employees of the third party with a need to know the information in order to perform the services.

#### **H.R. 10 Exception Authority**

It should be noted that there are a number of general exceptions to the requirement in H.R. 10 that information not be shared with nonaffiliated third parties unless the customer has been given notice and a chance to opt out. These exceptions include: as necessary to effect, administer or enforce a transaction; for asset securitization or secondary market sales; with the customer's consent; to protect against fraud; to law enforcement agencies (as permitted by law);

to consumer reporting agencies (e.g., credit bureaus); to the bank's attorneys, accountants and auditors; and in connection with the sale or merger or all or a portion of the bank. In addition, there are exceptions for third parties that perform functions on behalf of the bank, and for offering financial products and services under a joint agreement between financial institutions (where payments between the parties are based on business or profits generated). Also, joint employees of the institution are not considered to be nonaffiliated third parties. We believe many of the activities described earlier should be covered under these exceptions. However, with the vagaries of legislative drafting, inevitable legal challenges, and of the subsequent regulation and implementation, only time will tell if that is the case.

Importantly, H.R. 10 also gives banking regulators the authority to provide for additional exceptions by regulation consistent with the purposes of the legislation. Since it is unknown at this time whether or not all of the legitimate third party information sharing activities routinely conducted by banks would be covered by the statutory exceptions, this additional authority takes on enormous importance.

### **Regulatory Burden**

Madam Chairwoman, community banks are also concerned about the administrative and regulatory burdens that the privacy provisions of H.R. 10 portend. It is one thing for the banking industry and individual banks to adapt, adopt and adhere to privacy principles and practices voluntarily, and another to have rules prescribed by statute, implemented by regulations, and enforced through regular examination.

Community banks will have to devote time and resources to ensure that they strictly adhere to the statutory scheme, which we note treats information sharing in four ways: those instances in which neither notice nor opt out is required; those in which notice is required; those where notice and opt out is required; and those where there is a flat prohibition on sharing of information, even if the customer consents. While we appreciate that the scheme is different in many instances in order to allow certain types of information sharing without the associated burdens of notice and opt out, it is nonetheless confusing, and fraught with opportunity for misstep.

Community banks will have to make data processing and other administrative changes in order to accommodate the opt-out requirements, and devote time and resources to examination preparation, etc. This additional regulatory and administrative burden will impact community banks disproportionately because of our finite and limited resources, further reducing our ability to compete vis-a-vis larger institutions. And some community banks may decide it is not cost effective to offer related products and services to their customers because of these burdens, once again reducing customer options and choice.

### **Strengthening Consumer Confidence**

With regard to your request for suggestions that would strengthen consumers' confidence in their financial privacy without hindering our daily operations, my first suggestion would be to ensure that there is parity in whatever privacy policy is adopted. The privacy policy included in H.R. 10 fails this important test. We believe strongly that Congress should reject any financial information privacy proposal that would impose new burdens on the information sharing activities of community banks without affiliates, while exempting from such requirements information sharing activities between affiliates.

In addition, I believe Congress should examine and evaluate the effectiveness of the Privacy Principles adopted by the banking industry in 1997. These principles are attached to my testimony.

In addition, we believe that medical information should be held to a very careful standard of protection, and "pretext calling" should be prohibited.

#### **Community Banks Adapt Privacy Principles to Their Markets**

The ICBA has made the Banking Industry Privacy Principles available to our membership and encouraged member banks to adopt privacy policies consistent with these principles. Many banks have adopted and implemented such policies; some have modified these principles to better suit their community and their market. I would like to submit one such policy as being reflective of how individual financial institutions can adapt the Privacy Principles to their unique circumstances. (Policy Attached)

We believe these policies provide a workable framework from which each bank can devise a reasonable and appropriate privacy policy that will protect the confidential information customers entrust to their financial institutions, while permitting banks to provide their customers with the highest levels of product and service opportunities.

#### **Closing**

Madam Chairwoman, we appreciate this opportunity to present the views of our nation's community bankers on customer privacy. We believe this is an issue of utmost importance to all financial institutions, and speaking for our nation's community bankers, we stand ready to work with you to ensure customer trust and confidence in our banking system.

#### **Attachments**

## **U.S. Banking Industry Privacy Principles**

### **Recognition of a Customer's Expectation of Privacy**

Financial institutions should recognize and respect the privacy expectations of their customers and explain principles of financial privacy to their customers in an appropriate fashion. This could be accomplished, for example, by making available privacy guidelines and/or providing a series of questions and answers about financial privacy to those customers.

### **Use, Collection and Retention of Customer Information**

Financial institutions should collect, retain and use information about individual customers only where the institution reasonably believes it would be useful (and allowed by law) to administering that organization's business and to provide products, services and other opportunities to its customers.

### **Maintenance of Accurate Information**

Financial institutions should establish procedures so that a customer's financial information is accurate, current and complete in accordance with reasonable commercial standards. Financial institutions should also respond to requests to correct inaccurate information in a timely manner.

### **Limiting Employee Access to Information**

Financial institutions should limit employee access to personally identifiable information to those with a business reason for knowing such information. Financial institutions should educate their employees so that they will understand the importance of confidentiality and customer privacy. Financial institutions should also take appropriate disciplinary measures to enforce employee privacy responsibilities.

### **Protection of Information via Established Security Procedures**

Financial institutions should maintain appropriate security standards and procedures regarding unauthorized access to customer information.

### **Restrictions on the Disclosure of Account Information**

Financial institutions should not reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence, unless 1) the information is provided to help complete a customer initiated transaction; 2) the customer requests it; 3) the disclosure is required by/or allowed by law (e.g., subpoena, investigation of fraudulent activity, etc.); or 4) the customer has been informed about the possibility of disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (i.e., "opt out").

### **Maintaining Customer Privacy in Business Relationships with Third Parties**

If personally identifiable customer information is provided to a third party, the financial institutions should insist that the third party adhere to similar privacy principles that provide for keeping such information confidential.

**Disclosure of Privacy Principles to Customers**

Financial institutions should devise methods of providing a customer with an understanding of their privacy policies. Customers that are concerned about financial privacy will want to know about an institution's treatment of this important issue. Each financial institution should create a method for making available its privacy policies.

Approved March 3, 1979

**CONSUMER PRIVACY POLICY****PURPOSE**

This policy reaffirms our bank's realization of and respect for the privacy expectations and rights of our customers regarding financial information and other related information which the bank has or gathers in the normal course of business. It is intended to provide guidance to bank personnel as well as assurance to our customers.

**DEFINITION AND SCOPE**

The terms "employee" and "employees" as used in this policy statement include all directors, officers and employees of the bank as well as any attorneys, agents, or outside vendors, who become privy to customer information.

The terms "data", "information", or similar wording refer to any and all information regarding our customers provided to or obtained by the bank, regardless of the manner or medium in which such information is either obtained or is stored. It includes, but is not limited to, information regarding:

- ▶ The fact that an individual is a customer of the bank.
- ▶ Identification information including account numbers, social security numbers, driver's license numbers, similar identification numbers, or family names.
- ▶ Types of accounts, dollar amounts of such accounts, and the manner in which the customer has used or managed these accounts, currently or in the past.

**RESPONSIBILITY**

The board directs the Chief Executive Officer and the Vice President/Secretary to implement this policy.

**PRIVACY PRINCIPLES**

The bank recognizes the following eight elements of its privacy policy, which have become standard within the banking industry:

- 1) Recognition of Customer's Expectation of Privacy



- 2) Use, Collection and Retention of Customer Information
- 3) Maintenance of Accurate Information
- 4) Limiting Employee Access to Information
- 5) Protection of Information via Established Security Procedures
- 6) Restrictions on the Disclosure of Account Information
- 7) Maintaining Customer Privacy in Business Relationships with Third Parties
- 8) Disclosure of Privacy Principles to Customers

#### RECOGNITION OF CUSTOMER'S EXPECTATION OF PRIVACY

Customers of the bank are entitled to the absolute assurance that the information concerning their financial circumstances and personal lives, which the bank has obtained through various means, will be treated with the highest degree of confidentiality and respect. Certain expectations of privacy also contain legal rights of customers which are either granted or confirmed to them through various federal and state laws and regulations. All employees are directed by this policy to assure customers of the bank's commitment to preserving the privacy of their information. The bank will post a notice in all banking offices which contains an abbreviated version of this policy and the name and telephone number of the person from whom the customer can receive additional information. That notice is included in the appendix to this policy and is designed to be both a posted notice and a direct disclosure to customers under circumstances described later in this policy.

#### USE, COLLECTION AND RETENTION OF CUSTOMER INFORMATION

It is the policy and practice of the bank to collect, retain and use information about individuals, customers (both individual and corporate) only where the bank reasonably believes the gathering of such information would be useful and allowed by law to administer the bank's business and/or to provide products, services or opportunities to its customers.

#### MAINTENANCE OF ACCURATE INFORMATION

The Chief Executive Officer and Vice President/Secretary are directed to establish procedures to ensure that, to the extent practicable, all customer financial information is accurate, current and complete in accordance with reasonable commercial standards. The bank will respond promptly and affirmatively to any legitimate customer request to correct inaccurate information, including forwarding of corrected information to any third party who had received the inaccurate information. The bank will further undertake to record that such corrective action was requested by the customer and follow up with any third party to ensure that they have processed the correction.

#### LIMITATION ON EMPLOYEE ACCESS

The Chief Executive Officer and Vice President/Secretary will take all steps necessary to ensure that only employees with a legitimate business reason for knowing personally identifiable customer information shall have access to such information. To the extent practicable, access will be limited by computer access codes and granting limited access to areas in which sensitive customer information is retained. Employees will be informed at the time of their initial employment of these standards and periodically reminded of these standards during training sessions at least once during each calendar year. Willful violation of this element of this policy will result in disciplinary action against the offending individual. Inadvertent violations will be dealt with in a manner to ensure that such violations are not repeated.

#### PROTECTION OF INFORMATION

The bank will maintain appropriate security standards and procedures to prevent unauthorized access to customer information. Such procedures should prevent access by not only unauthorized employees, but others as well. Such others include but are not limited to, all non-employees with otherwise legitimate reasons for being on bank premises, computer "hackers", and all intruders on bank premises.

#### RESTRICTIONS ON THE DISCLOSURE OF ACCOUNT INFORMATION

The bank will not reveal specific information about customer accounts or other personally identifiable data to any unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information, or in the performance of corporate due diligence, unless it meets with one or more of the following criteria:

- 1) The information is provided to help complete a customer initiated transaction.
- 2) The customer requests it.
- 3) The disclosure is required or allowed by law, such as by subpoena, other legal process, or for investigation of fraudulent activity. (The policy recognizes further that, while the bank wishes to cooperate fully with law enforcement agencies, such agencies operate under the law and are not entitled to preferential access to customer information in the absence of clear legal authority to have such access.)
- 4) The customer has been informed about the possibility of disclosure for marketing or similar purposes through a prior communication,, and is given the opportunity to decline or "opt out."

**BUSINESS RELATIONSHIPS WITH THIRD PARTIES**

If the bank is requested to provide personally identifiable information to a third party and that request is in all respects consistent with other elements of this policy, the bank will accede to the request only if the third party agrees to adhere to similar privacy principles, no less stringent than set forth in this policy, that provide for keeping such information confidential.

**DISCLOSURE OF PRIVACY PRINCIPLES TO CUSTOMERS**

The bank will advise its customers of this privacy policy. The Chief Executive Officer and/or Vice President/Secretary are directed to develop, implement, and maintain a suitable information and disclosure process to that end. The disclosures may be in the form of, but not limited to:

- 1) Information provided at the time a customer opens a new account or obtains a new product or service.
- 2) Periodic disclosures, at least annually, mailed or otherwise distributed to customers (statement stuffers, customer newsletters, etc.).
- 3) Posting of Customer Privacy Policy, or an abbreviated form of the policy, at banking offices and the bank's Web site.

**INFORMATION SHARED WITH CREDIT REPORTING AGENCIES AND ERROR RESOLUTION**

The bank, as with the majority of financial institutions, shares information about accounts of its customers with consumer reporting agencies. The bank will take all steps necessary to ensure the accuracy of such information, and will take prompt remedial action to correct any information which the bank has reported which is found to be incorrect. If a customer believes that we have reported incorrect information to such an agency, he or she is directed to write the bank at its main office address:

The customer is required to include his or her complete name, current address, telephone number, and social security number. The writing should also include the account number, type of account, and the specific item of information in dispute, along with the reason the customer believes the information to be in error.

The bank is required to conduct an immediate investigation of the matter referenced in the customer's assertion of erroneous reporting. The bank must respond to the customer's assertion in writing within 10 business days of the bank's receipt of any such assertion and such writing must include the bank's findings on the matter, including any corrective measures taken. If the bank,

through reasons beyond its control, is either unable to confirm or deny the customer's assertion or if it is unable to effect the required corrective action within the allotted 10 business days, the customer will be informed of the bank's actions taken to date and the probable time frame during which the matter will be resolved.

The customer also has the right to "opt out", under the Fair Credit Reporting Act, from having information shared about his or her account with any third party, including a consumer reporting agency unless the transaction is "initiated by the customer". The latter condition is considered to be met if the customer has opened a deposit or loan account with the bank, or has granted permission to third party, consistent with the provisions of the Fair Credit Reporting Act, to inquire from the bank concerning specific past or present account activity. The condition is not met if the bank has received information regarding a customer from any other source.

A customer may elect to "opt out" of any sharing of information by the bank with any third party in those situations which are "not initiated by the customer" by writing to the bank at the address shown above. The bank will be bound, by the customer's request alone, to take immediate action to ensure that the information is not shared.

#### EMPLOYEE EDUCATION AND TRAINING

The Chief Executive Officer and the Vice President/Secretary are directed to provide a copy of this policy to all bank employees and to obtain a receipt from each employee acknowledging that fact. After any amendments or modifications to this policy have been duly adopted, a copy of the amended policy will also be given to each employee, again acknowledged by receipt.

At least once during each calendar year, the bank will conduct a meeting of all employees during which matter effecting customers' rights to privacy will be discussed. Such meetings will include discussions on the following:

- The proper use of customer information.
- Procedures for maintaining security of information.
- The importance of confidentiality and customer privacy
- Any incidents, or patterns of behavior, which are covered under this policy.

#### RECORD-KEEPING AND REPORTING

The Chief Executive Officer and Vice President/Secretary will maintain a separate file for the purpose of retaining any customer complaints which relate to this policy. The information regarding

any complaint should include the exact nature of the complaint, describe the corrective actions taken, and confirmation that the corrective actions resolved the complaint.

The Chief Executive Officer will make an annual report to the board concerning customer complaints which shall include the frequency and nature of such complaints and corrective actions taken. Complaints of a nature sufficient to present a risk of regulatory enforcement action and/or civil money penalties are required to be reported if and when they occur.

#### REVIEW OF POLICY

The board of directors will make a review of this policy at least once each year and make any revisions and amendments it deems appropriate. The Chief Executive Officer will be responsible for suggesting more frequent revisions as situations or changes in laws or regulations dictate.

**CUSTOMER INFORMATION PRIVACY  
STATEMENT**

The Bank recognizes that our customers both desire and have the right to privacy and confidentiality of the information they have entrusted to the bank. To that end, The Bank has adopted a "Customer Privacy Policy". The following eight Privacy Principles are included in that policy, which have been adopted as central guiding principles by several banking groups.

1. Recognition of Customer's Expectation of Privacy
2. Use, Collection and Retention of Customer Information
3. Maintenance of Accurate Information
4. Limiting Employee Access
5. Protection of Information via Established Security Procedures
6. Restrictions on the Disclosure of Account Information
7. Maintaining Customer Privacy in Business Relationships with Third Parties.
8. Disclosure of Privacy Principles to Customers

The above statement and list of principles offers only the issues addressed by the "Customer Privacy Policy". Customers, who have specific questions regarding the policy may contact The Bank, either in writing, or by telephone during regular business hours.

**Testimony**  
**of**  
**America's Community Bankers**  
**on**  
**Emerging Financial Privacy Issues**  
**before the**  
**Subcommittee on Financial Institutions and Consumer Credit**  
**Committee on Banking and Financial Services**  
**of the**  
**U.S. House of Representatives**  
**on**  
**July 20, 1999**

**Robert R. Davis**  
**Director of Government Relations**  
**America's Community Bankers**  
**Washington, DC**

Chairwoman Roukema and members of the Subcommittee, my name is Robert R. Davis. I am the director of government relations for America's Community Bankers.

America's Community Bankers (ACB) is the national trade association for progressive community banks of all sizes. ACB members have diverse business strategies based on consumer financial services, housing finance, small business lending, and community development, and operate under several charter types and holding company structures. We appreciate this opportunity to testify before the Subcommittee today on this very important issue.

Chairwoman Roukema, let me begin by commending you for holding these timely hearings on one of the most critical issues facing our nation's financial services industry and the customers we serve: protection of personal financial information privacy. Without a doubt, financial information privacy protection is one of the top issues facing our evolving financial services system and deserves the in-depth review and examination by Congress that these hearings represent.

All of us are well aware of the growing public concern about information sharing practices, both in the financial services industry and in other sectors of our nation's economy. The news is full of stories about people receiving telemarketing calls during dinner or bundles of direct mail solicitations in their mailbox, with no knowledge about how or from where their personal information was obtained. As a consumer, I am personally concerned about my name, address, telephone number, and financial information being on thousands of lists targeting me and my family for the sale of products and services I may not want or need.

At the same time, there are legitimate -- even essential -- reasons for businesses to share information. If the free flow of information were cut off, financial institutions and other businesses could not carry out most of the transactions initiated or requested by customers. They could not offer to consumers new lines of products and services. They could not carry out the reporting and monitoring activities required by law. While many consumers are understandably upset about the occasional excesses of information sharing and marketing practices, I am confident that virtually none of them would support laws which would effectively ban information sharing altogether, or significantly restrict legitimate marketing programs.

Clearly, information sharing practices should be subject to reasonable requirements. Those requirements should in part be the result of a self-examination by businesses of their own activities. In fact, many of them are now in the process of conducting such reviews. After all, the success of a company, particularly a financial institution, depends on establishing good relations with existing and potential customers. If a customer has reason to distrust or lose faith with a company with which they conduct business, that is one less customer a company will have the opportunity to serve. Good business sense dictates the old adage: "the customer comes first."

Government should have a role in ensuring that basic standards to protect personal financial information privacy are established and implemented by financial institutions. While most businesses are serious about doing what it takes to maintain good customer relations, it only takes one highly publicized, isolated incident to upset the apple cart. Because financial



institutions, particularly banks, depend on continued public faith in the integrity of the financial system, reports of excessive or abusive information sharing practices can have a detrimental impact on their ability to do business. ACB urges the 106<sup>th</sup> Congress to enact legislation which affirms its commitment to consumers that their basic privacy rights will be protected.

Such legislation must be balanced to ensure consumers that their personal information will be protected, while not unduly interfering with the routine, legitimate practices of financial institutions. ACB commends the House for its efforts to reach that balance in the privacy provisions found in H.R. 10 and supports moving the legislation forward, with some suggested modifications. We thank the Subcommittee for this opportunity to discuss ways to improve the privacy provisions in H.R. 10.

### Summary

In response to the questions you raised in your invitation letter of July 9, 1999, our testimony will focus on five major points: (1) ACB's policy position on customer information privacy; (2) some background and history of the financial information privacy debate; (3) our member institutions' experiences with information sharing; (4) some recommended improvements for the privacy protection provisions in H.R. 10; and (5) the effect that more stringent privacy protection requirements might have on the operations of our member banks.

As the voice for progressive, community banks, ACB strongly supports protecting the personal information privacy rights of consumers of financial services. On July 17, 1999, ACB's Board of Directors adopted the following official policy position on customer information privacy:

*ACB supports efforts to protect the non-public, personal information privacy rights of consumers of financial services. While existing laws and general industry practices have provided broad privacy protection for financial services customers, ACB supports the enactment of legislation which would properly balance the legitimate information sharing needs of a financial institution with the obligation to protect customer information privacy.*

*ACB supports requiring all financial institutions to develop an individual privacy protection policy that applies to all bank products or products shared with partners or through other relationships, and provide that policy to all customers. An institution should only be required to provide each customer with its privacy policy once, unless substantive changes are made to the policy. This requirement should cover all financial institutions, including but not limited to insured depository institutions, credit unions, broker/dealers, investment advisers, investment companies, and insurance companies. Enforcement of this requirement should be assigned to an institution's functional regulator, where one exists, and to the Federal Trade Commission for those institutions which are not functionally regulated. A new private right of action for violations of the disclosure requirement should not be created.*

*ACB recognizes that customers of community banks generally do not want their personal financial information sold to unrelated third party telemarketers. ACB does not oppose requirements that a customer be given the opportunity to opt out of having his or her personal financial information shared with unrelated third parties for marketing purposes, so long as*

*these requirements do not apply to: (1) the sale of the bank's own products and services; (2) the sale by the bank of products and services as part of a contractual agency relationship with another company; (3) joint ventures and the providing of products and services through common employees; (4) information sharing practices to facilitate routine services, such as authorization, settlement, billing, processing, check clearing, transfer, or collection; and (5) information sharing practices needed to effect the sale of mortgages in secondary markets. Such requirements should not unfairly discriminate against smaller community banks which use contractual relationships with third parties for the same legitimate purposes for which larger banks use affiliates.*

*Financial institutions should be required to notify customers once of the opportunity to opt out, and customers should be required to notify the financial institution within a reasonable, specified period of time if they choose to opt out. As with disclosure, this requirement should be applied to all financial institutions, not limited to insured depository institutions; overseen by the institution's appropriate functional regulator; and not subject to a new private right of action.*

*ACB also supports criminalizing the practice of obtaining the personal financial information of another person through false, fraudulent, or deceptive means.*

*To protect the health and medical information privacy rights of customers, ACB supports requirements that such information not be shared, unless the customer consents to such practices or directs that his or her health or medical information be shared with another party.*

This policy position is the result of substantial input and feedback, both from a public policy and real-life operational perspective, from a number of ACB member institutions. We are pleased that the approach taken in H.R. 10 generally tracks the key points in our policy position. We support legislation that, at a minimum, requires every financial institution to establish its own privacy policy and to share that policy with its customers; prohibits the sharing of health and medical information without the consent of the customer; and bans abusive pretext calling practices.

We also appreciate the fact that the House of Representatives responded to concerns raised by ACB members and other smaller community banks and carved out critical exceptions to the bill's opt-out requirement for information sharing with third parties. Prior to House floor action on H.R. 10, some segments of the financial services industry suggested legislative language as a substitute for the onerous privacy protection provisions in the House Commerce Committee's version of H.R. 10.

To ensure that smaller community banks had a say in the drafting process of privacy protection legislation, ACB and the Independent Community Bankers of America sent a letter on June 22, 1999 to Speaker Hastert and Minority Leader Gephardt requesting that financial privacy legislation not unfairly discriminate against community banks that use third party relationships for the same legitimate purposes for which larger banks use affiliates. We would like to thank

Chairwoman Roukema, Representative Deborah Pryce, Representative Martin Frost, and other leaders in the House for their efforts to address these concerns.

While we are not opposed to the bill's provisions to give consumers a say in whether or not their personal information is shared with third parties, we would like to suggest an alternative approach that will allow us to reach the same goal more efficiently and with greater certainty. Every day, smaller community banks use contractual relationships with third parties for the same legitimate purposes, such as marketing of products and services, while larger institutions often use affiliate relationships. H.R. 10 requires an opt-out procedure for these third-party information sharing activities, with certain carved out exceptions. Because it does not, however, impose a similar responsibility on sharing information with affiliates, H.R. 10 could still place smaller community banks at some disadvantage. While the bill's exceptions to the opt-out requirement will help mitigate this disadvantage by allowing banks to carry out routine activities, they may not cover all of the legitimate information sharing activities for which community banks use third parties. As a result, community banks would be forced to either tailor their activities to fit the bill's exceptions or give up activities the benefits of which cannot justify the cost of establishing an opt-out procedure.

Instead of using H.R. 10's approach of establishing a blanket opt-out requirement for information sharing with third parties and then carving out exceptions to this requirement, Congress should first determine which activities, practices, or relationships justify a required opportunity for a consumer to opt out, and apply that requirement only to those activities. This more direct approach would still give consumers the right to say no to the information sharing activities that give rise to a public policy concern. At the same time, it would protect smaller community banks from the cost and burden of having to justify each of their legitimate information sharing activities with third parties. While ACB commends the House for its efforts to date to help level the playing field between larger and smaller financial institutions, we do urge the House-Senate conferees to consider this alternative, targeted approach to the opt-out requirement.

### **Background and History**

As we work to identify and address the public concerns about protecting personal financial information privacy, it is important to remember how we got here. To suggest, as some have, that financial information privacy protection is a "new" issue is inaccurate. For years, customer information privacy has been addressed by a number of existing statutes and regulations, including the Fair Credit Reporting Act (FCRA), the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and others. In fact, just three years ago, Congress enacted a series of additional consumer protections when it reauthorized the FCRA.

But as advances in technology allow financial institutions to provide more products and better services to consumers, there remains an ongoing responsibility to reevaluate these laws and their adequacy in protecting privacy rights. While consumers want to reap the benefits of a modernized financial system, they also want their personal financial information to be secure.

Recent events, like the now-settled suit filed against U.S. Bancorp in Minnesota, have heightened public scrutiny of financial information sharing practices. In addition, well-publicized reports of abusive pretext calling practices have also raised concerns among consumers about the confidentiality of their personal financial information. Like it or not, these separate incidents could very well lead consumers to believe that their privacy rights might be threatened. That is not the case, and we cannot lead the public to believe it is. It is the responsibility of both the private and public sector to preserve consumer confidence in the integrity of our financial system.

The twin goals of providing consumers with greater benefits, such as more efficient delivery of services and access to a wider array of products, and protecting their personal financial information privacy rights are not and should not be deemed to be mutually exclusive. As we move forward down the information superhighway, we must reassure consumers that their personal financial information privacy rights will be honored, both in the daily practices of financial institutions and in the law.

#### **Information Sharing Practices of ACB Member Institutions**

In June, ACB conducted a comprehensive survey of select member institutions, asking detailed questions about their information sharing practices. Because of the diversity of ACB's membership, survey respondents were asked about information sharing activities with both affiliates and non-affiliated third parties. The banks responding to this survey ranged from those which engaged in numerous information sharing activities to those which engaged in none.

Information sharing activities engaged in by ACB members include: (1) use of outsourcers providing services for banks, e.g., check printing, credit card processing, ATM/EFT networks, data processing, etc.; (2) joint marketing arrangements with third parties, both for the sale by the third party of the bank's products and services and the sale by the bank of the third party's products and services; (3) mortgage activities, including mortgage servicing and securitization, and sales of mortgages in secondary markets; (4) activities involving dual or common employees; and (5) joint ventures, e.g., credit life insurance sales, and co-branding activities, e.g., credit cards. While this list is not exhaustive, it does illustrate the wide range of information sharing activities engaged in by ACB member institutions, both with affiliates and third parties.

Just as importantly, however, is the fact that many ACB member institutions which do not presently engage in these and other legitimate information sharing activities may want to do so in the future. Feedback from our member institutions indicate that overly onerous regulation or restriction on potential information sharing activities could foreclose the opportunity for community banks to provide new products and services to their customers.

#### **Privacy Protection Provisions in H.R. 10**

Even with the recently intensified efforts by financial institutions to reexamine their information sharing practices, many consumers may still feel that more needs to be done to protect their personal financial information privacy rights. In response to these concerns, the

House adopted the privacy provisions in H.R. 10. As I stated earlier in my testimony, these provisions are generally consistent with the scope of ACB's official policy position on customer information privacy. We would, however, like to suggest the following improvements to the bill's provisions.

#### Privacy Protection Obligation

Section 501 of H.R. 10 states that each financial institution has an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." ACB is concerned that the inclusion of this broad, vague legal obligation could have unintended, harmful consequences, such as creating an implicit private right of action by consumers. If Section 501 is retained, we ask that it be listed either as a non-binding statement of legislative intent or as part of Congressional findings.

#### Disclosure Requirement

Because we believe that an informed consumer makes a better customer, ACB supports the general requirement in Section 503 of H.R. 10 that each financial institution establish its own privacy policy and provide that policy to its customers. We do not believe, however, that such disclosure need be made at least once a year, as required by H.R. 10. Such disclosure should be provided to new customers at the time the customer relationship is established, to existing customers if the privacy policy is amended, and to existing customers within a reasonable period of time following the issuance of final regulations promulgated under the bill.

#### Opt-Out Requirement

ACB does not oppose the opt-out requirement found in Section 502 of H.R. 10 for information sharing activities with third parties. We would, however, suggest that targeting specific activities, practices, and relationships for an opt-out requirement would be a better and more direct approach toward resolving consumer concerns than the bill's blanket requirement for third-party information sharing activities with exceptions.

For example, an opt-out requirement could be imposed in cases where a third party uses a bank customer's information to telemarket its own products to the bank's customer. Such a requirement would help address the recently settled complaint raised in Minnesota against U.S. Bancorp. At the same time, it would not limit institutions from establishing new multiple-party marketing agreements or joint ventures, such as those related to expanded use of the Internet.

If the approach taken in Section 502 is retained, ACB would suggest expanding the bill's exceptions to the opt-out requirement. While the current exemption language in H.R. 10 covers many of the activities and relationships in which ACB member institutions are engaged, other practices, such as joint ventures and co-branding activities, should also be explicitly included in the list.

### Disclosure of Account Numbers

Section 502(d) of H.R. 10 prohibits the disclosure by a financial institution of account numbers to any unaffiliated third party for use in telemarketing to a consumer or for use in direct mail or electronic mail marketing. It should be amended to allow for the same exceptions applicable to the bill's opt-out requirement.

### Customer Lists

Under Section 509(4) of H.R. 10, "nonpublic personal information" is defined to include "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable information other than publicly available information." This broad definition could subject to an opt-out requirement any list or grouping of customers by a financial institution, no matter how broad the category. This definition should be narrowed to focus on the types of lists or groupings that the public finds objectionable.

### Other Recommendations

ACB also recommends that a broad federal preemption of state laws be included in the bill. In the absence of a federal preemption clause, financial institutions would not only have to comply with federal law, but also with a host of potentially conflicting state laws. This would make compliance unduly difficult and burdensome, particularly for those financial institutions with operations in more than one state.

ACB is pleased that the disclosure and opt-out requirements in H.R. 10 will be functionally regulated. Consistent with our official policy position, we also support the protection of health and medical information privacy in Section 351 of the bill and the ban on abusive pretext calling practices in Subtitle B of Title V.

We respectfully urge the House-Senate conferees to take our recommendations into consideration as they work out the differences between the privacy provisions in H.R. 10 and S. 900.

### **Effect of More Stringent Privacy Requirements**

If the privacy provisions in H.R. 10 are enacted, it would mark the biggest step ever taken by Congress to put in law basic standards to protect personal financial information privacy. Still, we recognize that there are members of Congress who believe that the privacy provisions in H.R. 10 should be even more stringent. Some of these proposals include imposing an opt-out requirement on information sharing between affiliates, requiring an opt-in procedure for information sharing with all third parties, or creating a private right of action as a means of enforcement. Given the experience of our member institutions with information sharing practices, ACB does not believe that such proposals warrant legislative action.

ACB supports the decision by the House not to include in H.R. 10 an opt-out requirement on information sharing activities between affiliates. The bill defines "affiliate" as "any company that controls, is controlled by, or is under common control with another company." Because of the required controlling relationship between a bank and an affiliated firm, any customer

information sharing in which these businesses engage must be kept within the same corporate family structure. An even tighter relationship can be found in cases where a bank owns a service corporation, as many ACB member institutions do.

At the same time, ACB reiterates its opposition to legislation that would unfairly discriminate against smaller community banks which use third party contractual relationships for the same information sharing purposes for which larger banks use affiliates. We do not, however, believe that imposing restrictions on affiliate information sharing practices is an acceptable way to ensure fairness. Instead, we continue to encourage Congress to target the opt-out requirement to specific information sharing activities, practices, or relationships which raise appropriate concerns, or failing that, to exempt from the opt-out requirement those legitimate activities, practices, or relationships with third parties. In addition, we believe that the study of affiliate information sharing required by H.R. 10 represents a prudent course at this time for identifying any future problems that should be addressed in law.

ACB would also oppose an opt-in requirement for information sharing with third parties. While this idea might seem attractive to some people in theory, the real-life impact of such a draconian requirement would mark the effective end of many marketing activities. Consumers would stand to lose the most from such a mandate, because they would lose access to information about many of the products and services that can be offered today as a result of appropriate information sharing arrangements.

Finally, ACB would oppose any proposal to create a private right of action as a means of enforcing privacy protection requirements. Such a right of action has the potential for flooding banks - particularly smaller, community banks - with frivolous litigation, thereby hindering their ability to serve their customers and communities. We believe that the bill's use of functional regulation represents the best means of enforcing the privacy protection requirements in H.R. 10.

#### **Conclusion**

As I conclude my statement, I would like to reiterate a point that I made at the outset of this testimony. In addition to working in the financial services industry, our members are also consumers. The practices in which they engage affect all of us. In order to maintain the trust and confidence of their customers, our members are committed to not engaging in excessive or abusive information sharing practices. They just want the continued ability to efficiently serve the financial needs of their customers and local community.

While financial information privacy has been a hot-button issue with the general public, it should not be forgotten that the financial services industry represents just one segment of our nation's economy, and the segment that is most secure. With every transaction you make - whether with a financial institution, a department store, a mail-order catalog company, or other business - information is created. Sometimes, the data you generate may be found later on someone's mailing or telemarketing list, but if it does, it most likely did not come from a financial institution.

While the information sharing practices of financial institutions should be examined by Congress, as these hearings do, other industries must be required to participate in the effort to reassure the public that their personal information will be protected. And with the ever expanding use of the Internet, the importance of their inclusion is almost certain to increase.

Again, Madame Chairwoman, let me commend you for holding these very important hearings and thank you for the opportunity to testify today on behalf of America's Community Bankers. We look forward to working closely with you, the Congress, federal regulators, and the general public to protect the personal financial information privacy rights of consumers. Speaking on behalf of our member institutions, I can assure you that we at ACB will do our part.



WRITTEN REPOSES TO QUESTIONS SUBMITTED BY  
CONGRESSMAN BRUCE VENTO (D-MN)

ROBERT R. DAVIS, DIRECTOR OF GOVERNMENT RELATIONS  
AMERICA'S COMMUNITY BANKERS

What are the specific cost problems with an annual disclosure of privacy policies? Couldn't this easily be met with a statement insert? Or as part of the routine information available in a monthly statement? What kinds of costs does this present?

ACB's official policy position on customer information privacy states that: "ACB supports requiring all financial institutions to develop an individual privacy protection policy that applies to all bank products or products shared with partners or through other relationships, and provide that policy to all customers." Our policy position recommends that an institution be required to provide each customer with its privacy protection policy once, unless substantive changes are made to the policy.

The costs associated with a disclosure requirement depend wholly on the specific demands of the mandate, such as frequency of notice. These costs would be substantially increased if financial institutions were required to provide annual notice as part of a separate mailing or transmission, as required by several bills proposed by members of Congress. These costs would obviously be mitigated if the disclosure requirement allowed financial institutions to provide notice as part of a routine statement, mailing, or transmission. Even so, an annual disclosure requirement would still entail additional production and delivery costs.

In requiring an annual disclosure of privacy protection policies, H.R. 10 does not currently speak to the issue of how the annual notice must be provided. If enacted in current form, the bill would seem to leave this matter to the assigned regulators. While we believe that a one-time notice procedure is sufficient to inform customers of an institution's privacy protection policy (with additional notification required if policies are changed), ACB would recommend that any annual disclosure requirement explicitly allow financial institutions to provide such notice as part of a routine statement, mailing, or transmission.

What is a legitimate reason to share a consumer's account number (coded or not) with any marketer WITHOUT that consumer's consent or knowledge?

ACB believes that there is never any circumstance where a charge should be placed against a consumer's account for a marketed product without that consumer's express consent and knowledge via express notification by the seller that the charge is being placed. As a practical matter, however, most consumers do not always have their account numbers available to authorize a charge for a desired product.

The ability to have an order processed in one conversation is one of the attractions of the telemarketing product/service distribution method. If the account information, perhaps with the account number scrambled but with the authorization code available (or *vice versa*), is available to complete the transaction, better customer service can result. (The payment authorization code that is not part of the embossed account numbers on the typical credit card can be used as a type of personal identification number for on-line credit card transactions.) If the risk of improper charges is deemed to be too great for this convenience to be offered, procedures will have to be changed, but that is not an unambiguous benefit to consumers. Of course, the possibility of the sharing of the account information, with a description of the procedures to be followed, should be included up-front and clearly disclosed to the bank customer/consumer.

You suggest that Congress first determine which activities, practices, or relationships justify a required opportunity for a consumer to opt out, and apply that requirement just to those activities. If you had to compile that list, what would you put on it?

As stated in our testimony, ACB does not oppose H.R. 10's provision requiring an opportunity for customers to opt out of having their personal, non-public information shared with non-affiliated third parties. We are, however, concerned that the bill's current approach, even with its current exceptions, could have the unintended effect of unfairly discriminating against community banks which use third parties for the same purposes that larger banks use affiliates. H.R. 10's blanket opt-out requirement on information sharing activities with third parties, even with its exceptions, could preclude community banks from engaging in new relationships that result from the rapid expansion in marketing technology.

If Congress believes that an opt-out requirement is indeed necessary to protect customer information privacy, ACB would recommend a better, more direct approach to reach that goal. Instead of establishing a blanket opt-out requirement for information sharing with third parties, as H.R. 10 currently does, Congress should target specific activities, practices, and relationships that warrant an opportunity for consumers to opt out and apply such a requirement only to those activities. Such an approach would protect consumers, while helping to prevent any harmful, unintended consequences from occurring.

**For example, Congress may determine that an opt-out opportunity should be provided for information sharing activities involving the marketing by third parties of their own products to a bank's customers. If so, Congress should impose an opt-out requirement on those specific activities. By doing so, Congress could achieve its goal of protecting consumer information privacy, while not unintentionally interfering with other information sharing activities, such as those necessary for smaller banks to engage in joint ventures and multiple-party agreements. Because it is impossible to anticipate today all of the various information sharing arrangements of tomorrow, a blanket opt-out approach could prove counterproductive in the future. We strongly urge Congress to take this more direct approach toward protecting customer information privacy.**

The provisions in H.R. 10 require an affirmative and continuing obligation to respect privacy do not create a private right of action, but instead create a FDICIA-like scheme of regulatory guidelines. Why do you think it would create a private right of action? What is the problem in your view with that if it were to be created?

**ACB appreciates the fact that the customer information privacy protection provisions in H.R. 10, as passed by the House, are to be enforced by an institution's functional regulator. We are concerned, however, that Section 501 has the potential for being misconstrued as providing a basis for a private right of action under common law.**

**The explicit or implicit creation of a private right of action has the potential for flooding banks, particularly smaller community banks, with frivolous litigation and hindering their ability to serve their customers. If Section 501 is retained, we asked that it be modified to specifically preclude any private right of action, or listed either as a non-binding statement of legislative intent or as part of Congressional findings.**



**Testimony of Michael D. Kloiber  
President/CEO of Tinker Federal Credit Union**

**on behalf of  
The National Association of Federal Credit Unions**

**Subcommittee on Financial Institutions and Consumer Credit  
Committee on Banking and Financial Services  
United States House of Representatives**

*Financial Privacy*

**July 20, 1999**

---

**National Association of Federal Credit Unions  
P.O. Box 3769 ♦ Washington, DC 20007  
703-522-4770**

The National Association of Federal Credit Unions (NAFCU), the only national organization exclusively representing the interests of our nation's federally chartered credit unions, appreciates this opportunity to appear before the Financial Institutions and Consumer Credit Subcommittee. Financial privacy issues, as they relate to the "*Financial Services Act of 1999*," are of great importance to our nation's approximately 11,000 member-owned credit unions. NAFCU itself is comprised of nearly 1,100 federal credit unions—non-profit financial cooperatives from across the nation--that collectively hold almost 70 percent of total federal credit union assets. In terms of individual credit union members, NAFCU-member credit unions serve the financial needs of approximately 25 million individual credit union members.

NAFCU and the entire credit union community welcomes this opportunity to participate in the discussion regarding privacy policies and provisions as they relate to the effective delivery of financial services. NAFCU takes seriously its responsibility to serve both as an advocate and as a liaison between the federal credit union community and policymakers in Washington. This role has been particularly critical over the course of the past year, as credit unions have worked with Congress and the National Credit Union Administration (NCUA) to address this issue.

NAFCU applauds the members of this Subcommittee as well as the members of the full Committee for the degree of personal interest they and their staffs have shown concerning this issue. Your continued interest in the unique concerns of the credit union community is reflected in the financial privacy issues we will discuss today.

### Credit Unions and Privacy

NAFCU believes that all financial institutions should have privacy policies and should disclose them to their members/customers. Because of their unique ownership structure and chartering laws, federal credit unions already go the extra mile in protecting their members' financial information.

Credit unions place a high value on protecting their members' financial records while at the same time delivering cost-effective financial services. As not-for-profit financial institutions, credit unions take the cooperative approach to doing business. A credit union's "*bottom line*" is *not* money. It is service. It is conducting affairs that meet the needs and interests of all its members. This contrasts with the "*bottom line*" of a commercial enterprise, which is simply profit.

The cooperative nature of credit unions also allows member-owners to have a voice in the day-to-day operation of their credit union. All credit unions have a democratically elected board of directors comprised of volunteers. If members are not satisfied with their board, they can elect new board members.

The service and member-ownership focus of credit unions provides credit union members with an unusual degree of security about their financial privacy. Democratically-elected boards are sensitive to their members' concerns for financial privacy and act on these concerns out of a service commitment to their members.

### Online Privacy

For credit unions, the Internet represents both opportunity and responsibility. The Internet provides an unparalleled opportunity to deliver cost-effective services to members, whenever and wherever they need them. Of the many challenges of the Internet, privacy, however, has risen above them all as the number one concern voiced by web-users when going online. In June 1998, the Federal Trade Commission (FTC) reported to Congress that:

“increasing numbers of consumers are concerned about how their personal information is used in the electronic marketplace. The research indicates that consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information.” (Federal Trade Commission, Privacy Online: A Report to Congress, June 1998)

These concerns need to be addressed since every day more financial institutions, including credit unions, start web sites. According to a Callahan and Associates May 1999 survey, there are over 2,000 credit union websites, with four more starting every day.

Nowadays, consumers simply do not go on-site to brokerages or financial institutions. In today's marketplace an individual can complete most financial transactions online without ever stepping foot into a brick and mortar building. Because of this, NAFCU recommends to all of its members that they post their privacy policies on their websites. It is important for the members to know why they need to give their information, what it will be used for and who else will be able to view that information.

NAFCU believes that, for credit unions, privacy is a matter of respect for their members. When credit union members feel secure in the confidence of their financial transactions—and many of them already feel this way—they will increasingly turn to the convenient, cost effective opportunities of alternative financial delivery systems, such as the

Internet.

### Committee Questions

In the letter inviting NAFUCU to participate in this hearing, NAFUCU was asked to submit our views on the following questions:

**1) For what purposes do your institutions collect and share customer information with affiliates and non-affiliates?**

Member information is collected for many reasons. One reason is that it allows the credit union to better serve its members. For example, it is the credit union's responsibility to protect its members from fraudulent activity. Credit unions who offer credit card accounts can track purchases of their members. By monitoring these transactions, the credit union can detect unusual spending patterns that may indicate fraud, thus preventing further loss to the member. In this instance, privacy is protected, not diminished, by the credit unions collection of member information.

Protecting their members against fraud is a high priority for credit unions. In addition to the example above, credit unions use members' personal information to help prevent check fraud and other types of fraud through the use of technology designed to detect such activities. Unfortunately, some consumers may see this collection of information as a nuisance or invasion of privacy, but in fact it is done for their protection.

In terms of sharing this information with affiliates and non-affiliates, some credit unions contract for services with their credit union service organization (CUSO) and/or third party vendors to help in areas such as marketing, ATM services, fund transfers, mortgage lending and loan processing. Of the credit unions we found that contract with third party



vendors, *all* of the contracts include agreements that protect the privacy of their members with regard to the use, confidentiality, and disclosure of information.

**2) Significant debate is occurring over whether financial institutions should be allowed to share customer information with their affiliates and non-affiliated third parties. Please comment on the benefits of information sharing and whether you believe additional protections are needed under the Fair Credit Reporting Act or other laws. Please provide comments specifically addressing the privacy provisions in H.R. 10 as passed by the House. In particular, please discuss the exceptions that are in the bill and whether they are sufficient to permit typical, everyday business transactions to continue.**

NAFCU and member credit unions agree that members' financial information should remain private. Our commitment to our member-owners demands no less. However, our members are also individuals who have agreed to participate in a financial delivery service and who each may have differing levels of comfort with the sharing of information. H.R. 10 recognizes, for example, that sharing certain kinds of information is a prerequisite to completing certain basic financial transactions. However, as under H.R. 10, sharing information can allow credit unions to better serve their members, particularly those who have a higher level of tolerance for the more fluid flow of data on the Internet.

Sharing provides the basis for more economical and better services for credit union members. Sharing of information involving "unrelated use" (as defined by H.R. 10) will facilitate trade and reduce the costs of bringing new technology, products and services to the marketplace. In terms of the Fair Credit Reporting Act, as amended in 1996, NAFCU

believes that it adequately protects the privacy of personal consumer information. We do wish to ensure, however, that the Fair Credit Reporting Act does not become an obstacle to implementing any sharing arrangements deemed appropriate by Congress in H.R. 10, especially as they relate to interactions with affiliates.

In reviewing the specific provisions of the *Financial Services Act of 1999*, (H.R. 10), it is clear that the legislation for the most part does not directly apply to credit unions. However, Title V, *Privacy of Consumer Information*, will have a direct impact on the entire credit union community. There are three main issues that NAFCU would like to address in relation to Title V: the "opt-out" provision; the affiliate relationship; and, the disclosure of information to third party vendors.

#### A. "Opt-Out" Provision

NAFCU believes that Congress took the correct approach in adopting the "opt-out" provision. Traditionally, credit unions provide the best service for the lowest cost. This provision will allow credit unions to continue to serve their members in the most efficient manner possible, given the individual member's tolerance for shared information. However, there should be a discussion on exactly how this provision will be managed. Congress should note that in some cases the sharing of information can help the consumer. As we discussed before, credit unions use information for safety and soundness purposes--to protect against fraud, bankruptcy losses and other instances of risk or loss. Because of their cooperative nature, any losses that are incurred by a credit union are in turn passed on and borne by the entire membership.

**B. Affiliate Definition**

NAFCU believes that H.R. 10 requires a better understanding of what an “affiliate” is. The importance of the affiliate exemption hinges largely on whether a credit union service organization (CUSO), as it is currently defined, meets H.R. 10’s definition of the term “affiliate” under Title V. We believe that H.R. 10 intended to include CUSOs and that care should be taken to ensure that this is done.

H.R. 10 defines an affiliate as “any company that controls, is controlled by, or is under common control with another company.” This definition suggests that a corporate relationship exists between the companies based on ownership—either one company owns the other, or both are owned by another entity.

However, the structure of CUSOs does not fit this definition neatly. Under the CUSO rule (see Appendix A), a credit union affiliates with a CUSO by investing in, and/or loaning to, the CUSO. An investing federal credit union is deemed either an equity holder of a corporation, member of a limited liability company, or a limited partner in a limited partnership. As such, the federal credit union does not carry legal responsibilities for the management or control of the CUSO, which serves to limit its legal liability. The rule also limits the amount of investments and loans a federal credit union can make to a CUSO; recommends that a CUSO not be treated as a department of the credit union; and, prohibits officials and senior management employees of the credit union from receiving compensation for any assistance provided in the operation of the CUSO. The general push is towards corporate separateness.

It is critical that a CUSO be included in the definition of an affiliate. Without a clearer understanding of "affiliate," credit unions could be placed under burdens never intended by H.R. 10. CUSOs perform many operational services on behalf of credit unions, such as: credit card and debit card services, check cashing and wire transfers, ATM services, electronic funds transfer services, consumer and mortgage loan origination, loan processing and accounting services. Many federal credit unions, particularly smaller institutions, rely heavily on the services of CUSOs because of their limited ability to perform these services in-house. Therefore, an enormous burden will be placed on federal credit unions if CUSOs are treated as third parties under H.R. 10.

### **C. Third Party Vendors**

As discussed earlier credit unions do use CUSOs and third party vendors to perform different types of operational services. For example, one federal credit union uses a third party vendor to tally the results of its board elections. For authenticity purposes, the credit union must send all the names of its members and their account numbers to the vendor, who then calculates the results and sends the information back to the credit union. This information is needed to protect against fraud in the election process. The credit union saves its members money by using the third party vendor. NAFCU has found that in most cases the vendor can provide the service at less cost than if the credit union handled the matter in-house. In such cases, most credit unions make third party vendors sign a confidentiality agreement, and in the process money is saved for members without compromising privacy. Virtually all credit unions have some type of third party arrangements.

**3) What effect would more stringent privacy laws (i.e. prohibition on information sharing with affiliates) have on your institutions?**

Depending on restrictions on third party vendor and the way a CUSO is treated, the legislation may have a major impact on the way a credit union operates and more importantly on their membership. As discussed earlier, due to the credit union's cooperative nature, any increase in the way a credit union does business will be passed on to its members.

**4) Do you have any suggestions for approaches that would strengthen consumers' confidence in their financial privacy, but would not hinder your daily operations?**

Currently, NAFCU is attempting to gain a clearer understanding of credit union privacy practices and our policy-makers are in the process of developing formal principles and policies on the issue. As a whole, NAFCU believes that credit unions currently do an excellent job of protecting their members' financial records. We will be pleased to share additional views and recommendations with the committee as our internal policy formulation process moves forward.

**Conclusion**

The National Association of Federal Credit Unions appreciates this opportunity to participate in this important discussion. Should any members of the Committee have questions regarding the credit union community's view on financial privacy or any other matters affecting their credit union constituents, please contact NAFCU. We look forward to working with you and your staffs throughout the 106th Congress.

## Appendix A

## Credit Union Service Organizations

712-1

**Part 712**

CREDIT UNION SERVICE ORGANIZATIONS (CUSOs) PART 712

August 1998

**Credit Union Service Organizations (CUSOs)**

§ 712.1-§ 712.3

**§ 712.1 What does this part cover?**

This part establishes when a Federal credit union (FCU) can invest in and make loans to CUSOs. CUSOs are subject to review by NCUA. This part does not apply to corporate credit unions that have CUSOs subject to § 704.11 of this title. This part does not apply to state-chartered credit unions or the subsidiaries of state-chartered credit unions that do not have FCU investments or loans.

**§ 712.2 How much can an FCU invest in, or loan to, CUSOs, and what parties may be involved?**

- (a) Investments. An FCU's total investments in CUSOs must not exceed, in the aggregate, 1% of its paid-in and unimpaired capital and surplus as of its last calendar year-end financial report. For purposes of paragraphs (a) and (b) of this section, "paid-in and unimpaired capital and surplus" means shares and undivided earnings. An FCU can only invest in a CUSO as an equity holder of a corporation, as a member of a limited liability company, or as a limited partner of a limited partnership.
- (b) Loans. An FCU's total loans to CUSOs must not exceed, in the aggregate, 1% of its paid-in and unimpaired capital and surplus as of its last calendar year-end financial report. Loan authority is independent and separate from the 1% investment authority of subsection (a) of this section.
- (c) Parties. An FCU may invest in, or loan to, a CUSO by itself, or with other credit unions, or with non-depository institution parties not otherwise prohibited by § 712.6 of this part.

**§ 712.3 What are the characteristics of and what requirements apply to CUSOs?**

- (a) Structure. An FCU can invest in or loan to a CUSO only if the CUSO is structured as a corporation, limited liability company, or limited partnership. For purposes of this part, "corporation" means a legally incorporated corporation as established and maintained under relevant state law. For purposes of this part, "limited partnership" means a legally established limited partnership as established and maintained under relevant state law. For purposes of this part, "limited liability company" means a legally established limited liability company as established and maintained under relevant state law, provided that the FCU obtains written legal advice that the limited liability company is a recognized

- legal entity under the applicable laws of the state of formation and that the limited liability company is established in a manner that will limit potential exposure of the FCU to no more than the amount of funds invested in, or loaned to, the CUSO.
- (b) Customer base. An FCU can invest in or loan to a CUSO only if the CUSO primarily serves credit unions, its membership, or the membership of credit unions contracting with the CUSO. However, if in order for the CUSO to provide a permissible service it is necessary for the CUSO to own stock in a service provider not meeting the customer base requirement, then the CUSO can buy and own the minimal amount of service provider stock necessary to provide the service without violating the customer base requirement.
  - (c) Federal credit union accounting. An FCU must account for its investments in or loans to a CUSO in conformity with "generally accepted accounting principles" (GAAP).
  - (d) CUSO accounting; audits and financial statements; NCUA access to information. An FCU must obtain written agreements from a CUSO, prior to investing in or lending to the CUSO, that the CUSO will:
    - (1) Account for all its transactions in accordance with GAAP;
    - (2) Prepare quarterly financial statements and obtain an annual opinion audit, by a licensed Certified Public Accountant, on its financial statements in accordance with "generally accepted auditing standards" (GAAS); and
    - (3) Provide NCUA and its representatives with complete access to any books and records of the CUSO and the ability to review CUSO internal controls, as deemed necessary by NCUA in carrying out its responsibilities under the Act.
  - (e) Other laws. A CUSO must comply with applicable Federal, state and local laws.

**§ 712.4 What must an FCU and a CUSO do to maintain separate corporate identities?**

- (a) Corporate separateness. An FCU and a CUSO must be operated in a manner that demonstrates to the public the separate corporate existence of the FCU and the CUSO. Good business practices dictate that each must operate so that:
  - (1) Its respective business transactions, accounts, and records are not intermingled;
  - (2) Each observes the formalities of its separate corporate procedures;
  - (3) Each is adequately financed as a separate unit in the light of normal obligations reasonably foreseeable in a business of its size and character;
  - (4) Each is held out to the public as a separate enterprise;
  - (5) The FCU does not dominate the CUSO to the extent that the CUSO is treated as a department of the FCU; and
  - (6) Unless the FCU has guaranteed a loan obtained by the CUSO, all borrowings by the CUSO indicate that the FCU is not liable.
- (b) Legal opinion. Prior to an FCU investing in a CUSO, the FCU must obtain written legal advice as to whether the CUSO is established in a manner that will limit potential exposure of the FCU to no more than the loss of funds invested in, or lent to, the CUSO. In addition, if a CUSO in which an FCU has an investment plans to change its structure under § 712.3(a), an FCU must also obtain prior, written legal advice that the CUSO will remain established in a manner that will limit potential exposure of the FCU to no more than the loss of funds invested in, or loaned to, the CUSO. The legal advice must address factors that have led courts to "pierce the corporate veil" such as inadequate

capitalization, lack of separate corporate identity, common boards of directors and employees, control of one entity over another, and lack of separate books and records. The legal advice may be provided by independent legal counsel of the investing FCU or the CUSO.

**§ 712.5 What activities and services are preapproved for CUSOs?**

NCUA may at any time, based upon supervisory, legal, or safety and soundness reasons, limit any CUSO activities or services, or refuse to permit any CUSO activities or services. Otherwise, an FCU may invest in, loan to, and/or con-tract with only those CUSOs that are sufficiently bonded or insured for their specific operations and only provide one or more of the following activities and services related to the routine, daily operations of credit unions:

- (a) Checking and currency services:
  - (1) Check cashing;
  - (2) Coin and currency services; and
  - (3) Money order, savings bonds, travelers checks, and purchase and sale of U.S. Mint commemorative coins services;
- (b) Clerical, professional and management services:
  - (1) Accounting services;
  - (2) Courier services;
  - (3) Credit analysis;
  - (4) Facsimile transmissions and copying services;
  - (5) Internal audits for credit unions;
  - (6) Locator services;
  - (7) Management and personnel training and support;
  - (8) Marketing services;
  - (9) Research services; and
  - (10) Supervisory committee audits;
- (c) Consumer mortgage loan origination;
- (d) Electronic transaction services:
  - (1) Automated teller machine (ATM) services;
  - (2) Credit card and debit card services;
  - (3) Data processing;
  - (4) Electronic fund transfer (EFT) services;
  - (5) Electronic income tax filing;
  - (6) Payment item processing;
  - (7) Wire transfer services; and
  - (8) Cyber financial services;
- (e) Financial counseling services:
  - (1) Developing and administering Individual Retirement Accounts (IRA), Keogh, deferred compensation, and other personnel benefit plans;
  - (2) Estate planning;
  - (3) Financial planning and counseling;
  - (4) Income tax preparation;
  - (5) Investment counseling; and



- (6) Retirement counseling;
- (f) Fixed asset services:
  - (1) Management, development, sale, or lease of fixed assets; and
  - (2) Sale, lease, or servicing of computer hardware or software;
- (g) Insurance brokerage or agency:
  - (1) Agency for sale of insurance;
  - (2) Provision of vehicle warranty programs;
- (h) and
- (3) Provision of group purchasing programs;
- (i) Leasing:
  - (1) Personal property; and
  - (2) Real estate leasing of excess CUSO property;
- (j) Loan support services:
  - (1) Debt collection services;
  - (2) Loan processing, servicing, and sales; and
  - (3) Sale of repossessed collateral;
- (k) Record retention, security and disaster recovery services:
  - (1) Alarm-monitoring and other security services;
  - (2) Disaster recovery services;
  - (3) Microfilm, microfiche, optical and electronic imaging, CD-ROM data storage and retrieval services;
  - (4) Provision of forms and supplies; and
  - (5) Record retention and storage;
- (l) Securities brokerage services;
- (m) Shared credit union branch (service center) operations;
- (n) Student loan origination;
- (o) Travel agency services; and
- (p) Trust and trust-related services:
  - (1) Acting as administrator for prepaid legal service plans;
  - (2) Acting as trustee, guardian, conservator, estate administrator, or in any other fiduciary capacity; and
  - (3) Trust services.

**§ 712.6 What activities and services are prohibited for CUSOs?**

- (a) General. CUSOs must not acquire control of, either directly or indirectly, another depository financial institution, nor invest in shares, stocks, or obligations of an insurance company, trade association, liquidity facility or similar organization, corporation, or association.
- (b) Real estate brokerage CUSO. An FCU may not invest in, or loan to, a CUSO engaged in real estate brokerage services after April 1, 1998, except as provided in § 712.9.

**§ 712.7 What must an FCU do to add activities or services that are not preapproved?**

In order for an FCU to invest in and/or loan to a CUSO that offers an unpreapproved activity or service, the FCU must first receive NCUA Board approval. The request for NCUA Board

approval of an unpreapproved activity or service must include a full explanation and complete documentation of the activity or service and how that activity or service is associated with routine credit union operations. The request must be submitted jointly to your Regional Office and to the Secretary of the Board. The request will be treated as a petition to amend § 712.5 and NCUA will request public comment or otherwise act on the petition within 60 days after receipt.

**§ 712.8 What transaction and compensation limits might apply to individuals related to both an FCU and a CUSO?**

- (a) Officials and Senior Management Employees. The officials, senior management employees, and their immediate family members of an FCU that has outstanding loans or investments in a CUSO must not receive any salary, commission, investment income, or other income or compensation from the CUSO either directly or indirectly, or from any person being served through the CUSO. This provision does not prohibit such FCU officials or senior management employees from assisting in the operation of a CUSO, provided the officials or senior management employees are not compensated by the CUSO. Further, the CUSO may reimburse the FCU for the services provided by such FCU officials and senior management employees only if the account receivable of
- (1) the FCU due from the CUSO is paid in full at least every 120 days. For purposes of this paragraph (a), “official” means affiliated credit union directors or committee members. For purposes of this paragraph (a), “senior management employee” means affiliated credit union chief executive officer (typically this individual holds the title of President or Treasurer/Manager), any assistant chief executive officers (e.g. Assistant President, Vice President, or Assistant Treasurer/Manager) and the chief financial officer (Comptroller). For purposes of this paragraph (a), “immediate family member” means a spouse or other family members living in the same household.
- (b) Employees. The prohibition contained in paragraph (a) of this section also applies to FCU employees not otherwise covered if the employees are directly involved in dealing with the CUSO unless the FCU’s board of directors determines that the FCU employees’ positions do not present a conflict of interest.
- (c) Others. All transactions with business associates or family members of FCU officials, senior management employees, and their immediate family members, not specifically prohibited by paragraphs (a) and (b) of this section must be conducted at arm’s length and in the interest of the FCU.

**§ 712.9 When must an FCU comply with this part?**

- (a) Investments. An FCU’s investments in CUSOs in existence prior to April 1, 1998, must conform with this part not later than April 1, 2001, unless the Board grants prior approval to continue such investment for a stated period.
- (b) Loans. An FCU’s loans to CUSOs in existence prior to April 1, 1998, must conform with this part not later than April 1, 2001, unless:
- (1) The Board grants prior approval to continue the FCU’s loan for a stated period; or
  - (2) Under the terms of its loan agreement, the FCU cannot require accelerated repayment without breaching the agreement.



September 8, 1999

The Honorable Bruce F. Vento  
 Committee on Banking and Financial Services  
 2129 Rayburn House Office Building  
 Washington, D.C. 20515

Dear Representative Vento:

I am writing on behalf of Michael Kloiber, President/CEO of Tinker Federal Credit Union, who was a recent witness for the Financial Institutions and Consumer Credit Hearings on Emerging Financial Privacy Issues. After Mr. Kloiber's testimony, you forwarded two questions to him through the National Association of Federal Credit Unions. The purpose of this letter is to answer those questions.

1. What kinds of marketing of their customers' information do credit unions typically engage in, if any?

The short answer is simply "none." Unlike for-profit businesses, credit unions do not look upon member mailing lists as commodities to be sold. I am not aware of any credit union that would sell its membership list to any outside vendor. We do sometimes contract with outside firms to offer our members non-credit union products, such as life insurance. In those instances, we provide a mailing list to the vendor, with the strict understanding that the list is to be used only for marketing the specific product we have negotiated on behalf of the members.

In addition, credit unions that own a Credit Union Service Organization (CUSO) also sometimes share member information with the CUSO so it can develop products and services tailored to the members' needs. It's important to note that a CUSO is a wholly owned subsidiary of the credit union.

2. Do most credit unions have privacy policies? Do you have "best practices"?

Once again, the short answer is "yes." Protecting member privacy is one of the basic philosophies of the credit union movement. While I can't speak for all credit unions, I think it's safe to say in general that credit unions have written policies requiring employees to maintain strict confidentiality when it comes to all member information. In

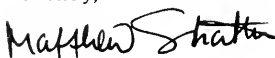
addition, credit unions require vendors, such as statement processing businesses, to maintain confidentiality of members' names, addresses and account information.

When you ask about "best practices", are you asking if credit unions evaluate their procedures to determine what works best and then share that information? If so, the answer is again "yes." The cooperative spirit of the credit union movement means that credit unions of all sizes regularly share information with each other, both formally and informally. Trade associations at the state and national levels gather and share information about all aspects of the credit union business through publications, conferences and monthly meetings. In addition to such formal information sharing, credit union management and staff routinely contact each other for advice and counsel. I'm not aware of a formal "best practices" program specifically related to privacy. However, if a privacy issue arose somewhere within the movement, you can be sure credit unions would be discussing it in meetings, in newsletters, on the web, and on the phone.

Credit unions are committed to maintaining the confidentiality of our members' financial information. We share information only to the extent necessary to deliver our products and services to the members themselves. It is important that we sometimes share information within the various departments of the credit union and between the credit union and our CUSO, but we do not sell or give that information to third parties unrelated to helping us provide products and services to our members.

If you have any other questions, please call me or Mr. Kloiber. We will be happy to help any way we can.

Sincerely,



Matthew Stratton  
Vice President of Marketing

cc: Michael D. Kloiber, President/CEO



Testimony for the House Subcommittee on Financial Institutions and Consumer Credit

Hearing on Emerging Financial Privacy Issues

Richard A. Barton  
Senior Vice President for Congressional Relations  
The Direct Marketing Association

July 20, 1999

## I. INTRODUCTION

Madam Chairwoman and distinguished members of the Subcommittee, my name is Richard A. Barton, Senior Vice President for Congressional Relations for the Direct Marketing Association. It is an honor to be testifying before you today.

The Direct Marketing Association ("The DMA") appreciates the opportunity to testify before you today. The DMA is an international trade association representing more than 4500 companies engaged in all forms of direct marketing, primarily by mail and telephone, and increasingly by electronic commerce, a marketing tool that we believe will grow exponentially in the next few years. Direct marketing is of enormous importance to the American economy, accounting in 1998 alone for more than \$1.3 trillion in sales of goods and services.

## II. DATA PRACTICES IN THE MARKETING INDUSTRY

Information is essential to this important and highly popular method of purchasing products and services. Information permits marketers to reach the consumers and businesses who are most likely to be interested in the product or service in question. Marketers collect and use information about individuals (e.g. names, addresses, telephone numbers, buying preferences, hobbies, activities, to name just a few) and general demographic information garnered from public sources such as the

U.S. census. This data is used to predict prospective customers' interests or preferences and to contact them with offers likely to be of interest to them. The single and only purpose of information access and use in the marketing process is to provide consumers and businesses with product and service offers that are useful and relevant to their interests and needs.

Data used by marketers is collected from a very wide array of sources, including publicly available information such as telephone directories, public record information, census data (used to estimate family income, for example), consumer surveys contained in product packages to which consumers voluntarily respond, and data regarding prior purchases. Many companies make their customer lists available for rental (lists are very rarely "sold") or exchanged. Credit card companies may prepare lists based on customer purchases, for example, lists of potential customers of golfing equipment based on their past golf (or other sports) related purchases.

While the collection and use of these data may be somewhat confusing to the layman, the end result is as benign as the receipt of a solicitation for a product, service, or charitable or political contribution. Lists are compiled in the aggregate for marketing purposes and normally do not reveal specific data about an individual or population upon which they might have been based, such as a list of individual purchases or transactions.

### III. SELF-REGULATION AND EXISTING LAW

However, this does not mean that direct marketers are not sensitive to privacy issues. On the contrary, the entire direct marketing process depends on consumer trust, including the protection of consumers' very legitimate privacy concerns.

To that end, The DMA has long promoted the concept of "notice and opt out." In other words, we have long expected companies engaged in direct marketing to inform customers of their policies regarding the use of information about them and, if they in any way transmit that information to third parties in the form of marketing lists, to give the customer a chance to say "no!" and to exercise control over information about them by opting out of such disclosures.

The Direct Marketing Association has also sponsored for many years both the Mail Preference Service and the Telephone Preference Service. These are nationally promoted lists of citizens who do not want to receive mail or telephone solicitations. Historically, those opting out of receiving these types of solicitations is a fraction of the direct marketing customer universe, less than 2-3%. In the last three years, the number of the individuals on the MPS file has risen from 2,949,367 in 1997 to a current 3,357,531. The Telephone Preference Service file has increased from 993,317 in 1997 to 2,358,476 in 1999.

We are currently in the process of developing a similar E-Mail Preference Service.

However, recognizing that we needed to take even stronger measures to ensure the success of self-regulation, we have developed a program known as the Privacy Promise to American Consumers, which went into effect on July 1 of this year – just three weeks ago. The program is really very simple in concept, but sweeping in effect.

From now on, all members of the Direct Marketing Association will be required to:

- Publish clearly and conspicuously their own policies for the use of individual information and, if the information is to be used outside the company, to give the individual the right to opt out of

its use,

- Maintain their own in-house files of people who have requested to be removed from their internal lists, both for further solicitations and for dissemination to third parties, and
- Use The DMA's Mail Preference Service, Telephone Preference Service and, when it becomes available, E-Mail Preference Service.

If any company is found not to be following these principles, they will be publicly expelled from membership in the association.

In addition to these programs, The Direct Marketing Association maintains its **Guidelines for Ethical Business Practice**, which among other things contains extensive privacy guidelines. Our Committee on Ethical Business Practice enforces these guidelines. The committee hears complaints from many sources, particularly consumers, regarding the potential violation of these guidelines. If the committee, following a rigorous fact-finding process, finds that a company is violating the guidelines, it first tries to work with that company to correct the problem. Failing that, the company may be subject to public censure and dismissal from the association.

Furthermore, any company that commits to The DMA's privacy promise risks prosecution for deceptive trade practices by the FTC and state attorneys general if it does not abide by that promise. We believe that this level of self-regulation goes a long way toward meeting both the demands and the requirement for protection of privacy in this increasingly technological society.

Nevertheless, The Direct Marketing Association has also worked with Congress, the Federal Trade Commission, the Federal Communication Commission, the Postal Service, and others to develop legislation and regulation affecting marketing data collection, use or disclosure practices to meet specific privacy concerns raised by disclosures of particularly sensitive data. These laws and regulations include:

- Cable Communications Policy Act of 1984
- Electronic Communications Privacy Act of 1986
- Video Privacy Protection Act of 1988
- Computer Matching and Privacy Protection Act of 1988
- Telephone Consumer Protection Act of 1991
- Customer Proprietary Network Information (CPNI)
- Consumer Credit Reporting Reform Act of 1996
- Children's Online Privacy Protection Act of 1998
- Drivers Privacy Protection Act of 1998
- Health Insurance Portability and Accountability Act of 1996

As a result of these and other laws, data practices of the marketing industry are subject to regulation in many instances involving sensitive information. For example, marketing data is regulated under the Fair Credit Reporting Act to the extent that it is used for credit or employment purposes—decisions that may have an adverse effect on an individual. By contrast, where information is not sensitive in nature and the only "harm" to a consumer is that he or she will or will

not receive an offer for a product or service that he or she may be interested in, self-regulation is the norm.

#### **IV. POSSIBLE ADDITIONAL REGULATION**

The Subcommittee has asked our views with regard to pending financial privacy legislation and with regard to regulation of electronic commerce.

##### **A. General Observations**

The DMA is strongly committed to principles of notice and opt-out for disclosures to third parties for marketing purposes, and to self-regulation as the most appropriate and effective means of achieving privacy protection in marketing practices. Our privacy promise program should be given an opportunity to work before Congress imposes new layers of regulation on marketing practices. In particular, we urge Congress not to disturb self-regulation of ordinary marketing data obtained from financial institutions and not to sweep non-financial identifying information into this legislation.

With regard to electronic commerce, we strongly believe, as the FTC recently confirmed in its report to Congress on privacy released last week, that self-regulation coupled with robust enforcement of existing laws governing unfair and deceptive practices is sufficient at the present time. As FTC Chairman Pitofsky cautioned the House Telecommunications Subcommittee last week, Congress should be careful not to stifle the growth of electronic commerce through premature regulation that will be unnecessary if privacy self-regulation continues to spread at its current pace in this new medium.

##### **B. Comments on H.R. 10, as amended in the House:**

H.R. 10 contains provisions requiring the affected financial institutions to disclose their privacy policies and provide consumers with the ability to "opt out" of the sharing of nonpublic information with nonaffiliated third parties. These provisions are consistent with our own self-regulatory policies. As stated before, we believe strongly that self-regulation is working and is preferable to legislation. However, we do not oppose provisions covering the sensitive areas of privacy of medical information and so-called "pretext calling."

The amended H.R. 10 also contains provisions prohibiting the sharing of account numbers, credit card numbers, and other similar information under any circumstances with "telemarketers," and "direct mail marketers." We oppose these provisions as currently written because they would severely limit use of information that in encrypted or other encoded form is an important tool for marketers to insure the accuracy of their data, assist customers and businesses in making safe and secure transactions, and protect against fraud and theft.

In normal practice, when this type of information is passed on for direct marketing purposes, it is done in encoded form so that the data cannot be read or understood by just anyone. In fact, even the encoded data is rarely, if ever, seen by those who make the telemarketing calls or prepare the mail.



The Direct Marketing Association Guidelines for Ethical Business Practice states this general policy with regard to the transfer of account numbers:

“The DMA considers credit card numbers, checking account number, and debit account numbers to be personal information and therefore should not be transferred, rented, sold or exchanged when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the nature of such personally identifying numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers.”

A typical transaction occurs something like this. A financial institution prepares abstracts of customer files, combines them into a targeted marketing list and transmits the list to the third party for marketing purposes. Account numbers may be scrambled and the files are encrypted. The third party may further process the file by running it against other suppression files such as The DMA's Mail Preference Service and the Postal Service's "pander" file. Throughout the entire process, account numbers, if they are included, are either scrambled in varying orders according to different algorithms, or the numbers are replaced with alphas. The scrambled account number is never shown to the actual telemarketers or people responsible for the preparation of mail.

The account information thus encoded does have many useful purposes, some of which are important privacy and security enhancers.

1. It can provide a direct and unique way to identify customers and verify a purchase, reducing the chance for both error and fraud.
2. It can permit the institution selling the product or service to gather accurate and verified data for customer service purposes.
3. It is an important tool in improving the accuracy of mailing and telephone lists.
4. It can be an important tool in allowing the customer to charge a purchase to an existing account without having to reveal the number to the actual direct marketer, thus adding a further element of security.

Other witnesses with more experience in the technical details of the actual marketing process can provide you with more details. Suffice it to say that properly encrypted account data can actually increase the security of a transaction and provide important tools both to ease the process of a transaction and to positively identify a customer in the marketing process. H.R. 10 could remove these positive benefits to both business and the consumer.

Second, we are concerned that the definitions in the bill—particularly the definition of "nonpublic personal information"—are unclear because they tend to blur the differences between personally identifiable financial information and other types of personally identifiable information. They might be read to interfere seriously with use of certain non-financial identifying information to

make marketing databases more accurate. This result would do little or nothing to advance privacy, while compromising the accuracy of marketing. As a result, a significant number of mailings, for example, would go to the wrong address, and would not reach consumers who have chosen not to opt-out of receiving marketing offers. This would hardly be a victory for privacy, would undermine consumer choice, and would hurt a very important sector of the American economy.

## V. CONCLUSION

Thank you again for the opportunity to testify on this important subject. We would be happy to offer our assistance to the committee to work on legislation that assures the privacy of customers of financial institutions while at the same time preserving important marketing tools to businesses and customers alike.

### Contact:

Richard A. Barton  
Senior Vice President for Congressional Relations  
The Direct Marketing Association  
1111 19<sup>th</sup> Street, N.W. Suite 1100  
Washington, D.C. 20036  
Telephone: 202.861.2416  
e-mail: [rbarton@the-dma.org](mailto:rbarton@the-dma.org)

# Marketing

---

# Online

## Privacy Principles and Guidance



# MARKETING ONLINE

## PRIVACY PRINCIPLES AND GUIDANCE

*While The DMA's Guidelines apply to marketing in all media, the following principles and illustrations highlight issues unique to online and Internet marketing. They cover online notice and opt out, unsolicited marketing e-mail, and online data collection from or about children.*

### Online Notice and Opt Out

All marketers operating online sites, whether or not they collect personal information online from individuals, should make available their information practices to consumers in a prominent place. Marketers sharing personal information that is collected online should furnish individuals with an opportunity to prohibit the disclosure of such information.

#### The Online Notice

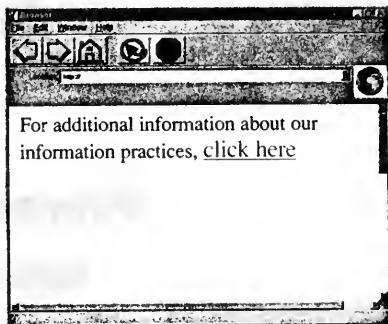
The notice should be easy to find, easy to read, and easy to understand.

- A marketer should post its notice so as to readily enable the consumer to learn about the marketer's information practices in a manner that permits a consumer effective choice over the collection and disclosure of personal information.

For example:

A marketer operating a World Wide Web site that collects personal information from individuals who visit it could post notice of its information practices on its home page or on the page where information is collected (e.g., survey questionnaire).

A marketer could provide an icon on its home page that, when clicked, will furnish the consumer with access to additional screens disclosing the marketer's information practices.



The notice should identify the marketer, disclose an e-mail and postal address at which it can be contacted, and state whether the marketer collects personal information online from individuals. If the marketer collects personal information online, the notice should contain disclosures about:

- The nature of personal information collected with respect to individual consumers.

Depending on the circumstances, information collected about a consumer may include:

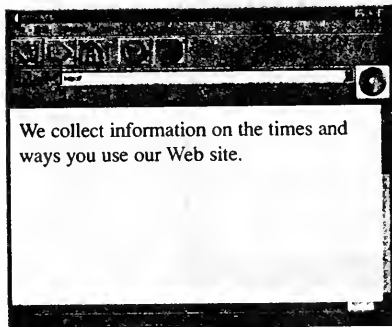
- contact or locator information (such as name, postal, and e-mail addresses),
- billing information (such as financial account and credit card number),
- transactional information (such as data on purchases a consumer makes),
- navigational information (such as data revealing consumers' preferences or the choices they make among the range of products, services, or sites, and the times of day they are made), and
- the content of correspondence or messages directed to a marketer.

For example, a marketer could include language such as:

"We keep the information you provide in responding to our questionnaire."

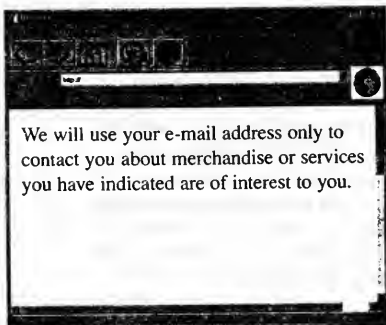
"We maintain your name, postal, and e-mail addresses, telephone number, and payment and order processing information. We also may keep information on your communications with our customer service representatives."

"We collect information on the times and ways you use our Web site."



• **The nature of uses of such information.**

The information may be used, for example, to ensure that a consumer is properly billed, for marketing by e-mail, or for evaluating and understanding consumer reactions to content, services, or merchandise offered online. It also may include using the consumer's name and address for marketing by mail or other media.



For example, a marketer could include language such as:

"We will use your e-mail address only to contact you about merchandise or services you have indicated are of interest to you."

"We use information for billing purposes and to measure consumer interest in our various services or pages."

• **The nature and purpose of disclosures of such information, and the types of persons to which disclosures may be made.**

This may include disclosure of names and postal and e-mail addresses to other merchants for marketing purposes or to

firms that conduct market research for the marketer, or disclosure of additional information for bill collection purposes.

• **The mechanism by which the individual may limit the disclosure of such information.**

An opt out will traditionally be the means offered to consumers to limit the disclosure of information collected about them.

**The Means of Opting Out**

**All marketers sharing personal information that is collected online should furnish consumers with the opportunity to opt out from the disclosure of such information. The notice and opt-out process should enable consumers to request that their personal information not be rented, sold, or exchanged.**

- Marketers' notices should clearly and accurately inform consumers of their opt-out choices (e.g., transfer of all information to third parties, contact by third parties in a particular medium, re-contact by the marketer, etc.)
- Marketers should suppress in a timely fashion the personal information of individuals who request that their personal information not be rented, sold, or exchanged.
- Whenever possible, marketers should provide consumers with the opportunity to opt out via e-mail.
- In opting out from lists used for online solicitation purposes, consumers may also seek to opt out from solicitations in other media, such as mail or telemarketing. Marketers should honor these consumer requests for opt outs from solicitations in other media.

I do not want (please check all that apply):

Transfer of information to third parties

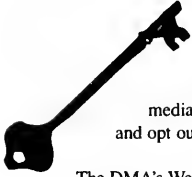
Contact by third parties

Future offers from us

click [here](#) to register your preferences

**As an illustration, The DMA's present notice of its Web site practices and opt out is reprinted below. The DMA's notice is limited because the type of consumer information collected at the site is limited. If, for example, sales were transacted or a chat room were sponsored at the site, then the notice would require additional disclosures.**

## The DMA Web Site Privacy Policy



For years the The DMA has developed guidelines and programs to meet consumer privacy expectations through notice of its information practices to consumers and by offering consumers the ability to remove their names from marketing lists. As interactive media evolve, The DMA renews its commitment to notice and opt out in this new medium.



The DMA's Web site is maintained by the Direct Marketing Association, Inc., 1120 Avenue of the Americas, New York, NY 10036-6700. You can reach us by phone at 212 768-7277.

This site recognizes the home server of visitors, but not their e-mail addresses. Therefore, individually identifiable e-mail addresses are not captured or stored for future use, unless you provide them by posting a message to The DMA. Data on visitors' home servers are aggregated for internal review and then discarded.

Persons who communicate with The DMA, and therefore supply The DMA with an e-mail address will receive future communications from the Association by e-mail. Persons who do not wish to receive e-mail messages from The DMA may notify the membership department by e-mail ([dma@the-dma.org](mailto:dma@the-dma.org)). E-mail addresses will NOT be disclosed or sold to other parties.

Persons who request information about The DMA, its services or educational events, and who supply the Association with their name and postal address will be added to our database to receive future Association mailings related to Association programs and events.

The DMA occasionally makes the lists of postal addresses volunteered on its Web site available to other carefully screened associations or companies whose products or services you may find of interest. If you no longer wish to receive such mailings, please copy your mailing label exactly (or clip it out) and send your request to The DMA's membership department at the above address, or you may contact the Association by e-mail ([dma@the-dma.org](mailto:dma@the-dma.org)).

## Unsolicited Marketing E-Mail

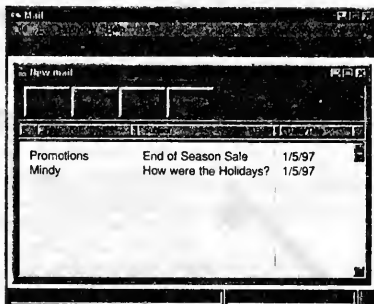
### 1. Online solicitations should be posted to newsgroups, bulletin boards, and chat rooms only when consistent with the forum's stated policies.

- To facilitate adherence to this principle, forum operators should publicize their policies regarding solicitations in their forums, for example, "We would like to send offers for valuable services and products that may be of interest to consumers."
- Marketers should inquire about the forum's policies before directing online e-mail solicitations to the forum.

### 2. Online e-mail solicitations should be clearly identified as solicitations and should disclose the marketer's identity. Marketers using e-mail should furnish consumers with whom they do not have an established business relationship with notice and a mechanism through which they can notify the marketer that they do not wish to receive future online solicitations. Marketers using e-mail should furnish consumers with whom they have an established business relationship with notice and a mechanism through which they can request that the marketer suppress their e-mail addresses from lists or databases rented, sold, or exchanged for online solicitation purposes.

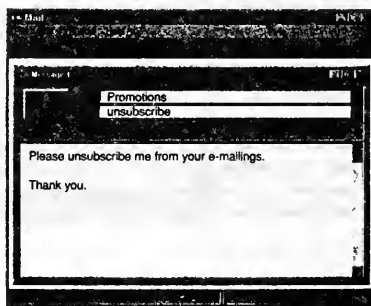
- Online solicitations should be identified in a way that allows recipients to readily recognize them as solicitations.

For example, a marketer should use clear language, such as "End-of-Season Sale," that ensures that—without reading more than the first paragraph—a consumer will recognize the e-mail message as a solicitation.



- Marketers should have systems in place that will honor consumer requests to not receive future online solicitations or, in the case of consumers with whom they have an established business relationship, to have their e-mail addresses removed from their lists or data bases that are made available for rental, sale, or exchange for online solicitation purposes.

For example, a marketer could say, "We value our relationship with you and if you wish to opt out of receiving further e-mail advertisements, let us know. To get on our opt-out list, all you have to do is send an "unsubscribe" message to ..."





- The identifying information in the solicitation should include the name of the marketer making the solicitation and an e-mail address, postal address, and telephone number at which it can be contacted.

For example, a marketer could say, "Here's how you can reach us ... (name, address, etc.)."

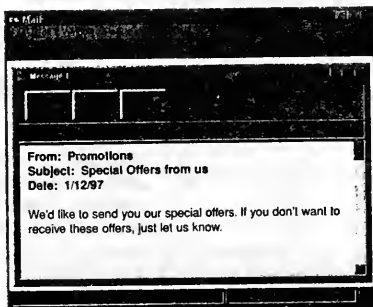
- Whenever possible, consumers should be provided with the opportunity to opt out via e-mail. Marketers should identify where consumers are invited to send such opt-out e-mail requests, particularly if the e-mail address is different than the one from which the marketing e-mail solicitation is sent.
- Because of the unique characteristics of automated mailing lists (e.g., listservs), subscribers to such lists cannot individually opt out if the list manager permits online solicitations to be directed to its subscribers. This prevents a marketer from suppressing online solicitations to some subscribers of a listserv but not to others. Consequently, a marketer directing online solicitations to subscribers of an automated mailing list should honor the list manager's stated policies regarding online solicitations. To facilitate adherence to this principle, managers of automated mailing lists should identify themselves and make their policies known to marketers and their agents prior to a solicitation. Marketers should also ask about policies that effect them.

**3. Any person who uses for online solicitation purposes e-mail addresses or screen names collected from the online activities of individuals in public or private spaces should see to it that those individuals have been offered an opportunity to have this information suppressed.**

- Ideally, marketers using e-mail addresses and related information they have harvested should provide consumers with an opportunity

to opt out prior to using the information for online solicitations.

For example, a marketer could say, "We see that you frequent the ( ) site — we'd like to send you offers of (computer equipment). If you don't want to receive these offers, just let us know."



- When using lists of e-mail addresses harvested by others, marketers should ensure that consumers have already been offered an opportunity to have their e-mail addresses and related information removed. Marketers should contractually require the sellers of harvested lists to contain the e-mail addresses of only persons who did not respond to a notice and opportunity to opt out.

**4. Marketers who operate chat areas, newsgroups, and other public forums should inform individuals using these spaces that information they voluntarily disclose in these areas may result in unsolicited messages to those individuals by others.**

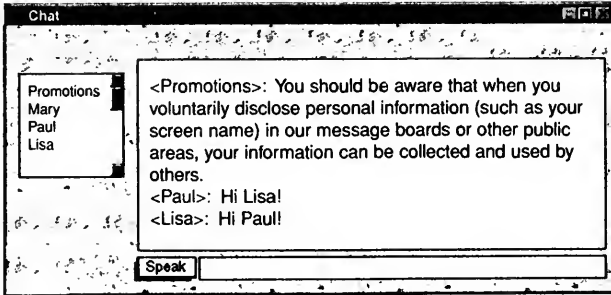
- For example, a marketer may inform visitors to a Web site with a message board that: "You should be aware that when you voluntarily disclose personal information (such as your screen name) in our message boards or other public areas, your information can be collected and used by others."

- Marketers should also support industry and other efforts to help educate consumers about ways to protect their privacy online.

**5. All persons involved in the use, rental, sale or exchange of lists and data for online solicitation purposes should take reasonable steps to ensure that such sharing of lists and data adheres**

**to these industry principles. Industry groups should take appropriate steps to encourage their members to follow these principles.**

- For example, marketers should incorporate these principles into their list rental contracts and should furnish these third parties with a copy of The DMA's Guidelines for Ethical Business Practice.



## Online Data Collection from or about Children

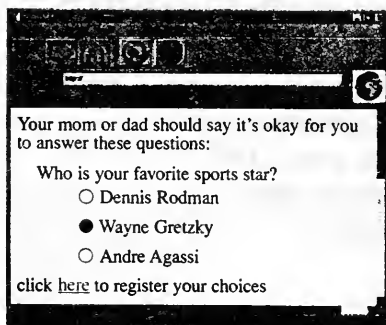
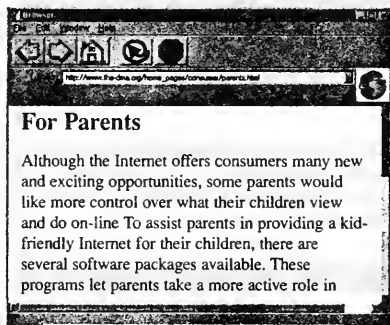
This section contains additional principles that apply to online activities that are directed primarily at children who, more so than adults, may not understand the nature of information elicited from them nor the uses to which the information may be put. Because of this difference in maturity, marketers operating online or Internet sites directed primarily at children should encourage parents to share in and monitor their children's online experiences.

1. In making decisions whether to collect data from or communicate with children online, marketers should take into account the age, knowledge, sophistication, and maturity of their intended audience.

For example, marketers should encourage young children to obtain their parents' permission, using language such as "Your mom or dad should say it's okay for you to answer these questions."

2. Marketers should be sensitive to parents' concerns about the collection of their children's names, addresses, or other similar information, and should support the ability of parents to limit the collection of such data for marketing purposes through notice and opt out.

- Marketers should encourage children to consult with their parents before furnishing data.

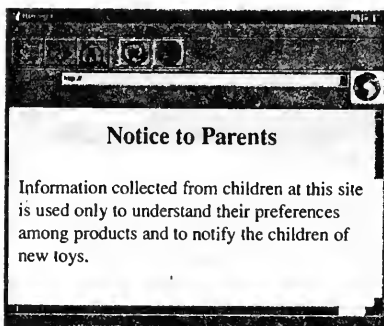


- Marketers should also support industry and other efforts to help educate parents about ways to protect their children's privacy online, including informing them about software tools and parental access controls that prevent their children from disclosing their name, address, or other personal information.

The DMA's Web site, for example, hosts a special "For Parents" section on its "Consumer Assistance" page, which informs parents of the various software packages available for helping parents provide a kid-friendly Internet for their children. Marketers could hyperlink to this page.

3. In conjunction with supporting the ability of parents to limit the collection of such data online, marketers should limit the use of data collected from children in the course of their online activities to the promotion, sale, and delivery of goods and services, the provision of all necessary customer services, the performance of market research, and other appropriate marketing activities.

4. Marketers should also effectively explain that the information is being requested for marketing purposes.



- For example, a toy manufacturer's disclosure to young children might state: "If you give us your e-mail address, we will tell you when new \_\_\_\_ arrive at the stores, but it's important that you ask your parents if that's okay."

- The same toy manufacturer's disclosure to parents might say: "Information collected from children at this site is used only to understand their preferences among products and to notify the children of new toys."

5. Marketers should implement strict security measures to ensure against unauthorized access, alteration, or dissemination of the data collected online from children. [Marketers should consult Articles 7, 8, and 9 of the The DMA's Guidelines for Personal Information Protection for suggested measures that should be taken to ensure security. These articles lay out the guidelines direct marketers should follow for the security of personal data; for authorization of visitors to areas where personal data are processed and stored; and for secure transfer of data.]

**For additional information contact:**  
**Ethics and Consumer Affairs Department**  
**The Direct Marketing Association, Inc.**  
**1111 19th Street, N.W., Suite 1100**  
**Washington, DC 20036-3603**  
**202 955-5030**

**Responses to Congressman Bruce F. Vento's Questions Relating to the Testimony of Richard Barton, of The DMA, at the Financial Institutions and Consumer Credit Hearings on Emerging Financial Privacy Issues.**

1. **“In your experience, are abstracts of files used for data mining for marketing limited to financial institutions? Are other sectors participating in this as well?”**

**ANSWER:** As mentioned in the testimony, direct marketing relies on a myriad of sources of information to target markets and prepare marketing messages. Financial institutions, nonprofits, and political campaigns are among the countless entities that legitimately use information about consumers to define their audiences and markets.

2. **“How does a customer know who is not a member of The DMA?”**

**ANSWER:** On July 1, 1999, The Direct Marketing Association launched its Privacy Promise Program in which all members are required to inform their customers of their privacy policies and give them the option to opt out of the use of their information for marketing purposes. Members for whom the program applies display a logo. Customers should look for that logo as an assurance that the association's privacy policies are being followed.

3. **“How do we protect consumers from bad actors with self regulation in marketing and on the Internet?”**

**ANSWER:** The Direct Marketing Association maintains an active ethics monitoring program, with a committee that hears complaints from customers on unethical practices and works to resolve those complaints and correct unethical practices. Several other business associations have similar programs. However, as outlined in the testimony, there are already a number of significant laws on the books regarding privacy. And we have strong anti-fraud laws and regulations enforced by organizations such as the Federal Trade Commission and the Postal Inspection Service. These laws and law enforcement activities apply to marketing on the Internet as well as the traditional marketing methods.

4. **“Are there financial institutions that are members of The DMA?”**

**ANSWER:** Yes, 145 financial institutions are currently members of The Direct Marketing Association.

5. **“Is e-mail marketing captured by The DMA policies for consumers to opt out of receiving solicitations?”**

**ANSWER:** Yes. E-mail is included in the “Privacy Promise” program described above and in our testimony. We also publish “Marketing Online: Privacy Principles and Practices.” These are guidelines on the ethical conduct of business online, which also apply to e-mail. A copy of this publication is attached.

STATEMENT OF D. BARRY CONNELLY  
PRESIDENT OF ASSOCIATED CREDIT BUREAUS, INC.  
WASHINGTON, D.C.

HEARING ON  
FINANCIAL PRIVACY

Before the Subcommittee on Financial Institutions  
and Consumer Credit of the  
Committee on Banking and Financial Services

of the  
United States House of Representatives

Washington, D.C.

Tuesday, July 20, 1999

Associated Credit Bureaus, Inc.  
1090 Vermont Avenue, NW  
Suite 200  
Washington, D.C. 20005  
202.371.0910 TEL.  
202.371.0134 FAX  
[www.acb-credit.com](http://www.acb-credit.com)

Madame Chair and members of the Subcommittee on Financial Institutions and Consumer Credit, my name is Barry Connelly and I am president of Associated Credit Bureaus, headquartered here in Washington, D.C. ACB, as we are commonly known, is the international trade association representing over 1000 consumer credit and mortgage reporting as well as employment and tenant screening agencies operating here in the United States and around the world. Over 400 of our members are also in the collection service business.

We want to commend you for choosing to hold this oversight hearing on financial privacy. Our country has a strategic global advantage resulting from the legitimate and balanced use of information. As an example, according to the Tower Group, a Boston-based consulting firm, the consumer reporting industry's information products are the infrastructure upon which our country has built a mortgage-backed securitization process that results in net savings of 2% off of the cost of a mortgage for the average consumer. Economic advantages, consumer benefits and consumer rights are all elements of a balanced equation. It is the art of maintaining this delicately balanced equation that remains crucial to your thinking as our nation's lawmakers.

I now turn to the general subject matter outlined in the Subcommittee's letter of invitation.

#### **CONSUMER REPORTING INDUSTRY OVERVIEW -**

The following thumbnail outline of our industry will answer some of your general questions about our members.

Consumer reporting agencies are essentially libraries of information on individual consumer payment patterns associated with various types of credit obligations. The data compiled by these agencies is used by creditors and others permitted under the strict prescription of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to review the consumer's file.

Consumer credit histories are derived from, among other sources, the voluntary provision of information about consumer payments on various types of credit accounts or other debts from thousands of data furnishers such as credit grantors, student loan guarantee and child support enforcement agencies as well as collection agencies.

A consumer's file may also include certain public record items such as a bankruptcy filing, judgment or lien. For purposes of data accuracy and proper identification, our members generally maintain information such as a consumer's full name, current and previous addresses, Social Security Number (when voluntarily provided by consumers) and place of employment.

This data is loaded into the system on a regular basis to ensure the completeness and accuracy of data on each consumer.

It is interesting to note that the vast majority of data in our members' systems simply confirms what most of you would expect; that consumers pay their bills on time and are responsible, good credit risks. This contrasts with the majority of systems maintained in other countries, such as Japan or Italy, which often store only negative data and do not give consumers recognition for the responsible management of their finances.

In discussions of consumer credit histories, I have found it helpful to also point out some facts about the types of information our members do not maintain in consumer credit reports. Our members do not know what consumers have purchased using credit cards (e.g., a refrigerator, clothing, etc.) or where they are using credit (e.g., which stores or restaurants a consumer frequents the most often). They also don't know when consumers have been declined for credit or another benefit based on the use of a credit history. Medical treatment data isn't a part of the databases, and no bank or brokerage account information is available in a consumer report.

In closing this section of my testimony let me reiterate that our members don't track data on what consumers purchase or where they shop. We compile data on how consumers pay their bills.

#### **PERMISSIBLE USES OF CONSUMER REPORTS & INFORMATION PRODUCTS -**

You also asked about how our members' information is used and what types of products they sell.



First, the FCRA is an effective privacy statute, which protects the consumer by narrowly limiting the appropriate uses of a consumer report (often we call this a credit report) under Section 604 (15 U.S.C. 1681b), entitled "Permissible Purposes of Reports."

Some of the more common uses of a consumer's file are in the issuance of credit, subsequent account review and collection processes. Reports are also, for example, permitted to be used by child support enforcement agencies when establishing levels of support. A complete list of permissible purposes can be found under Appendix A of this testimony.

A question that we hear with some frequency relates to how data found in a consumer's credit report may be used other than for credit reporting. Let me first point out that any data defined as a "consumer report" under the FCRA may not be used for any purpose other than for those outlined under Section 604.

However it is a fact that some of our members do use consumer identification information to develop high-value information-based products such as fraud prevention and authentication products; risk management systems; and locator services, just to name a few. Some of our members also develop direct marketing lists in order to stay competitive in the broader information marketplace. Note that the data used for direct marketing purposes is not the credit history information defined as a "consumer report" under the FCRA.

#### CONCLUSION -

In concluding my testimony, let me urge the committee to consider carefully the strategic importance of information in our country and how it benefits consumers. We have moved beyond an industrial economy, and information use is a critical catalyst for our new service economy's growth. Balanced laws such as the Fair Credit Reporting Act, which was significantly amended in the 104th Congress (Public Law 104-208, Subtitle D, Chapter 1), is an excellent example of the balance needed. We do believe there are times where innovative solutions can be found that don't require new laws. The creation of responsible self-regulatory regimes can create a flexible bridge between call for consumer protections and the unintended rigidity of new laws. Thank you for this opportunity to testify.

Appendix A

Submitted by Associated Credit Bureaus

July 20, 1999

**Section 604 (15 U.S.C. 1681b) - Permissible Purposes for Reports.**

1. In response to an order of a court or grand jury subpoena.
2. In accordance with the written instructions of the consumer.
3. For use in connection with credit transactions; employment purposes; underwriting of insurance; review for certain governmental licenses or benefits; portfolio analysis; or other legitimate business need associated with a transaction initiated by the consumer.
4. Review for establishing ability to pay child support.
5. Review by agencies administering a plan under Section 454 of the Social Security Act (42 U.S.C. 654) when setting child support awards.

**Section 625 (15 U.S.C. 1681u) - Disclosures to FBI for Counterintelligence Purposes.**

This section of the Act does allow limited access to consumer reports by the Federal Bureau of Investigations as indicated in the title.

**TESTIMONY OF**  
**Consumer Federation of America**  
**Consumers Union**  
**And the**  
**U.S. Public Interest Research Group**

**On Financial Privacy**  
**Before the Subcommittee on Financial Institutions and Consumer Credit**  
**Honorable Marge Roukema, Chair**  
**20 July 1999**

**by Edmund Mierzwinski**  
**Consumer Program Director, U.S. PIRG**

Madame Chair, Ranking Member Vento, members of the committee: Thank you for the opportunity to testify before you on the important topic of financial privacy. My testimony today is on behalf of three consumer organizations, Consumer Federation of America,<sup>1</sup> Consumers Union<sup>2</sup> and U.S. PIRG<sup>3</sup>.

We would like to make the following points today about financial privacy.

**(1) Congress needs to act now to address serious gaps in financial privacy protection.**

Numerous surveys, such as the recent AARP reports, have documented that consumers value their financial privacy. For example, AARP found that 81% of its members opposed the internal sharing of their personal and financial information with affiliates and 92% opposed companies selling their personal information.<sup>4</sup> Numerous news reports, lawsuit settlements and complaints have documented that the threat to financial privacy is real. Yet, under federal law, even our video rental records are protected better than the confidential "experience and transaction information" held by financial institutions. This financial privacy gap can easily be closed and financial modernization legislation is the right place to do it.

**Ideally, consumer groups believe that Congress should enact legislation that relies on Fair Information Practices<sup>5</sup> and does the following:**

- Gives consumers the right to opt-in for all information sharing for secondary purposes, whether to affiliates or to third parties.<sup>6</sup>
- Gives consumers clear notice and full disclosure of a bank's privacy policies for both affiliate and third party sharing and of the consumer's right to choose.
- Gives consumers full access to all of their records and a right to dispute and correct errors.
- Provides consumers with enforceable legal rights against violators.

**(2) The current version of HR 10 is inadequate to do the job.** It allows continued sharing, without even an opt-out, of both experience and transaction information among both affiliates and also with non-affiliated third parties. Further, the sweep of the exception allowing continued sharing with non-affiliated third parties is broad [See detailed attachment below]. Further, while the

provision includes a limited restriction on providing account numbers to non-affiliated third parties, that section is narrow and only restricts the sharing of these account numbers for marketing, but no other, purposes. In addition, the purported disclosure provision of the amendment (Section 503) is narrowly crafted and does not enhance consumer disclosures concerning the practices of affiliate sharing.

**Instead, at a minimum, the Congress should have enacted the compromise Markey-Barton bi-partisan privacy opt-out amendment** (similar to the amendment that passed the Commerce Committee by voice vote) which was unfortunately not made in order by the Rules Committee. That amendment would give consumers the protections they have demanded. The Markey-Barton amendment would give consumers the right to an opt-out that would have protected all their financial information from being used for secondary purposes by either an affiliate or any third party. As Representative Barton stated on the floor during consideration of HR 10:

The question I ask this body and this country is: If we are concerned about the selling and sharing of information to third parties, should we not be just as concerned about the selling, sharing, transmitting, or accessing that information inside of these affiliates if there are going to be dozens or hundreds of these affiliates? ... **Until we solve the riddle of handling information within the affiliate structure, we do not have privacy. We do not have privacy.**<sup>7</sup>

We note that while the Markey amendment passed the Commerce Committee by a bi-partisan voice vote, a similar Inslee amendment failed narrowly in the Banking Committee, during consideration of HR 10. We commend Rep. Inslee for offering that amendment and we also commend the committee members who supported it, including Madame Chair Roukema.

**(3) Privacy invasions are made by both affiliates and third parties.** Failing to give consumers control over their information when it is shared among affiliates is failing to solve the problem. In monetary terms, one of the worst information sharing violations documented so far-- the Nationsbank/NationsSecurities case, which resulted in a total of \$7 million in civil penalties--was an inside affiliate sharing arrangement, not a third party violation. Nationsbank shared detailed customer information about maturing CD holders with a securities affiliate, which then switched the conservative investors into risky derivative funds.<sup>8</sup> The merger of Citibank and Travelers Insurance provides the first example of the potential for the risky sharing of financial and medical information for marketing or underwriting purposes.<sup>9</sup>

Companies also share information with third parties. Most recently, a lawsuit brought in June by the Attorney General of Minnesota against US Bank has documented that the nation's largest banks have routinely shared confidential customer "experience and transaction" information with third-party firms for telemarketing and other purposes. The telemarketer doing business with US Bank, Memberworks,<sup>10</sup> had contracts with numerous other banks, as did at least one other competitor, BrandDirect,<sup>11</sup> which has also been the subject of consumer complaints. In the Minnesota settlement agreement with US Bank, the bank agreed to stronger privacy protections than those offered by HR 10. In particular, the bank agreed to "provide notice of customers' rights to "opt out" of the sharing of information with bank affiliates for purposes of marketing financial products and services.<sup>12"</sup> As noted in the fact sheet below, HR 10's minimal protections will still allow third party sharing for marketing, as well as other, purposes.

**(4) Title V needs a savings clause ensuring that stronger state privacy protection laws are not preempted.** In our previous testimony concerning HR 10, we have noted that its preemption provisions are severely flawed and may actually apply to all activities permitted under the act, not only to its insurance provisions. It is essential that states have the ability to enact and enforce laws that protect the privacy of their consumers, especially as the banking industry is further deregulated. Such a savings provision should encompass proposed, as well as existing laws, since numerous states are considering financial privacy laws. For example, in June, Governor Paul Celluci of Massachusetts introduced a package of legislation that includes opt-in provisions that would be stronger than HR 10.

**(5) Telling Consumers To Vote With Their Feet Is Not Acceptable.** We fundamentally disagree that merely requiring the disclosure of privacy policies and then letting consumers “vote with their feet” is good enough. First, in numerous other sectors of the economy, from cable television to telecommunications to video rental records, consumers have enforceable privacy rights. In nearly every country of the world, privacy is a basic human right, not a market condition. The notion offered by U.S. banks and direct marketers that voluntary self-regulation either works, or is sufficient to guarantee privacy, is not only unfounded but also “out of step with the rest of the world,” according to a recent international study of privacy laws.<sup>13</sup> Consumers should be given a level of privacy protection, based on Fair Information Practices, rather than being allowed to vote their Hobson’s choices.

Second, letting the market decide on the minimal level of privacy protection won’t work. In June, Consumers Union and U.S. PIRG tested the marketplace and found it does not work [See attached chart]. Our review of the disclosed Internet privacy policies of the nation’s ten largest banks found that none offered either adequate privacy protection or adequate disclosure.

- None of the firms offered greater privacy protection than the minimum required by law. None provided an opt-in or even an opt-out for the sharing of “experience and transaction” information either with affiliates or third parties.
- Only 4 out of 10 banks disclosed on their web sites that consumers had a right to opt-out of the sharing of “other” information, such as information the bank derived from either credit reports or account applications.<sup>14</sup>
- Only 4 out of 10 banks provided an opt-out for third party marketing lists.

Because many banks have grossly failed to comply with even the modest terms of existing law on disclosure and opt-out of “other” information, the nation’s chief bank regulator recently issued guidance describing how to comply with the law.<sup>15</sup>

**(6) The consumer group platform does not seek a ban on information sharing, nor would providing informed consumer consent defeat the purposes of financial modernization.**

As noted above, consumer groups seek only to give consumers control over the use of their confidential customer information for secondary purposes. Sharing of information for compliance with other laws, or for completing transactions associated with a consumer’s existing accounts, is acceptable and possible under both versions of the Markey amendment and also under the original Insee amendment offered in the House Banking Committee.

**(7) Sharing Leads To Sale of Over-Priced, Deceptively Marketed Products No One Wants Or Needs.** Information sharing with affiliates and third parties can lead to the sale of over-priced, unneeded, aggressively-pitched cross-marketed products. Among the most notorious of these products are credit insurance and credit card protection. As the ads say, “Who will pay your credit cards if you are disabled or laid off?” Your bank won’t, but it aggressively markets programs that claim it will. The small print discloses that the bank will **only** pay your minimum balance, for only a year, only if you qualify. A recent report by Consumers Union and the Center for Economic Justice found that credit insurance price gouging costs consumers over \$2 billion each year.<sup>16</sup> CU/CEJ found that consumers who should be receiving payouts of at least 75 cents per premium dollar were receiving only 38 cents.

So-called credit card protection merely duplicates coverage required by law—limiting your liability to only \$50 if your card is lost or stolen. Credit card protection is routinely sold by scam artists, as well as by banks.

Often, these credit card add-on or “cramming” practices target lower-income or even mentally disabled consumers. These consumers, both less sophisticated and less desirable (higher risk, higher interest rate) customers, find their credit card fee and interest payments soaring. Yet, they are often unable to pay down their principal balances, due to the expense of paying off crammed add-ons. One lawsuit recently filed against Provident Bank “cites examples of alleged offences, including one customer who was allegedly charged an \$89 processing fee, a \$59 annual fee, an APR of 23.99 percent, and a monthly fee of \$7.95 for credit protection for a credit card with a \$300 credit limit.”<sup>17</sup> According to a front page Wall Street Journal expose, credit firms are targeting the mentally disabled. One such consumer who purchased 8 separate credit card protection plans and various insurance plans ended up owing “\$1987 in charges for low-value telemarketed add-on services.”<sup>18</sup>

**(8) It is an industry myth that the U.S. has successfully relied on a voluntary self-regulatory approach to privacy on a sector-by-sector basis.** While it is true that the U.S. has relied on a sector-by-sector approach to privacy, rather than an over-arching privacy law, it is emphatically not true that voluntary self-regulation has worked. Although industry groups have succeeded in defeating numerous attempts to enact an overarching privacy law, stronger laws protect consumers in several other sectors, including telecommunications, video records, cable television and credit reports. For example, in June, the local telephone company, Bell Atlantic, sent the following “opt-in” notice to its customers:

“We understand that privacy is very important to all our customers. So unless we have your permission, Bell Atlantic does not share information about your account – not even with our affiliates – such as Bell Atlantic Mobile and Bell Atlantic Internet.”

Since consumers value their financial privacy highly, the financial sector should be subject to even stronger laws than those in these sectors. Further, changes in the marketplace are causing the convergence of sectors. As privacy expert Marc Rotenberg has noted, it is time to consider such an over-arching privacy law:

Those who argue that the United States has typically protected privacy by self-regulation and industry codes know very little about the long tradition of privacy legislation in this country. It is, however, correct to say that the United States, over the last twenty years, has taken a sectoral approach as opposed to an omnibus approach to privacy protection in the private sector. But it is also important to note that the sectoral approach has several

weaknesses. For example, we have federal privacy laws for video records but not for medical records. There are federal privacy laws for cable subscriber records but not for insurance records. I think the problems with the sectoral approach will become increasingly apparent as commerce on the Internet grows. The Internet offers the ideal environment to establish uniform standards to protect personal privacy. For the vast majority of transactions, simple, predictable uniform rules offer enormous benefits to consumers and businesses. It is also becoming increasingly clear that the large industry mergers in the telecommunications and financial services sectors have made the sectoral approach increasingly obsolete. Firms now obtain information about individuals from many different sources. There is a clear need to update and move beyond the sectoral approach<sup>19</sup>

**(9) As it applies to credit reporting agencies, the Fair Credit Reporting Act generally relies on Fair Information Practices-based rules. However, its exceptions are glaring, and have led to problems.**

Our organizations constantly seek to improve the Fair Credit Reporting Act. Nevertheless, as it applies to credit bureau records, the FCRA generally is based on Fair Information Practices. Its most glaring loophole, however, is the affiliate sharing exception that is the crux of the problems under review today. The FCRA does not regulate affiliate sharing under Fair Information Practices, but instead allows it by exception. During the seven years that our organizations worked to strengthen the FCRA prior to 1996, the proposed affiliate sharing exception was the most controversial issue before the Congress. The provision was strongly opposed by the Federal Trade Commission, as well as by consumer groups. The provision was not the subject of a detailed hearing record, but was in fact inserted as the price of industry support for the legislation.<sup>20</sup> Other flaws in the act, such as the so-called "credit header" loophole that allows social security numbers to be sold by information brokers and other firms, can also be closed by legislation such as HR 1450 (Kleckza).<sup>21</sup>

**(10) Emerging industry practices are reducing the coverage of the act and increasing the need for action.** The rise of affiliate sharing may signal the demise of the consumer protections offered by the Fair Credit Reporting Act. As the National Consumer Law Center has pointed out in its encyclopedic FCRA Legal Manual:

This exclusion from the definition of consumer reports is potentially so broad that many purposes of the FCRA may be undermined. As financial institutions expand merge, and nationwide conglomerates come to dominate credit and other markets, less and less information about consumers will be subject to the FCRA. Indeed a likelihood exists that many banking establishments will establish their own in-house credit bureaus free of the consumer and privacy protections and other strictures of the FCRA.<sup>22</sup>

At least one bank, Wells Fargo, for example, now has a type of credit bureau subsidiary. Its subsidiary, Norwest Mortgage, has a business called "Verification of Income and Employment." VIE seeks enactment of state laws that allow it to collect confidential wage information from state labor departments. Several states participate. However, in the last two months, at least two states, California and Pennsylvania, have cancelled pending contracts with the firm, due to concerns over potential privacy invasions.

Comptroller Hawke's recent tough speech<sup>23</sup> on practices such as those exposed at US Bank was actually on two topics. The other topic was the new practice of banks failing to share customer records with credit bureaus.<sup>24</sup> According to news accounts, the practice is growing and is done allegedly for competitive purposes—banks are supposedly protecting information about their best customers.

As financial firms get larger and contain more subsidiaries and affiliates, they may no longer need to contact credit bureaus for their own underwriting and marketing decisions. Consumers will not be able to shop around for credit (let alone for privacy policies).

HR 10 can only be expected to expand the capabilities of banks, especially bigger banks, to make credit decisions without using credit bureaus. Consumers will face denial without benefit of the full panoply of FCRA rights. In addition, consumers whose banks aren't reporting positive (or negative) information to the credit bureau will find that while their own bank's affiliates might make credit offers, that others will not, since their credit bureau report does not include their full positive credit history. If these practices grow, and if more banks begin to make decisions based on their own subsidiary credit bureaus, the effects not only on privacy, but also on competition and credit allocation, will be significant.

**(11) Other Issues:** The committee also posed questions concerning international issues and information brokers. While we commend the committee for its attempt to address the serious problem of pretext calling by information brokers, we believe the provision needs to be strengthened in several ways before it will be effective. Most importantly, consumers need a strong private right of action against both information brokers and financial institutions that break the law.

Our organizations are all members of the Trans Atlantic Consumer Dialogue (TACD), an international association of consumer groups concerned with trade policy. In April, the TACD issued a strong statement condemning the US-proposed privacy "safe harbor" for firms doing business under the European Data Directive. Here is the text of that statement:

The Safe Harbor proposal now under consideration by the United States and the European Union fails to provide adequate privacy protection for consumers in the United States and Europe. It lacks an effective means of enforcement and redress for privacy violations. It places unreasonable burdens on consumers and unfairly requires European citizens to sacrifice their legal right to pursue privacy complaints through their national authorities. The proposal also fails to ensure that individual consumers will be able to access personal information obtained by businesses.

Therefore,

1. The TACD urges the European Commission and the Ministers of the European Council to reject the Safe Harbor proposal. The proposal will undermine the purpose of the EU Data Directive and compromise the privacy interests of European citizens.
2. The TACD recommends the development and adoption of an International Convention on Privacy Protection that will help safeguard the privacy interests of consumers and citizens in the twenty-first century.
3. The TACD further urges national governments to ensure that consumer organizations are given a more central role in the future development of international privacy policies and practices that affect consumer interests.<sup>25</sup>



## ENDNOTES:

<sup>1</sup> CFA is a non-profit association of some 240 pro-consumer groups that was founded in 1968 to advance the consumer interest through advocacy and education.

<sup>2</sup> Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about good, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of Consumer Reports, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, Consumer Reports with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

<sup>3</sup> U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups. PIRGs are non-profit, non-partisan consumer and environmental advocacy groups active around the country.

<sup>4</sup> AARP Data Digest #39, Spring 1999, based on national telephone survey. AARP also commissioned a survey of all consumers, which found that only 14% of Americans "completely trust" their credit card companies to protect information about them. 17 Mar 99. AARP Poll: Nearly One In Five Americans Report They've Been Victimized By Fraud <<http://www.aarp.org/press/1999/nr031799a.html>>

<sup>5</sup> As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices. Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs. "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy," October 1997.

<<http://www.privacyrights.org/AR/fairinfo.html>> The document cites the version of FIPs in the original HEW guidelines, as well as other versions: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973 [From The Law of Privacy in a Nutshell by Robert Ellis Smith, Privacy Journal, 1993, pp. 50-51.]

1. Collection limitation. There must be no personal data record keeping systems whose very existence is secret.  
2. Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

<sup>6</sup> Thus opt-in right is provided in the original Markey bills, HR 1339 and HR 1340, introduced in the 106<sup>th</sup> Congress. The bills apply to financial institutions (H.R. 1339) under the jurisdiction of the Banking Committee and to broker-dealers and other firms (HR 1340) under the jurisdiction of the Commerce Committee. The opt-in is very clear: "upon the affirmative written request, or with the affirmative written consent, of the customer to whom the information pertains."

Floor debate on HR 10, Congressional Record, Page H5513, 1 July 1999.

<sup>8</sup> See SEC Release No. 7532 And Release No. 39947, May 4, 1998, ADMINISTRATIVE PROCEEDING AGAINST NATIONSBANK, NA AND NATIONSSECURITIES, File No. 3- 9596, In The Matter Of : ORDER INSTITUTING CEASE-AND- DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTIONS:15(B)(4) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934 AND FINDINGS AND ORDER OF THE COMMISSION. See < <http://www.sec.gov/enforce/adminact/337532.txt>> (Note, total civil penalties of nearly \$7 million includes fines paid to other state and federal agencies, as well as to the SEC.) From the order:

"NationsBank assisted registered representatives in the sale of the Term Trusts by giving the representatives maturing CD lists. This provided the registered representatives with lists of likely prospective clients. Registered representatives also received other NationsBank customer information, such as financial statements and account balances. These NationsBank customers, many of whom had never invested in anything other than CDs, were often not informed by their NationsSecurities registered representatives of the risks of the Term Trusts that were being recommended to them. Some of the investors were told that the Term Trusts were as safe as CDs but better because they paid more. Registered representatives also received incentives for their sale of the Term Trusts."

<sup>9</sup> We understand that the committee is hearing from other witnesses about medical privacy protections.

<sup>10</sup> On Friday, 16 July 1999, the Minnesota Attorney General filed suit against Memberworks. At least four other states (Florida, California, Washington and Illinois ) are investigating the firm. See The Washington Post, "Telemarketer

Deals Challenged in Suit, Sale of Consumer Financial Data Assailed," by Robert O'Harrow Jr, Saturday, July 17, 1999: Page E01.

<sup>11</sup> For articles on BrandDirect and Chase Manhattan, see for example, The Seattle Post-Intelligencer, "You may be a loser -- buying something you didn't want", by Jane Hadley, Thursday, April 8, 1999 or Newsday, "Company Had Her Number / Woman discovers to her surprise card issuer gave out account data" by Henry Gilgoff, 9 May 1999.

<sup>12</sup> Joint press release of Minnesota Attorney General and US Bank, 1 July 1999, <[http://www.ag.state.mn.us/home/files/news/pr\\_usbank\\_07011999.html](http://www.ag.state.mn.us/home/files/news/pr_usbank_07011999.html)>

<sup>13</sup> See Global Internet Liberty Campaign, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice," October 1998, <<http://www.gilc.org/privacy/survey/>>

<sup>14</sup> The firms may have provided these required disclosures in additional materials not available on the Internet site.

<sup>15</sup> See Office of Comptroller of Currency release AL 99-3, Subject: Fair Credit Reporting Act, March 29, 1999 <<http://www.occ.treas.gov/ftp/advisory/99-3.txt>> The guidance was a follow-up to several tough

speeches by former Acting Comptroller Julie Williams on the subject.  
 "But, unfortunately, it has been known to happen that the affiliate-sharing "opt out" disclosure is buried in the middle or near the end of a multi-page account agreement. For existing accounts, some institutions have gotten into the habit of reducing the required "opt out" disclosures to the fine print along with a long list of other required disclosures. Few consumers are likely to have the fortitude to wade through this mass of legal verbiage, and fewer still will take the time to write the required "opt out" letter. I have even heard of people getting two separate notifications covering different types of information, requiring two separate letters to opt out. Such techniques may fall within the letter of the law, but they certainly fall short of its spirit." Remarks by Julie L. Williams, Acting Comptroller of the Currency before the Banking Roundtable Lawyers Council, May 8, 1998, <<http://www.occ.treas.gov/ftp/release/98-50a.txt>>

<sup>16</sup> See "Credit Insurance: The \$ 2 Billion a Year Rip-off," by Consumers Union and the Center for Economic Justice, March 1999, < <http://www.consumersunion.org/finance/credredc499.htm>>.

<sup>17</sup> See Cards International, June 16, 1999, "Providian shares plummet"

<sup>18</sup> Wall Street Journal, "Credit Cards Invade A New Niche: The Mentally Disabled," by Joseph Cahill, 10 November 1998, page 1.

<sup>19</sup> Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives May 7, 1998

<<http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>>

<sup>20</sup> The Consumer Credit Reporting Act of 1996 (Pub. L. No 104-208, 30 Sept 1996) was finally enacted after 7 continuous years of contentious deliberations between consumer groups, credit bureaus, the financial services industry and Congress. In addition to the special interest affiliate sharing loophole, its other major flaw was its partial preemption of stronger state consumer laws. Its major omission was its failure to grant any consumer the right to review his or her credit report for free, on request.

<sup>21</sup> The credit header exception from the definition of credit report allows certain "header" information -- name, address, social security number -- to be sold without the protection of the FCRA. The exception is not allowed by statute, but by an FTC interpretation in a 1994 consent decree with TRW (now Experian). Sale of confidential consumer information leads to identity theft and other privacy invasions. Numerous firms that sell social security numbers and other confidential information to private detectives and information brokers have organized into an association known as the Individual References Services Group (IRSG). In 1997, against the views of privacy groups, the FTC agreed to allow this association to self-regulate its compliance with the law. To our knowledge, the IRSG has not made the results of its independent audits of compliance available to either the FTC, the public or to Congress.

<sup>22</sup> Ogburn and Faulkner, National Consumer Law Center, "Fair Credit Reporting Act: 1997 Cumulative Supplement," page 35. Boston, MA.

<sup>23</sup> Remarks by John D. Hawke, Jr. Comptroller of the Currency Before a Conference Sponsored by The Consumer Bankers Association Robert Morris Associates San Francisco, California June 7, 1999

<<http://www.occ.treas.gov/ftp/release/99%2D51a.txt>>

<sup>24</sup> See also the Washington Post, "Some Lenders Hold Back Good Reports From Credit Bureaus in Bid to Keep Top Customers," By Kenneth R. Harney, Saturday, May 22, 1999; Page G03

<sup>25</sup> See <http://www.tacd.org/meeting1/electronic.html>

---

**ATTACHMENT #1  
FACT SHEET**
**What's Wrong With The "Privacy" Provisions of HR 10?**

The House-passed privacy provisions in HR 10 fail to protect consumers' financial privacy. Consumers need the ability to control the sharing of their financial data – notice, access and at least the chance to say "no" to sharing financial information with *any* entity. While the House had the chance to provide real privacy protections by voting for the Markey compromise, it bowed to industry pressure and passed a weak financial privacy provision that is riddled with loopholes, sanctioning the rampant information sharing by financial firms.

**What's in HR 10?**

- **Limited Notice Provisions:** HR 10 requires only that an institution notify consumers about their policies and practices related to "protecting" the information or disclosing to nonaffiliated third parties. There is no requirement to tell consumers about the types of information collected or the information sharing practices related to affiliates and any other entity or person.
- **Opt-Out to "Nonaffiliated Third Parties" Only:** The provision's limited third party opt-out does not apply at all to internal affiliate sharing—affiliates can still share and sell information and consumers have no ability to stop them.
- **Marketing still Permitted with Nonaffiliated Third Parties:** Even if a consumer opts-out, information may still be shared with third parties *marketing* financial products on behalf the institution or pursuant to a "joint agreement" between two or more financial institutions to offer, endorse or sponsor a financial product. Therefore, with regard to *any* financial product, the consumer has no right to stop the disclosure of their information.
- **Loopholes Galore:** In addition to loopholes for sharing information among affiliates and third parties for financial products, the amendment restricts the sharing of extremely confidential account numbers with third parties for marketing purposes but the financial institution can provide these account numbers to affiliates and third parties for non-marketing purposes.

**How does the Markey Amendment that the House Voted Against Provide *Real* Privacy Protection?**

- **Notice about Information Sharing Practices with *All Entities*:** The Markey amendment would require institutions to provide full disclosure of their information sharing policies with all entities, including the categories of information collected and categories of persons/entities to whom the information may be shared.
- **Opt-Out of Information Sharing with *All Entities – Affiliates and All Third Parties – for All Purposes*:** The amendment that was defeated by the House would give consumers an across the board opt-out so they could say "no" to information sharing, for any purpose, with affiliates and third parties. This is the minimum protection consumers need – anything less is sanctioning widespread information sharing and violations of consumers' privacy.
- **Access to Information:** The amendment would give consumers access to and correction of information sold to third parties. The industry balked at even letting consumers have access to their own information so HR 10 does not provide any access to data for consumers.

---

### Why is it Important for Consumers to have the Choice to Stop information Sharing with Affiliates?

- **Harm to Consumers from Affiliate Sharing is Great:** Financial firms are interested in sharing information with and selling the products of their affiliates. Financial institutions can use affiliates to sell or market any of their products. Rather than use third parties, they will simply bring everything into the affiliate structure.

The most glaring example of the harm from unauthorized information sharing involves affiliate sharing -- the *NationsBank* case in which *NationsBank /Securities* settled securities laws violations by paying \$7 million to the SEC and other agencies. The allegations included the bank sharing lists of customers with expiring CDs with NationsSecurities. The securities affiliate allegedly sold uninsured, risky products in a misleading manner that were not suitable to unsuspecting CD holders. Thousands of consumers were affected, losing portions of their life savings. HR 10 as passed by the House does nothing to address this affiliate sharing problem but rather, gives its okay to widespread affiliate sharing without giving consumers any ability to stop such sharing.













































As Representative Barton (R-TX), who co-sponsored with Rep. Markey the stronger privacy amendment that was denied a vote by the Rules Committee, stated on the floor during the debate over HR 10 on July 1, 1999 --

*The question I ask this body and this country is: If we are concerned about the selling and sharing of information to third parties, should we not be just as concerned about the selling, sharing, transmitting, or accessing that information inside of these affiliates if there are going to be dozens or hundreds of these affiliates? ... Until we solve the riddle of handling information within the affiliate structure, we do not have privacy. We do not have privacy.*

### What do consumers need?

- **Notice and Control over their Financial Information:** Consumers need to be meaningfully and fully informed about the institution's information sharing and privacy practices. Consumers also need control over the sharing of their information. Financial firms should not be permitted to share or sell a consumer's financial information with any entity, affiliate or third party, without the consumer's prior consent -- an "opt-in." As a first step, consumers should be able to say "no" to disclosure of their information to any entity/person -- an across the board "opt-out."
- **Access and Accountability:** Consumers are entitled to know and determine what information the institutions hold on them and what their rights are. Consumers should also be able to hold institutions that violate their privacy accountable for the violations. Consumers should have access to the information institutions hold on them to ensure the information is accurate and relevant and the ability to correct erroneous information.
- **Security and Protection of Data:** The holders of data are in the best position to protect and secure the information on consumers. Banks and other financial firms should have a duty to protect the confidentiality of customers' financial and personal information and be held legally responsible when they violate the confidentiality standards.

The Markey privacy provisions that were defeated in the House by a vote of 232-198 represent a first step toward providing the type of protection consumers need. By voting against even this compromise measure, the House action paved the way for more sharing of consumers' personal financial information among financial firms against the clear demand and desire of the public. By choosing to support the greed of financial firms over the public they represent, the House gave its imprimatur to continuing violations of consumers' privacy.

Financial Institution	Privacy 		Piracy 		
	Opt-Out: Companies <i>can</i> disclose unless Consumers say No		Opt-In: Companies <i>cannot</i> Disclose unless Consumers say Yes		
	Affiliate Sharing		Third Party Sharing	Affiliate Sharing	Third party Sharing
	Only credit report Information (FCRA required)**	All Financial data			
NationsBank					
Citibank					
Chase Manhattan					
Bank of America					
First Union					
Morgan Guaranty Trust					
Bankers Trust					
Wells Fargo					
Fleet					
First Nat'l Bank of Chicago (BankOne)					

**epic.org**

**ELECTRONIC PRIVACY INFORMATION CENTER**

Testimony and Statement for the Record of

Marc Rotenberg, Director  
Electronic Privacy Information Center

Hearing on  
Financial Privacy and  
The Financial Services Act of 1999

Before the

Subcommittee on Financial Institutions and Consumer Credit  
Committee on Banking and Financial Services  
U.S. House of Representatives

July 20, 1999  
2218 Rayburn House Office Building

My name is Marc Rotenberg.<sup>1</sup> I am the Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, DC.<sup>2</sup> I appreciate the opportunity to testify today before the Subcommittee on Financial Institutions and Consumer Credit regarding financial privacy and H.R. 10, The Financial Services Act of 1999.

Financial privacy is a critical concern for American consumers. The rise of new financial institutions, new financial practices, and new banking regulations, has also caused growing public concern over the privacy of personal information and the risk of disclosure of private financial data. More than a quarter of a million Americans opposed a banking regulation that would have established extensive government reporting requirements on routine financial transactions. And polls routinely show that the lack of privacy protection is contributing to growing public unease about the use of the Internet for commercial transactions.

It is therefore important that the Subcommittee on Financial Institutions continues to look closely at issues concerning financial privacy. Consumer confidence is critical to the stability of the financial system and the development of new commercial services. Without real safeguards for private personal information, the consumer expectation of privacy in routine financial transactions will be severely undermined.

In the statement below, I have answered the various questions put forward by the Subcommittee. In some sections, I have described broadly some of the recent developments that may help the Members understand the problem of privacy protection in a larger context. These include the development of new marketing practices, the impact of the EU Data Directive, and the relationship between federal and state privacy laws.

In other sections, I have described in more detail specific problems with the privacy provisions in H.R. 10., including Title V and section 351 on medical record confidentiality. These sections contain specific recommendations for how the bill could be changed to better protect the private information of American consumers.

In summary, there will be significant benefits to consumers in the rise of new financial services and products. But until strong privacy safeguards are established, the process of financial modernization will remain unfinished.

---

<sup>1</sup> Executive director, Electronic Privacy Information Center; adjunct professor, Georgetown University Law Center; editor, *The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Development*; editor (with Philip Agre) *Technology and Privacy: The New Landscape* (MIT Press 1998).

<sup>2</sup> The Electronic Privacy Information Center is a project of the Fund for Constitutional Government, a non-profit charitable organization established in 1974 to protect civil liberties and constitutional rights. More information about EPIC is available at the EPIC web site <http://www.epic.org>.

## QUESTIONS POSED

*1. Significant debate is occurring over whether financial institutions should be allowed to share customer information with their affiliates and nonaffiliated parties. Please comment on the benefits of information sharing and whether you believe additional protections are needed under the Fair Credit Reporting Act or other laws.*

First, the concept of "affiliate sharing" is very much at odds with traditional privacy protection. Simply stated, privacy protection is the ability of individuals to limit the use of their personal information for a particular purpose. When, for example, a patient gives information to a doctor regarding a medical condition so that the doctor can provide a comprehensive diagnosis, there is a clear understanding that personal information will not be used for unrelated purposes, and if it is shared with a third party, it is only for purposes necessary to render the service provided.

Affiliate sharing transfers control over personal information from consumers to a corporate entity that may be engaged in a wide range of business practices unrelated to the specific purpose for which the information was provided. If a customer provides financial information to a bank for the purpose of getting a home loan and that information is subsequently used by an affiliated insurance company to provide information about insurance products, then it is clear that the customer's expectation of privacy when he or she provided that information to obtain a home loan was violated. As Justice Thurgood Marshall once wrote, "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."<sup>3</sup>

Second, the growth of the Internet and the rise of electronic commerce are leading many businesses to rethink their business models. I think it should also encourage more careful consideration of innovative privacy approaches and whether it is really necessary to collect so much personal information for a business to succeed in the age of the Internet. On the one hand, Internet-based businesses create new and unique privacy risks. It is much easier to track and profile customers on-line than it is in the physical world. If you grab a brochure in a bank for an IRA or clip out an ad in a newspaper for a home equity loan, those facts are still private information until you actually contact the bank or the lender. In the on-line world, if you download an ad for the same IRA or click on an ad for that same home equity loan, chances are good that some record will be created of your interest in these financial products.

---

<sup>3</sup> *Smith v. Maryland*, 442 U.S. 735, 749 (1979)(Marshall, J., dissenting).



At the same time, there are many ways to do business online that require the collection of less personal information and actually reduce privacy risks. It has become so easy to set up an electronic storefront on the World Wide Web that many of the costs associated with brick and mortar businesses have literally disappeared. Marketing is cheaper and more efficient. Information is much more widely available to consumers.

The bottom-line is that access to personal information held by affiliated parties is not needed for a company to be profitable or to provide services to customers. Individuals should retain the ability to decide for themselves how personal information is to be used. That is the basis of privacy protection.

*2. If you believe that additional financial privacy protections are necessary, please describe how new government mandates can be balanced with the information flow that is necessary to conduct daily business operations. In particular, discuss how the additional privacy protections you propose would affect credit availability and the ability of institutions to offer consumers lower cost products.*

While the relationship between privacy and the free flow of information is oftentimes described as a "balance" or a "trade-off," it is important to understand that there are many instances where privacy protection is necessary to ensure the free flow of information. Consider how valuable the telephone system or the mail service is for the daily exchange of information on everything from confidential business plans to medical record to private messages among friends and family. It is precisely because privacy is provided in these network environments that businesspeople are willing to place valuable commercial documents in a paper envelope or people feel free to tell their most intimate secrets into a device that connects millions of users across the country.

Similar issues arise with the disclosure of personal information to financial institutions. If customers cannot be assured that their personal information will not be improperly disclosed, then they may be less willing to provide information and to take advantage of new commercial services. Privacy protection is clearly an essential element of establishing trust and confidence in the online world.

I cannot specifically assess how new privacy rules would affect credit availability or the ability of institutions to offer consumer lower cost products, but I will make two observations. First, credit markets in the United States seem to operate fairly well even with government regulation and government oversight. Second, the price competition that is developing on the Internet today, which has enabled consumers to find many products at much lower costs than they could previously, seems to have very little to do with the sharing of personal information. Instead price competition has resulted from much better

access to price information that has made consumers more knowledgeable and markets more efficient. I think it would be a mistake to assume that lower prices for consumers requires extensive collection and use of personal information.

*3. Please provide comments specifically addressing the privacy provisions in H.R. 10 as passed by the House. In particular, please discuss the exceptions that are in the bill and whether they are sufficient to permit typical, everyday business transactions to continue.*

*Comments on TITLE V- PRIVACY; Subtitle A - Disclosure of Nonpublic Personal Information*

H.R. 10 fails to adequately protect consumer privacy in a variety of ways:

- There is no limitation on use of publicly available information.
- There is no control whatsoever over disclosure to institution affiliates
- There is no opt-out for disclosure to an institution's marketing partners
- There is no notice to consumers of particular uses of information, undermining the utility of opt-out measures
- There is no requirement of convenient opt-out procedures
- There is no consumer access and verification of institution-held information

Overall, H.R. 10 keeps consumers in the dark about the dissemination and use of even their most personal financial data. It allows unfair information practices on the part of financial institutions, including confusing privacy policies, burdensome opt-out procedures, and abuse of the Act's wide range of exceptions

For example, the Act regulates disclosure of "personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or the service performed for the consumer; or (iii) otherwise obtained by the financial institution."<sup>4</sup> Nonpublic personal information also includes "any list, description, or other grouping of consumers" assembled using private information held by the financial institution (e.g., a listing of the names and addresses of all account holders whose daily balance exceeds \$1M).<sup>5</sup>

Unfortunately, the Act leaves the definition of publicly available information, which is not covered, to individual administrative agencies. This makes it impossible to

---

<sup>4</sup> § 509(4)(A).

<sup>5</sup> § 509(4)(C).

determine which information categories fall under the Act's provisions. Nonetheless, one can reasonably expect names, addresses, and listed telephone numbers to be deemed publicly available. Instead of allowing financial institutions to continue providing the direct marketing industry with up-to-date mailing lists, the Act should limit disclosure of all personally identifying information. Currently, financial institutions may sell this information without customer notice or consent. At the very least, the Act should require adequate notice of all disclosures, even those involving publicly available information.

The Act also regulates disclosure of personal information only to nonaffiliates of the financial institution.<sup>6</sup> Thus, "any company that controls, is controlled by, or is under common control with another company" may freely receive account numbers, spending habits, and other sensitive information.<sup>7</sup> Consumers must have the opportunity to opt-out of disclosures to all third parties, excepting those who perform specific servicing or processing functions related to a consumer's account (e.g., printing checks). While section 502(e)(1) attempts to implement an exception of this type, the definition of necessary services, section 509(7), is overly broad. In particular, section 509(7)(C) allows insurance companies to obtain private information for such nebulous purposes as "account administration." This language should be tightened to allow free access to consumer personal information only by third parties directly involved in the maintenance of the consumer's account.

The Act's most salient feature is its litany of exceptions to the notice and opt-out provisions. First, even unaffiliated third parties may obtain sensitive information "to perform services or functions on behalf of the financial institution, including marketing of the financial institution's own products or services or financial products or services offered pursuant to joint agreements between two or more financial institutions."<sup>8</sup> This clause allows marketing companies to continue compiling highly specific consumer profiles without the consumer's consent. The compilation of such profiles would likely qualify as a "service or function" under this section. Other exceptions are equally troubling. § 502(e)(3) authorizes unrestricted disclosure of personal information "to protect the confidentiality or security of [a financial institution's] records pertaining to the consumer." It is unclear how a consumer's privacy interests are protected by free disclosure of spending habits and other personal information. Finally, the purposes served by § 502(e)(4)—access to financial record information for the purposes of rating and regulating the institution—do not require disclosure of personally identifiable information. A guarantor can do her job with account numbers and balances that are not tied to particular individuals.

---

<sup>6</sup> § 502(a).

<sup>7</sup> § 509(6).

<sup>8</sup> § 502(b)(2).

Disclosure to third parties that do not fall into one of the Act's many exceptions need only be preceded by notice and an opportunity for consumers to block disclosure.<sup>9</sup> The Act requires a statement of an institution's privacy policies and practices "at the time of establishing the customer relationship with the consumer and not less than annually."<sup>10</sup> The policy must include the "categories of persons to whom the information is or may be disclosed." § 503(b)(1)(A). However, since this category is limited to nonaffiliated third parties (even those that perform marketing services for the institution), institutions are likely to include this uninformative phrase in their privacy statements. A consumer will not know what to make of a phrase like "nonaffiliated third party," yet such a disclosure, without more, would appear to satisfy an institution's duties under the Act. Furthermore, there is no provision for disclosure of particular uses of a consumer's personal information. Language requiring a clear explanation of who will receive personal information, and what will be done with it, should be added.

Finally, as noted above, consumers should be informed of an institution's disclosure policies regarding publicly available information as well nonpublic data categories. The opt-out requirement applies only to unaffiliated third parties who are not included in the marketing exception described above.<sup>11</sup> Thus, consumers are powerless to prevent widespread dissemination of their personal information to marketing firms as well as any institutions that have entered joint agreements with a consumer's institution. This result is inconsistent with the fundamental privacy principle of individual control over dissemination and use of personal information. Consequently, the Act should at least allow consumers to opt-out of any disclosure of personally identifiable data. Enacting an "opt-in" procedure would further the goals of information privacy even more. By making non-disclosure the default, an opt-in system gives individuals true control over their personal information. Because the data in question is so personal—purchase information, account numbers, and so on—an opt-in procedure should be implemented. In the alternative, the Act should at least specify that nondisclosure options be reasonably convenient for the consumer to exercise. As written, the Act requires only "an explanation of how the consumer can exercise" an opportunity "to direct that such information not be disclosed."<sup>12</sup> Thus financial institutions can create burdensome opt-out conditions in hopes of reducing the number of customers exercising the option. This is clearly incompatible with the Act's privacy protection objective. Consequently, the Act should require convenient opt-out procedures.

---

<sup>9</sup> § 502(a)-(b).

<sup>10</sup> § 503(a).

<sup>11</sup> § 502(b)(2).

<sup>12</sup> § 502(b)(1)(B)-(C).

Finally, the Act includes no language ensuring consumers an opportunity to access and verify personal information after collection. A robust access and update system benefits both consumers and institutions. Allowing individuals to check the relevance of personal data held by financial institutions will foster a sense of empowerment among consumers, who will disclose information more readily knowing that they can verify it later. Along with the benefits of increased consumer trust, institutions stand to gain up-to-date personal information provided by the consumers themselves. Access and verification rights shift some of an institution's updating costs to the consumer. For these reasons, the Act should require access and correction procedures.

*Comments on TITLE III; Subtitle E - Confidentiality; Sec. 351, Confidentiality of Health and Medical Information*

One of the biggest privacy issues that the country faces today is the protection of medical record information, and both the Senate and the House are actively working to adopt legislation to protect the medical records of Americans. Section 351 of the Financial Services Act of 1999 attempts to address the medical privacy issue by limiting the disclosure of certain medical information. However well intended the privacy provision may be, it is likely to cause more problems than it solves.<sup>13</sup> It will almost certainly reduce the level of privacy protection for medical records that most Americans currently enjoy under state law or are likely to receive under either guidelines developed by the Secretary of HHS or medical privacy legislation passed by Congress.

Section 351 is a privacy provision only to the extent that it attempts to limit the disclosure of certain personal information. It does not contain the other elements of Fair Information Practices, including most significantly the right to obtain access to one's own medical record. This right is currently recognized in at least 34 states. Second, the exceptions in Section 351 are extremely broad. Law enforcement agencies could gain access to sensitive medical records upon a showing of far less information than is required to obtain a warrant.<sup>14</sup> Third, section 351 could effectively preempt state medical privacy provisions that are stronger than the language in the Financial Services Act.

The National Coalition for Patients' Rights has produced a useful paper "Protecting the Privacy of Medical Records: An Ethical Analysis" that provides an excellent basis for developing medical privacy legislation.<sup>15</sup> The recommendations

<sup>13</sup> "Still Not Private Enough," *The Washington Post*, July 8, 1999 at A24.

<sup>14</sup> In "compliance with a . . . investigation . . ." Sec. 351(a)(3)(E).

<sup>15</sup> <http://www.nationalcpr.org/WP-request.html>

outline the need to address such issues as record confidentiality, patient access, disclosure limitations, third party payers, psychotherapy, biomedical research, health services research, clinical research, law enforcement access and other topics.<sup>16</sup> The Model State Public Health Privacy Project, an effort currently underway at Georgetown University, has also developed a very good model statute for privacy protection.<sup>17</sup> Finally, there are the recent recommendations of the Health Privacy Working Group that are also worth close attention.<sup>18</sup>

I strongly urge you to either drop section 351 in the meeting of the conference committee or to adopt much stronger language in line with the National CPR proposal, the MSPHPP undertaking, and the PHPP Best Principles approach. There is clearly widespread support for strong medial privacy protection. I am sure that Americans do not want sensitive medical records to be freely shared between banks, insurers, and securities dealers

*4. Currently consumers are afforded privacy protection under a combination of Federal and State laws. With respect to financial privacy, how do federal and state laws complement, reinforce, or overlap one another?*

Currently financial privacy laws provided an incomplete framework for protection. For example, there is no comprehensive protection for insurance records, while there is better protection for credit reports.

Some states have moved quickly to address public concerns about financial privacy, while others have moved more slowly. Enforcement of current law is oftentimes uneven, though a prosecution can have a significant impact across an entire industry

In general the best approach to privacy protection is for the Congress to establish minimum standards for state regulatory schemes. For example, the Video Privacy protection Act of 1988 states simply "The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section."<sup>19</sup> In this manner, the exercise of federal authority to protect privacy still allows that states to function as "laboratories of democracy."<sup>20</sup>

The Financial Services Act should be make similar allowances for state regulatory authorities to develop new safeguards and new privacy protection as circumstances require.

---

<sup>17</sup> <http://www.critpath.org/msphpa/privacy.htm>. cited in *Privacy Law Sourcebook* 542.

<sup>18</sup> "Best Principles for Health Privacy," [[http://www.healthprivacy.org/latest/Best\\_Principles\\_Report.pdf](http://www.healthprivacy.org/latest/Best_Principles_Report.pdf)].

<sup>19</sup> 18 U.S.C. § 2710(f) cited in *Privacy Law Sourcebook* 139.

<sup>20</sup> *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

5. Please discuss any concerns you may have about the Federal and State governments collecting and disseminating consumer information. For instance, it appears that State divisions of motor vehicles routinely provides vehicle registration information to commercial entities. In addition, last year IRS employees were found to have been "snooping" into neighbor and other people's files. Should consumers have the right to "opt out" of the government sharing information? Please discuss what changes, if any, you would recommend with respect to Federal and State government privacy policies and practices.

Consumers who provide information to a federal or state agency to obtain a service, receive a benefit, or comply with a legal obligation, have little choice when asked to provide personal information.

In the past week my organization filed a brief in the Supreme Court in the case concerning the Drivers Privacy Protection Act of 1994 because we believe that there are significant privacy interests in the collection and use of personal data maintained by state agencies.<sup>21</sup> Under the DPPA states are regulated only to the extent that they choose to take personal information provided to a state agency for the purpose of a obtaining a license to operate a motor vehicle on a public roadway and then subsequently sell or disclose that information to purposes unrelated to the operation of the Department of Motor Vehicle or the protection of public safety. We recommended to the Court that the DPPA be upheld over the objection that some of the states have made on federalism grounds.

More generally we support the establishment of rights based on the Privacy Act of 1974 that give individuals greater control over their information that is collected and used by federal and state agencies.

6. The government agencies all have websites. These websites contain privacy policies. Are the policies "clearly and conspicuously disclosed" to consumers? Some of the agencies collect information, while others do not. Some use "cookies," while others do not. Should the privacy policies, collection of information and use of cookies by the government be consistent?

I have no specific information about whether the privacy policies at government websites are "clearly and conspicuously disclosed" to consumers. However, EPIC did conduct the first comprehensive survey of web site privacy policies back in 1997. We

---

<sup>21</sup> Brief Amicus Curiae of the Electronic Privacy Information Center in Support of Petitioners, *Reno v. Condon*, U.S. Supreme Court, No. 98-1464 (filed July 15, 1999).  
[[http://www.epic.org/privacy/drivers/epic\\_dppa\\_brief.pdf](http://www.epic.org/privacy/drivers/epic_dppa_brief.pdf)]

reviewed 100 of the most frequently visited web sites on the Internet.<sup>22</sup> We checked whether sites collected personal information, had established privacy policies, made use of cookies, and allowed people to visit without disclosing their actual identity.

We found that about half of the sites that we surveyed in 1997 collected personal information. This was typically done for on-line registrations, surveys, user profiles, and order fulfillment. We also found that few web sites had explicit privacy policies (only 17 of our sample) and none of the top 100 web sites met basic standards for privacy protection. We also noted that users were unable to exercise any meaningful control over the use of cookies. However, we noted that anonymity played an important role in online privacy, with many sites allowing users to access web services without disclosing personal data. We said that:

Users of web-based services and operators of web-based services have a common interest in promoting good privacy practices. Strong privacy standards provide assurance that personal information will not be misused, and should encourage the development of on-line commerce. We also believe it is matter of basic fairness to inform web users when personal information is being collected and how it will be used.

We recommended that:

- Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the home page by looking for the word "privacy."
- Privacy policies should state clearly how and when personal information is collected.
- Web sites should make it possible for individuals to get access to their own data
- Cookies transactions should be more transparent
- Web sites should continue to support anonymous access for Internet users.

In 1998 the FTC conducted its own survey of privacy policies. Although the survey looked at more web sites, the FTC survey was in some critical respects narrower than the original EPIC survey.<sup>23</sup> The FTC focused on the number of web sites that collect personal information and also on the number of web sites that had a privacy policy. But

---

<sup>22</sup> EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [<http://www.epic.org/reports/surfer-beware.html>]

<sup>23</sup> FTC, "Online Privacy: A Report to Congress" (1998) [<http://www.ftc.gov/reports/privacy3/index.htm>].



the FTC largely ignored the crucial role of anonymity in privacy protection. The FTC also lowered the bar by defining Fair Information Practices to be simply "notice," "choice," "access" and "security."<sup>24</sup> Although we did not look at the full range of Fair Information Practices in 1997, we followed the OECD practice in inquiring whether there were "use limitations" or "secondary use restrictions" in the privacy policies we found. This point is important because much of privacy law turns on the principle of finality – the principle that information is collected for a particular purpose and that information should be used only for that purpose unless meaningful consent is obtained from the data subject.

In 1998 we undertook a second survey to determine whether industry was doing a good job encouraging its own members to adopt privacy policies. "Surfer Beware II: Notice is Not Enough" surveyed the privacy policies of 76 new members of the Direct Marketing Association (DMA).<sup>25</sup> We chose the DMA because it has been a leading proponent of self-regulation and because it has undertaken a number of efforts to encourage privacy protection through self-regulation. These included a policy announced in October 1997 that the DMA would require future members to post a privacy policy and provide an opt-out capability. Of the 76 new members we examined, only 40 had Web sites and of these, only eight sites had any form of privacy policy. We examined these policies and found that only three of the new members have privacy policies that satisfied the DMA's requirements set out in October 1997. None of the sites examined allowed individuals to gain access to their own information. We concluded that the DMA's efforts to promote privacy practices is having little impact on its new members, even after repeated assurances from the DMA that this approach is effective.

There should be comprehensive federal guidelines for government web sites and these guidelines should reflect the principles of the Privacy Act of 1974. Individuals should be able to determine whether there are records held in an agency that contain information concerning that individual. And people should have the ability to gain access to personal information about them held by federal agencies. Simply posting a notice is not enough to ensure that the principles of the Privacy Act are upheld.

On the topic of cookies, it is important to distinguish between cookies that collect personal identifiable information and those that do not. A cookie that is tied to a known user raises significant privacy issues. Although any collection of personal information presents a privacy risk, the risk is more serious with cookies because the collection of the identifying data is often surreptitious, and lacking any reasonable means for individuals

<sup>24</sup> Prepared statement of the Federal Trade Commission on "Internet Privacy" before the Subcommittee on Courts and Intellectual Property of the House Judiciary Committee. March 26, 1998 [<http://www.ftc.gov/os/1998/9803/privacy.htm>]

<sup>25</sup> [<http://www.epic.org/reports/surfer-beware2.html>]

to exercise control over the collection and use of data. Thus a cookie policy for the federal government should begin by noting whether personal identifiable information is collected from the person visiting the web site.

Finally, in this discussion of website policies for Federal and State governments, I would add that everything should be done to ensure that individuals are able to access information from government agencies anonymously, i.e. without being required to disclose one's identity. A person who goes to the IRS web site, for example, to download a form or publication should be able to do so without any concern that a record will be created of that inquiry. Of course consumers should remain free to disclose personal information when it may be beneficial to receive some additional service or information. But federal and state governments would stay on the right track if they kept in mind the value of providing information to consumers without requiring the collection of personally identifiable information. This is far more important than whether a privacy policy is clear and conspicuous.

*7. Please identify and discuss your group's privacy policy. Is your privacy policy clearly and conspicuously disclosed to members and supporters of your group? Does your group rent, sell or lease its membership list to third parties? Are your members and supporters given the opportunity to "opt out" of information sharing with third parties?*

The EPIC Privacy Policy is displayed on our homepage.<sup>26</sup> It states simply:

#### **EPIC Mailing List**

If you are interested in receiving the EPIC Alert, we ask for your email address so that we can send it to you. You can also receive the EPIC Alert by visiting the EPIC Alert archive at our web site. The EPIC Alert mailing list is used only to mail the EPIC Alert and to send notices about EPIC activities. We do not sell, rent or share our mailing list. We also intend to challenge any subpoena or other legal process seeking access to our mailing list. We do not enhance (link to other databases) our mailing list or require your actual name.

#### **EPIC Web Site**

We do not enable cookies and we do not collect personally identifiable information at our web site. We periodically delete usage logs.

---

<sup>26</sup> "EPIC Privacy Policy," [http://www.epic.org/epic/privacy\\_policy.html](http://www.epic.org/epic/privacy_policy.html).

## EPIC and Amazon

We are an Amazon Associate and sell books at the EPIC Bookstore on topics that we think will interest our users. Amazon will ask you for certain personal information, such as mailing address and credit card number, to fulfill your order. Amazon also has a privacy policy and does not sell or rent information about its customers. EPIC does not receive any personally identifiable information about EPIC Bookstore customers from Amazon.

Another web site that we manage – [privacy.org](http://www.privacy.org) – has a simple but direct privacy policy:<sup>27</sup>

The Privacy Page collects no personally identifiable information, maintains no mailing list, and does not put cookies (or anything else) on your hard disk. We are an information resource, not an information sponge.

Have a nice day.

As I indicated, privacy protection is more about practices than policies. A very large notice that says "We collect your personal information and toss it in the street" provides much less protection than an actual set of procedures that reflects a substantive commitment to privacy protection.

For example, we believe that mailing lists should be operated on an opt-in basis and that it should be as easy to get off a list as it is to get on a list. It is as easy to unsubscribe to the EPIC Alert as it is to subscribe to it.<sup>28</sup> Every EPIC Alert that we send out includes instructions at the end for unsubscribing. And we have built a mailing of over 10,000 subscribers to the EPIC Alert who have opted-in. We have always avoided the practice of merging lists or adding people to our list without their actual consent.

We recognize also that there are some people who may like to get information without subscribing to a mailing list. So all the information that is sent out in the EPIC Alert is also available at our web site and it can be viewed anonymously, without any requirements that personal information be disclosed.

Now some may say that as a privacy organization we have to be particularly sensitive to privacy concerns and so it is understandable that we would have a very good privacy policy, and I think that is true. But it is also true that we understand that privacy

<sup>27</sup> "The Privacy Policy of Privacy.org," [http://www.privacy.org/privacy\\_policy.html](http://www.privacy.org/privacy_policy.html).

<sup>28</sup> "Subscribing to the EPIC Alert," <http://www.epic.org/alert/subsription.html>.

protection is not just about what you'll do with personal information; it's about what you actually do. It's about procedures and practices, and not just the words on a web site.

It's also important to note that for many years, a very high level of privacy protection characterized the Internet, at least in terms of data collection practices. There were few incentives to collect and use personal information. People could routinely access web sites without disclosing their actual identity and mailing lists all observed the convention of opt-in. It is only recently that we are beginning to see the rapid increase in the collection of personal information. Privacy policies are doing little to slow that process.

*8. In the United States, privacy laws are designed largely on an industry basis while many other countries have one comprehensive privacy statute. Given the fundamental difference between U.S. privacy laws and other countries, what effect will compliance with the EU Directive have on U.S. commerce abroad?*

I believe the E.U. Directive has already had several very positive effects on U.S. commerce abroad. First, it has simplified the process of doing business in Europe. Prior to adoption of the E.U. Data Directive, European countries operated with many different privacy laws that made it difficult not only to conduct trade within Europe but also for U.S. firms operating in Europe to comply with the laws of the various countries. Large, established firms such as Citibank and American Express had the resources and the incentives to develop close ties to privacy agencies and to develop practices that complied with national law. But for most small and medium sized firms the obstacles were great.

With the adoption of the E.U. Data Directive, European countries sought to promote trade within Europe and to remove the barriers to the free flow of good and services, labor and capital. The Directive has helped firms outside of Europe develop policies and practices that will now be acceptable across the European Union. There is now a single reference document that covers virtually all of the privacy obligations for financial firms operating in Europe. I suspect this is a simpler regulatory approach than the one faced by foreign firms operating in the United States.

Second, the EU Data Directive also led to the creation of institutions that have focused on the problem of how to protect privacy in the years. The Working Group, established by Article 29 of the Directive, has been the source of some of the most significant proposals and policy recommendation of any government entity in the world. The Article 29 working group has tackled such issues as anonymity, cookies, and self-regulation in an even-handed manner

The United States would have benefited greatly over the last several years if there were a similar agency with the expertise and authority to provide guidance and recommendation in this critical area of public policy.

The third significant advantage of compliance with the EU Data Directive is that it has forced a raising of privacy protection in the United States by focusing on the central question of whether we really have adequate privacy protection in this country. The EU Data Directive is not so much a problem as it is a reminder that our privacy laws are out of date and that there is much work to be done in this country to ensure the protection of this essential freedom. Further action against the EU Data Directive will not make the privacy concerns in the United States go away. In the end, we need stronger privacy safeguards not to satisfy European government, but to assure the protection of our own citizens.<sup>29</sup>

*9. Commerce taking place over the Internet is largely subject to a variety of industry self-regulatory efforts. Do you believe that self-regulation is sufficient at the present time, or are new government mandates warranted?*

I believe that the current efforts to promote industry self-regulation will not adequately address the public concerns about privacy and the Internet. Industry policies are typically incomplete, incoherent, and unenforceable. They are having little impact on actual data collection practices. Instead of reducing the demand for personal information or encouraging the development of privacy enhancing techniques, industry privacy policies are literally papering over the growing problem of privacy protection online.

A better approach would be to establish a legal framework that provides simple, predictable, uniform rules to regulate the collection and use of personal information. Not only is this approach consistent with US privacy legislation, it would also provide clarity and promote trust for consumers and businesses in the new online environment. I also believe that protecting privacy rights in law would encourage the development of better techniques to protect privacy and, in the long term, reduce the need for government intervention. The key to effective privacy legislation is to pursue the enforcement of Fair Information Practices and the development of methods that reduce the need for personally identifiable information.

---

<sup>29</sup> Testimony and Statement for the Record of Marc Rotenberg Director, Electronic Privacy Information Center Adjunct Professor, Georgetown University Law Center on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives May 7, 1998 [<http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>]. See also Rotenberg, *The Privacy Law Sourcebook* 505-29 ("Materials on 'Safe Harbor' Proposal").

Up until a few years ago, legislating privacy protection was a straightforward problem. The basic goal was to outline the responsibilities of organizations that collect personal information and the rights of individuals that give up personal information. These rights and responsibilities are called "Fair Information Practices" and they help ensure that personal information is not used in ways that are inconsistent with the purpose for which it was collected. Fair Information Practices typically include the right to limit the collection and use of personal data, the right to inspect and correct information, a means of enforcement, and some redress for individuals whose information is subject to misuse.<sup>30</sup>

Fair Information Practices are in operation in laws that regulate many sectors of the US economy, from companies that grant credit to those that provide cable television services.<sup>31</sup> Your video rental store is subject to Fair Information Practices as are public libraries in most states in the country. The federal government is subject to the most sweeping set of Fair Information Practices. The Privacy Act of 1974 gives citizens basic rights in the collection and use of information held by federal agencies. It also imposes on these same agencies certain obligations not to misuse or improperly disclose personal data.<sup>32</sup>

Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection. The most well known of these international guidelines are the OECD Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.<sup>33</sup> The OECD Privacy Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation.<sup>34</sup> These are:

---

<sup>30</sup> See generally, Robert Gellman, "Does Privacy Law Work?" in P. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press 1998)

<sup>31</sup> *Privacy Law Sourcebook* 1-37, 100-02 (Fair Credit Reporting Act of 1970, Cable Communications Policy Act of 1984).]

<sup>32</sup> *Privacy Law Sourcebook* 38-56.

<sup>33</sup> *Privacy Law Sourcebook* 179-205.

<sup>34</sup> BASIC PRINCIPLES OF NATIONAL APPLICATION

**Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

**Data Quality Principle.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

**Purpose Specification Principle** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

The United States and more than a hundred US companies pledged to support the OECD Guidelines almost twenty years ago. It is worth noting also that the United States has a particularly strong tradition of extending privacy rights to new forms of technology. For example, subscriber privacy provisions were included in the Cable Act of 1984. New protections for electronic mail were adopted in the Electronic Communications Privacy Act of 1986.<sup>35</sup> Video rental records were safeguarded as a result of the Video Privacy Protection Act of 1988.<sup>36</sup> And auto-dialers and junk faxes were regulated by the

purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

**Use Limitation Principle.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

**Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

**Openness Principle** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

**Individual Participation Principle.** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

**Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

*Privacy Law Sourcebook* 181-82.

<sup>35</sup> *Privacy Law Sourcebook* 103-36.

<sup>36</sup> *Privacy Law Sourcebook* 137-39.

Telephone Consumer Protection Act of 1991.<sup>37</sup> Even the original Privacy Act of 1974 came about in response to growing public concern about the automation of personal records held by federal agencies.

Viewed against this background, the problem of privacy protection in the United States in the early 1990s was fairly well understood. The coverage of US law was uneven: Fair Information Practices were in force in some sectors and not others. There was inadequate enforcement and oversight. Technology continued to outpace the law. And the Europeans were moving forward with a comprehensive legal framework to safeguard privacy rights of their citizens.

Unfortunately, just at the point in time when there was need for leadership in government to promote a privacy policy based on extending Fair Information Practices, the Administration and Congress turned away from well established legal standards and traditions and proposed instead a search for solutions based on industry self-regulation.

Some said that the interactive nature of the Internet made possible a new approach to privacy protection, one that focused on individuals exercising privacy "choice" or "preferences." But providing a range of choices for privacy policies turns out to be a very complicated process, and there is no guarantee that a person's privacy preferences on one day will be the same the next. In the rush to avoid a "one size fits all approach," those who focused on privacy choices may have discovered, paradoxically, that "many sizes fits none." In other words simple, predictable, uniform rules make it easier for individuals to exercise control over their personal information than an endless selection of choices that turn out to be meaningless.

Other industry approaches emphasized the easy online availability of privacy policies. But in practice, making use of a web site privacy policy turns out to be cumbersome and impractical, and almost the antithesis of the Internet's architecture. The very networked nature of the Internet that enables users to move freely from one site to the next discourages standards that vary from one site to the next. If a user will click past a site because a graphic takes too long to load, can we reasonably expect that same person to read through the fine print of a privacy policy? Both of these approaches, which are the outcome of pursuing the industry policy of self-regulation, have made it more difficult -- not easier -- for individuals to protect their privacy online.

An additional problem was created by the somewhat awkward role of the Federal Trade Commission. Because the United States lacks an agency with the expertise and competence to develop privacy policies, the FTC was cast in the role of *de facto* privacy agency. But the FTC did not itself have the authority to enforce Fair Information Practices or to promote the development of the various privacy enhancing techniques that

---

<sup>37</sup> *Privacy Law Sourcebook* 149-57.



were being pursued by other privacy agencies around the world.<sup>38</sup> The FTC relied instead on its Section 5 authority to investigate and prosecute fraudulent or deceptive trade practices.

The better approach would have been to look at the Internet and ask how could it make it easier to apply and enforce Fair Information Practices. For example, one of the hard problems in privacy protection is ensuring that individuals are able to access and correct information about themselves. In the paper world, the right of access is an elaborate and costly process for both businesses and consumers. Records must be copied and sent by mail. In the online world it is much easier to provide ready access to profile information. In fact many web sites today, from airline reservations to online banking, are making information that they have about their customers more readily available to their customers over the Internet. It is not "choice" that customers are exercising but rather "control" over their personal information held by others.

The Internet is also offering interesting developments in the use of techniques for anonymity and pseudo-anonymity to protect online privacy. These techniques enable commercial transactions while minimizing or eliminating the collection of personal information. Such techniques avoid the need for privacy rules simply by avoiding the rights and responsibilities that result from the collection and use of personal data.

*10. Please feel free to provide any additional comments you may have on these issues.*

The key to privacy protection is to give the give consumers the ability to control personal information held by third parties, and where possible to limit or eliminate the collection of personally identifiable information. I believe the Internet offers enormous opportunities to develop innovative, effective means to protect online privacy, but these efforts will only succeed if the goal is well understood. Simply posting a privacy policy will not protect privacy. It may in fact have the exact opposite effect if the policy serves the purpose of disclaiming any reasonable privacy claim that the consumer might have otherwise pursued. Thus the adequacy of these policies becomes crucial and the need to make very clear in statute the essential elements of Fair Information Practices is critical. It is not enough to simply state that a financial institution has an "affirmative and continuing obligation to respect the privacy of its customers," – the nature of these obligations should be spelled out and made clear to both customer and financial institutions.<sup>39</sup> This was the approach taken in the Privacy Act of 1974, and that Act has

<sup>38</sup> See, e.g., EC Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, "Anonymity on the Internet" (1997) reprinted in *Privacy Law Sourcebook* 404-15.

<sup>39</sup> § 501(a) ("Protection of Nonpublic Personal Information").

done well over the years. Where problems arise, it is from absence of enforcement or an overly broad reading of certain exceptions. But the key to effective privacy legislation is the articulation of specific Fair Information practices that make clear the rights of individuals who give up personal information and the responsibilities of those organizations that collect personal information

It is also very important to pursue innovative solutions to privacy issues. There, are so many ways today to market, advertise and sell products without collecting personal information. Just to give one example, as an Amazon Associates, EPIC receives some its revenue from the sale of books related to privacy, and civil liberties on the Internet. The EPIC Online Bookstore has done very well and we recently became an Amazon Affiliate so that we could also sell our publications through Amazon. But what is most extraordinary about all of this is that we are able to sell books to customers at our web site without collecting any personal information. All of the data is collected by Amazon.

The study proposed in section 508 is a good idea, but a more extensive and far-reaching project would look at the many emerging opportunities to conduct online commerce by means of transactions that do not require the collection and use of personal information. This may be a good project for the National Research Council. And if a good solution is found – if robust techniques for enabling online commerce while protecting the collection and use of personal information are discovered – it will greatly benefit consumers and financial institutions in the years ahead.

Finally, I hope you will reconsider limitations on the reporting requirements contained in the Bank Secrecy Act and the proposed rollback of the entire regulatory requirement. Many privacy problems can be avoided simply by reducing the collection and use of personal information. The Bank Secrecy Act is simply too broad, too burdensome, and too intrusive. Efforts to repeal the Act are certainly worth pursuing.



TESTIMONY BEFORE THE  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE  
OF THE HOUSING AND FINANCIAL SERVICES COMMITTEE  
ON

EMERGING FINANCIAL PRIVACY ISSUES

JULY 20, 1999

2128 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, D.C.

WITNESS: JACK BRICE

For further information, contact:  
Roy Green  
Federal Affairs Department  
(202)434-3800

601 E Street, NW Washington, DC 20049 (202) 434-2277 [www.aarp.org](http://www.aarp.org)  
Joseph S. Perkins *President* Horace B. Deets *Executive Director*



Good morning, Chairwoman Roukema and members of the Subcommittee on Financial Institutions and Consumer Credit. My name is Jack Brice. I live in Decatur, Georgia, and I serve as a member of AARP's Board of Directors.

The Association appreciates this opportunity to present our views regarding the important issue of protecting the personal financial information and medical records of individual Americans. AARP recognizes the potential that a modernized financial services industry may offer in the way of new and useful products and services, as well as the potential for cost savings to the consumer. However, the Association is concerned about the risks involved in allowing the integration of the financial services industry without also updating consumer information privacy protections.

In December of 1998, AARP sponsored an independently conducted national telephone sample survey of its membership regarding their awareness of privacy issues. Results from this widely reported survey include the following findings:

- 78 % of respondents disagreed, 56 % disagreeing strongly, with the statement: "Current Federal and state laws are strong enough to protect your personal privacy from businesses that collect information about customers."
- At least 87 % of respondents reported that it would bother them if personal information were sold by businesses, government agencies or Web sites to other businesses.

- 81 % of respondents opposed newly affiliated companies being allowed to internally share personal and financial information about customers.
- Over two-fifths (42 %) of respondents indicated that they “didn’t know” who they would turn to for assistance if a company were inappropriately sharing or selling their personal information.
- Nearly one-fifth (19 %) indicated that they had been approached by a company offering to protect their information privacy for a fee.

An analysis of the full survey is provided as an appendix to our written testimony.

The issue of financial privacy has emerged from a recognition that our nation lacks a consistent, binding process for protecting the privacy rights of consumers with regard to personal financial information collected and disseminated by private financial enterprises. It is clear from AARP’s survey that mid-life and older Americans feel vulnerable to the complex and fundamental changes that have already occurred in this period of financial transformation. Survey respondents were concerned that they would be put at further risk by the financial mergers that are yet to occur -- if adequate personal privacy safeguards are not put into place.

Extensive personal information is already routinely gathered and distributed by a wide range of financial institutions. As banks merge with securities and insurance firms, financial privacy protection for confidential information grows increasingly important. It is clear that financial privacy of consumers should not be considered as incidental to the modernization of the financial services industry – but rather as an inherent part of it.

In fact, there is good reason for consumers and financial service providers to agree on the need for improved security and confidentiality measures that protect personal financial information. Both consumers and service providers can appreciate that this type of information has great value and is worth protection – if for different reasons. For example, AARP concluded, along with a wide cross-section of interests representing the financial industry, and many other consumer advocacy groups, that the proposed “Know Your Customer” program proposed by the four major federal financial regulatory agencies represented a significant breach by the federal government of the firewall protecting the individual’s right to privacy. This program would have gone well beyond clarifying suspicious transactions for which financial institutions are already authorized to be on the lookout, to a requirement that financial institutions construct customer data warehouses that would be exploitable by the most sophisticated data mining technologies. This program also could have led to increased use by financial institutions of customer data segmentation, and more highly targeted marketing campaigns. This widely opposed governmental intervention into personal financial affairs was withdrawn.

Financial services industry and consumer interests have another opportunity to work together to protect the security and confidentiality of personal financial information on the issue of “pretext calling”. While the House and Senate have passed different versions of financial modernization legislation, both include provisions that would make it a federal crime to use false pretenses (so-called pretext calling) to gather private information about an individual from a bank.

However, the essential question raised by your letter of invitation to testify before this Subcommittee is: Can the actual or perceived costs in the loss of privacy to the individual through the largely unfettered use of personal information collected by private sector financial institutions, ever outweigh the benefits of new and useful services and products—and potential savings – to the consumer it may offer? How can we balance and manage those risks?

Federal and state financial privacy protections available to consumers today are limited, and in some aspects dated by the development of new information technology that has led to new forms of business and business practices. For example, the concept of the “virtual company”, where business information and personnel are distributed across computer-linked networks that require a minimum physical presence in any one site or nation, is predicated on the use of technology in this manner. The Fair Credit Reporting Act (FCRA) plays a marginalized role in this context, as it only regulates the collection and use of personal data by credit-reporting agencies to unaffiliated third parties. The Equal Credit Opportunity Act (ECOA) prohibits creditors from gathering certain types of personal and demographic information from credit applicants. The Right to Financial Privacy Act (RFPA) of 1978 limits the ability of financial institutions to disclose customer information to agencies of the federal government.

More specifically with regard to the FCRA, while the Act restricts the sale of consumer credit information, such as credit card accounts, there is generally no restriction on credit

bureau sales of personal background information such as date of birth and Social Security number. Two of the three largest credit-reporting agencies in the United States have voluntarily stopped selling such information. However, the U.S. Federal Trade Commission (FTC) recently took action against the third agency to stop such sales.

Efforts were made to address these gaps in protection during committee deliberations regarding H.R. 10, the Financial Services Act of 1999. AARP was disappointed, however, that many of the personal information privacy protections included in the version of the bill reported out of the House Commerce Committee were dropped from the version finally passed by the full House. AARP was encouraged by Commerce Committee bill provisions requiring that:

- Financial firms have and disclose a privacy policy.
- Consumers be given the opportunity to say no to, or “opt out” of, personal information being transferred among financial firms’ business affiliates as well as unrelated third-parties, such as telemarketers.
- Consumers have access to their information held by third-party companies, as well as the ability to correct the information.

AARP believes that financial services modernization legislation should go even further to protect consumers. Specifically, AARP believes that:

- Consumers should not be compelled to pay to block such information dissemination.
- Nor should they be forced to comply with cumbersome procedures to ensure that protection.
- Consumers’ explicit and recorded consent should be obtained before any sale or sharing of their non-publicly available financial records to third parties or to business affiliates.



- In addition, businesses that maintain customer databases should be required to mark the data files of customers who do not want information about themselves disseminated and to notify consumers of the opportunity to prevent distribution of information.
- At a minimum, this notification and opportunity to prevent distribution of their information should be renewed when new data is being collected or added, as well as in instances of business mergers or acquisitions.
- Consumers should be provided avenues for redress if they are harmed by an inappropriate disclosure or use of their personal information.

The version of HR 10 that passed the House allows a financial service provider to continue the practice of sharing individual financial information with its affiliates, as well as unrelated third-parties that market products in alliance or partnership with the data-collecting institution, without the customer's consent. The House-passed HR 10 only requires the customer's consent before allowing the financial services provider to share private account information with telemarketers and other unrelated third-parties.

Many in the financial services industry have raised concerns that updating financial privacy requirements in this fashion would reduce the benefits of HR10. There has been a great deal of discussion with regard to the benefits of the "synergism" that will be created through modernization and cross-marketing of financial services by individual financial institutions.

Often cited as an important source of those benefits is information management along with associated technologies. One of the most rapidly expanding sectors within information technology is adaptable records management and retention software. AARP

believes that the synergism of information being used by the financial services sector to develop and market new and useful products and services can effectively be adapted or adopted to manage the personal information privacy choices of those same customers. The efficient and effective sharing of individual-linked data bases within or across organizations ultimately depends on the information technologies used to manipulate it.

AARP believes that individuals should participate in the decisions regarding the sale, use and dissemination of any personal financial information collected on them. Such a relationship would not prohibit the mutually beneficial collection, retention or distribution of personal data, but rather enhance its value to business and customer alike. *A performance-binding information disclosure policy would, at the points of information collection, help to educate individuals regarding its intended uses – not inhibit its efficient use.* Performance standards need to be put into place that take advantage of the efficiencies and conveniences that information technology can provide, while providing security, confidentiality and privacy for the customer's personal data.

The medical records provisions of HR 10 are also of concern to AARP. A medical history contains some of the most private information collected about any individual. It is critical that individuals be able to participate actively in decisions about how these data will be used, *and to consent to whom will have access to their personally identifiable medical information.* AARP believes that minimum federal standards for maintenance of the privacy and confidentiality of personal health information would best be established

through comprehensive federal legislation applying to all health information, no matter where, or why collected.

In particular, AARP believes Section 351 of HR 10, the Confidentiality of Health and Medical Information provision, is deficient on at least two points. First, it permits far too much “sharing” of personally identifiable health information within the financial services industry – that will extend beyond the knowledge or consent of the affected individuals. Section 351 would legislate to financial institutions much more authority to share confidential health care information than currently exists within the health care business. Second, consideration of comprehensive health information privacy and confidentiality legislation is already being debated in the Senate. After passage of a comprehensive medical privacy act, Section 351 would be unnecessary. AARP believes that the Congress should continue the extensive legislative work that has already been accomplished in this area, and enact comprehensive federal legislation applicable to the management of all personal health information.

### **Conclusions**

The bottom line is that AARP believes that consumers have a right to be involved participants in financial service provider decisions regarding the dissemination of their financial information and medical records. The Association believes that consumers have the right to reject unauthorized use of personal financial information and medical records outside the original business context in which and for which the data were

collected. We will look closely at the conference report on HR 10, if it develops, to determine whether individual, including medical, privacy is being compromised.

AARP looks forward to working with you, Chairwoman Roukema, the other members of this Subcommittee, and members of the House and Senate, as the work of the conference committee approaches. Again, the Association appreciates this opportunity to offer its views on an issue of fundamental importance to older and younger Americans alike. I would be happy to respond to any questions you may have.

In compliance with House Rule XI, clause 2(g) regarding information of public witnesses, attached is AARP's statement disclosing federal grants and contracts by source and amount received in the current and preceding years.

# PUBLIC POLICY INSTITUTE

## AARP MEMBERS' CONCERNS ABOUT INFORMATION PRIVACY

### Introduction

Consumers today face an increasing array of challenges to their personal privacy, particularly the privacy of their personal information. Advances in computer technology and in data collection techniques have allowed public and private organizations to collect vast quantities of information on consumers, including who they are, where they live, how much they earn, and how they spend their money.

Currently there are few legal constraints on the collection, use, and dissemination of information about individuals.<sup>1</sup> Many of the legal privacy protections that do exist were, by and large, crafted to specify how the federal government could use information it gathered about citizens. As a consequence, there are only limited restrictions on information collected by private companies or by state and local governments.

### Study Purpose

An increasing number of Americans are concerned about threats to their personal privacy. In a 1978 study sponsored by the Center for Social and Legal Research, 64 percent of Americans reported that they were "very concerned" or "somewhat concerned" about such threats. By 1998, this percentage had risen to 88 percent, more than a one-third increase in 20 years.<sup>2</sup>

<sup>1</sup> Board of Governors of the Federal Reserve System. *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud*. March 1997, pages 20-21.

<sup>2</sup> Center for Social and Legal Research. *The Privacy Concerns & Consumer Choice Survey*. November 18, 1998, p. 9.

Each year thousands of new privacy measures are considered in state legislatures around the country and in Congress.<sup>3</sup> This trend is expected to continue in 1999.

In light of this trend, AARP conducted a national survey to measure its members' awareness of privacy issues and to ascertain their attitudes toward current practices of selling and sharing customer information.

### Methodology

International Communications Research of Media, Pennsylvania conducted 501 interviews with a sample of randomly selected AARP members. The survey's margin of error is plus or minus 4 percent. All respondents were aged 50 and older and were asked a series of questions regarding privacy of personal and financial information.

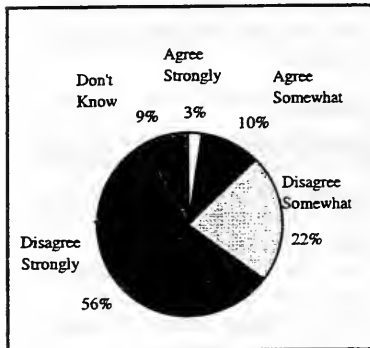
### Findings

The survey results indicate that AARP members are very concerned about threats to their personal privacy. A majority of respondents believed that businesses can gather personal information about consumers without their permission, including whether they pay their bills on time (82%), the long distance carrier they use (76%), their Social Security number (68%), their medical histories (60%), and the amount of money in their bank accounts (55%).

<sup>3</sup> Center for Social and Legal Research. *Privacy and American Business*. November/December 1998, p. 1.

AARP members think that current laws are inadequate to protect consumers. Respondents were asked to agree or disagree with the following statement: "Current federal and state laws are strong enough to protect your personal privacy from businesses that collect information about consumers." Seventy-eight percent of respondents disagreed with that statement, with 56% disagreeing strongly (Figure 1).

**Figure 1. Percent of Respondents Who Agree or Disagree that Current Laws are Strong Enough to Protect the Privacy of Consumers**

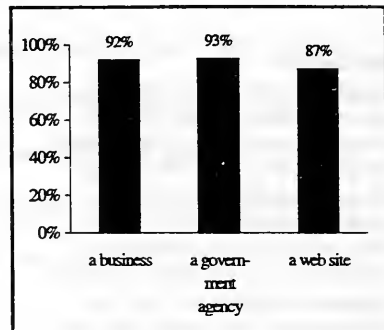


Source: 1998 AARP Survey on Information Privacy

The survey revealed a high level of aversion to businesses, government agencies, or Web sites selling information about customers to other businesses. In each case, at least 87% of respondents reported that it would bother them if their personal information was sold in this manner (Figure 2).<sup>4</sup>

<sup>4</sup> Respondents were asked, "Would you mind if a company you did business with sold information about you to another company?" They then received follow-up questions regarding sales of

**Figure 2. Percent of Respondents Who Would Mind if Personal Information About Them Was Sold By:**



Source: 1998 AARP Survey on Information Privacy

The results of this survey were further analyzed to see whether the findings were consistent when respondents were grouped by age, education, income, marital status, and political party affiliation. These tests revealed a high degree of consistency, with only minor differences between groups. These modest variations<sup>5</sup> included:

- Women (95%) were slightly more likely than men (89%) to feel that companies should not sell personal information about customers.
- Men (16%) were more likely than women (9%) to agree (strongly or somewhat) that existing consumer protection laws are strong enough.
- Younger members ages 50 to 69 (91%) were more likely than those members 70 and older (81%) to

information by government agencies and Web sites.

<sup>5</sup> These differences were statistically significant at the .05 level, providing a 95 percent probability of accuracy.

oppose Web sites selling their personal information.

During 1998, Congress considered a measure that would allow banks, insurance companies, and securities firms to be owned by a single corporation. One issue in the congressional debates was whether the newly affiliated companies would be allowed to share information about customers and customer accounts.

The AARP survey gathered data on this issue. Eighty-one percent of respondents opposed the internal sharing of customer personal and financial information by corporate affiliates. Only 10% supported it, and the majority of these said that affiliated companies should be required to notify and obtain written permission from customers before sharing their personal information.<sup>6</sup>

Relatively few respondents (18%) reported knowing of an instance where a company had inappropriately shared or sold their personal information. More than two-fifths (42%) of survey respondents indicated that they "didn't know" whom they would turn to for assistance if a company was inappropriately sharing or selling their personal information. This compares to 16% who said they would contact a lawyer, 15% who would contact their state attorney general's office, and 8%

who would call the Better Business Bureau.<sup>7</sup>

Almost one-fifth (19%) of respondents reported that they had received solicitations from companies offering to protect their information privacy for a fee.

### Summary

AARP members are concerned about the privacy of their personal information. In this sense they are like all U.S. consumers, according to recent survey research. Irrespective of age, gender, education, income, or political views, a high proportion of AARP members believe that existing consumer protections are not strong enough to protect information privacy, and they strongly believe that companies, government agencies, and Web sites should not sell information about them to other companies.

*See page four for a complete list of the survey questions.*

Written by Kristin Moag, Public Policy  
Institute, Consumer Team, Research Group  
February 1999

© 1999 AARP. Reprinting with permission only.  
AARP, 601 E Street, N.W., Washington, DC 20049  
www.aarp.org

<sup>6</sup> The remaining 10% of respondents either did not have an opinion or said they "did not know" whether information sharing should be allowed. Older persons with a college education were somewhat less likely than those with a high school education to oppose information sharing.

<sup>7</sup> This was an open-ended question, and respondents could report more than one answer. As a result, the percentages reported here should not be totaled, and there were additional response categories that are not listed here.

SURVEY QUESTIONS <sup>8</sup>

1. Computers have made it easier to collect, share, and sell information, including personal information about individuals. As far as you know, which of the following pieces of information can businesses gather about you without first getting your permission?

	% Yes
a. the amount of money in your bank account	55
b. your medical history	60
c. the types of products or services you buy, such as at the grocery store or drug store	56
d. the long distance telephone carrier you use	76
e. whether you pay your bills on time	82
f. your Social Security number	68
g. your annual income	65
h. financial assets you own, such as mutual fund shares	56

2. Please tell me if you agree or disagree with the following statement: "Current federal and state laws are strong enough to protect your personal privacy from businesses that collect information about consumers."

	%
Agree strongly	3
Agree somewhat	10
Disagree somewhat	22
Disagree strongly	56
D. Don't Know	9

3. Have you ever been in a situation where a company had information about you or your accounts that was wrong?

	%
1. Yes - CONTINUE	27
2. No - SKIP TO Q.5	69
D. Don't Know - SKIP TO Q.5	4

4. Were you able to correct that information?

	%
1. Yes	75
2. No	21
D. Don't Know	4

5. Would you mind if a company you did business with sold information about you to another company?

	%
1. Yes	92
2. No	7
D. Don't Know	1

<sup>8</sup> Due to rounding, response totals for some questions may not equal 100%.



6. Would you mind if a government agency, such as the state department of motor vehicles, sold information about you to businesses?
- |               | %  |
|---------------|----|
| 1. Yes        | 93 |
| 2. No         | 6  |
| D. Don't Know | 1  |
7. Would you mind if a Web site you visited sold information about you to other businesses?
- |               | %  |
|---------------|----|
| 1. Yes        | 87 |
| 2. No         | 4  |
| D. Don't Know | 8  |
8. In the future, banks, insurance companies, and investment firms may be able to merge into a single company. If they do, would you support or oppose these newly merged companies from internally sharing information about your accounts or your insurance policies?
- |   | %  |
|---|----|
| 1. Support - SKIP to Q.9                | 10 |
| 2. Oppose - SKIP to Q.11                | 81 |
| 3. Don't Care/No Opinion - SKIP to Q.11 | 6  |
| D. Don't Know - SKIP to Q.11            | 4  |
9. Should companies be required to notify you before sharing your personal financial information with newly affiliated companies?
- |               | %  |
|---------------|----|
| 1. Yes        | 79 |
| 2. No         | 15 |
| D. Don't Know | 6  |
10. Should newly merged companies be required to obtain your written permission before sharing information about you with another?
- |               | %  |
|---------------|----|
| 1. Yes        | 71 |
| 2. No         | 27 |
| D. Don't Know | 2  |
11. If you thought that a company was inappropriately sharing or selling your personal information, who would you turn to for assistance? (Open-ended question)
- |                                  | %  |
|----------------------------------|----|
| Don't know                       | 42 |
| A lawyer                         | 16 |
| State Attorney General's Office  | 15 |
| Government                       | 8  |
| Better Business Bureau           | 8  |
| The company itself/in question   | 5  |
| Congressman                      | 4  |
| Local consumer protection agency | 4  |
| Senator                          | 2  |
| State Representative             | 2  |

(The total of response percentages for this question exceeds 100 percent since respondents could indicate more than one source of assistance; responses offered by fewer than 2% are not listed.)

12. Have you ever experienced a case where a company was inappropriately sharing or selling your personal information?

	%
1. Yes	18
2. No	76
D. Don't Know	6

13. Have you been approached by any companies offering to protect your information privacy for a fee?

	%
1. Yes	19
2. No	79
D. Don't Know	2

© AARP, 1999



**CUNA & Affiliates**

**Credit Union National Association, Inc.**

805 15th Street, NW Suite 300  
Washington, D.C. 20005  
(202) 682-4200

TESTIMONY OF  
CREDIT UNION NATIONAL ASSOCIATION  
BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS  
AND CONSUMER CREDIT  
OF THE  
COMMITTEE ON BANKING AND FINANCIAL SERVICES  
U.S. HOUSE OF REPRESENTATIVES

JULY 20, 1999

The Credit Union National Association, on behalf of 9,961 federal and state chartered credit unions and 74 million Americans who are credit union members, is pleased to provide testimony today on the credit union perspective regarding financial privacy. From a legislative standpoint, this issue has developed with extraordinary speed, given the complexity of the technological and operational aspects of information-sharing practices.

As member-owned financial cooperatives, credit unions value the unique relationship they have with their members and respect their members' right to financial privacy. This relationship stems from a long held credit union core belief that credit unions are "not-for-profit, not-for-charity, but for service." Member service drives everything a credit union does, including all decisions made regarding a member's financial information.

But member service also involves providing the widest range of financial options at the best possible price, something that cannot be effected unless the member is apprised of choices in the marketplace. In fact, financial products that would be right for members may not even be offered by their credit union, often because their credit union is small and has limited in-house resources necessary to support a full-range of products.

Given that 61 percent of all credit unions have assets less than \$10 million, the practice of information sharing in order to provide a wider range of member services is not surprising. By necessity, credit unions work with outside companies to promote their financial products and services. Of course, credit unions also share information with third-party entities to perform services such as check printing, credit reporting, credit card processing and other essential data processing functions. [Question #1]

Historically, credit unions have refrained from involvement in the debate on how banks, securities firms and insurance companies might form into financial conglomerates. In the last six weeks, however, privacy has become a pivotal issue in the H.R. 10 debate. Since credit unions will likely be subject to privacy requirements incorporated into any legislation enacted, CUNA has a basic question about how the new requirements will affect credit union operations:

*Will credit unions and other smaller financial institutions that do not operate within affiliate structures be subject to a heavier disclosure burden than those financial institutions with affiliates?* [Question #3]

CUNA commends Chairwoman Marge Roukema, Ranking member Bruce Vento, Chairman Jim Leach and several other House negotiators for responding to CUNA's concerns about the problems presented for credit unions by the onerous "opt out" provision in H.R. 10. Their work to improve the privacy section by creating reasonable exceptions for third-party information sharing improved the legislation significantly before it reached the House floor. [Question #2]

Additionally, CUNA believes the House-enacted exceptions from disclosure and opt-out requirements are comprehensive enough to allow the efficient completion of operations and other processing services that credit unions typically obtain through third-party providers. [Question #2]

We supported the inclusion by the House Banking Committee of criminal penalties for fraudulent access of financial information by "pretext callers," originally part of H.R. 30 and subsequently included in H.R. 10. CUNA believes that the pretext calling language will result in credit unions formalizing training programs of their employees in handling member information requests. This will be a positive and useful step. However, CUNA notes there is no apparent coordination between the new privacy language added in Section 501 et seq. and the pretext calling provisions which start at Section 521. [Question #4]

Even now, CUNA is working to gain a clearer understanding of credit union information sharing practices and how the H.R. 10 provisions may affect these practices. CUNA's Operations Subcommittee of our Governmental Affairs Committee has undertaken this task. We have several unanswered questions about the privacy provisions that passed the House at the beginning of this month:

- How do the annual disclosures required by Section 503 correlate to the disclosures required by Section 502, and how do the Fair Credit Reporting Act disclosure requirements correlate with the annual disclosures required by Section 503?
- Does usage of experience and transaction data free a financial institution from being classified as a "consumer reporting agency" but still require disclosure? Does this apply to information sharing by all financial institutions or only sharing with nonaffiliates?
- Do the agency standards expected under Section 501(b) correlate to the agency guidance expected under Section 525? [Questions #2 and 3]

CUNA has concluded that certain amendments to the privacy provisions that passed the House as part of H.R. 10 on July 1 should be considered during the upcoming House/Senate Conference:

1. Finalize regulations in twelve, not six months, after the enactment of the law. The Treasury Department study of financial privacy mandated by Section 508 of the legislation is due six months after enactment. With a 12-month period to develop implementing regulations, the agencies and Congress would have six additional months to consider Treasury's findings and recommendations.

The scope of the proposed Treasury privacy study should be clarified as well. Although the title indicates the study is intended to be limited to information sharing among affiliates, the first item under Section 508(a)(1) indicates that the Treasury is to study information sharing with affiliates and nonaffiliated third parties. [Question #2]

2. Amend the definition of "joint agreement" by eliminating the requirement that "and payments between the parties are based on business or profit generated." As not-for-profit entities, credit unions do not fit comfortably into this requirement and may encounter problems with NCUA regulations. This language may also raise problems under state insurance laws regarding prohibitions on profit-sharing arrangements between an insurance company and a non-licensed entity.

3. Amend the definition of "affiliate" to recognize the unique structure of institutions providing financial products and services to credit union members. Credit unions do not typically have affiliated organizations, beyond the limited number of credit union service organizations (CUSOs) that are wholly owned by one credit union. The majority of credit unions' third-party relationships for the promotion and sale of financial products, particularly insurance products, are with companies that are mutually and cooperatively owned by many credit unions. The cooperative nature of individual credit unions made it logical for credit union leaders to form a national mutual insurance company and for credit unions at the state level to organize state corporations, including CUSOs, to provide financial products and services complementing those offered directly by credit unions. Cooperative, mutual organizations within the credit union system should be viewed as comparable to an "affiliate" company structure. The definition of "affiliate" in Section 509(6) should be amended to recognize this similarity. [Question #3]
4. Have similar rules for sharing account information among affiliates and with third parties so long as the third party is a financial institution as defined in this new privacy legislation. The House has already decided to allow information sharing among affiliates. Therefore, information sharing with third parties which are financial institutions should also be allowed *as long as* there is a specific contractual agreement between the financial institutions that requires confidentiality, prohibits any subsequent re-use by another third party, and prohibits third-party financial institution from initiating payments against a consumer's account without the consumer's authorization. CUNA believes it is especially important to allow sharing of confidential information in these guarded situations so that there are not unnecessary constraints on electronic purchases of financial products and services. [Question #4]
5. Apply Section 503(b)(1) annual disclosures to the release of information to affiliated and nonaffiliated entities. Giving consumers a complete picture of actual and potential information sharing possibilities should be a goal of any privacy reforms. Making this change would also clarify how Fair Credit Reporting Act requirements conform to new privacy provisions. [Question #4]
6. Eliminate from the definition of "non-public personal information" subparagraph 509(4)(C) that includes public information lists of names and addresses compiled by sorts using non-public information *as long as* the information is provided to a third party which operates under a contractual restriction requiring confidentiality and the promotional materials sent by the third party to people on the list include information allowing them to ascertain what financial institution provided their names. We feel this promotional materials disclosure rule should apply equally to affiliates using such lists when it would not be obvious to the consumer that information has been shared because the affiliates do not share a common corporate name.
7. Correct NCUA's rulemaking and enforcement authority throughout the bill.
- (a) Under Section 504, the reference should be to the "National Credit Union Administration."
- (b) Under Section 505(a)(2) Enforcement, NCUA properly should only have enforcement authority for federal credit unions, and the Federal Trade Commission should have enforcement for state chartered credit unions, similar to the division of enforcement responsibilities under the

Equal Credit Opportunity Act, the Electronic Funds Transfer Act, the Fair Credit Practices Act, the Fair Credit Reporting Act, the Fair Debt Collections Practices Act, the Consumer Leasing Act, and the Truth-in-Lending Act. (The 1994 enactment of the Truth-in-Savings Act was an aberration to this normal enforcement pattern of consumer protection laws.)

(c) NCUA has not had an "Administrator" since the enactment of P.L. 95-630 in 1978 when the three-member NCUA Board was created. Similar technical mistakes appear in Sections 505(a)(2) and 506(a)(2).

(d) Regarding Subtitle B on Fraudulent Access to Financial Information, credit unions are specifically covered under the definition of "financial institution." Therefore, CUNA urges that NCUA be included in Section 525 and Section 526 on agency guidance and the FTC's consultation with other agencies.

Credit unions want to play a constructive role as Congress and regulatory bodies assess the largely unexplored universe that is financial privacy. Technology and business practices have outpaced the law, and we understand that Congress is going to address this issue. We hope that new requirements are crafted with care and caution, so that the very consumers whom you are trying to protect are not disadvantaged by limited information and choices in financial products.

WRITTEN TESTIMONY OF  
THE CUNA MUTUAL GROUP

SUBMITTED TO THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS  
AND CONSUMER CREDIT  
OF THE  
COMMITTEE ON BANKING AND FINANCIAL SERVICES  
U.S. HOUSE OF REPRESENTATIVES  
CONCERNING  
HEARINGS ON FINANCIAL PRIVACY HELD  
JULY 20, 1999 AND JULY 21, 1999

The CUNA Mutual Group appreciates the opportunity to submit written testimony to the Subcommittee on Financial Institutions and Consumer Credit regarding financial privacy. CUNA Mutual Insurance Society, the holding company of the CUNA Mutual Group, was created in 1935 by credit unions to provide insurance to credit unions and their members. Over the years we have played a substantial role in supporting the credit union movement. Ninety-nine percent (99%) of the eleven thousand (11,000) credit unions in the United States have one or more of our products and we serve approximately thirty million (30,000,000) credit union members with a variety of insurance and financial products. With five thousand (5,000) employees, assets of more than \$7.6 billion and a tradition of serving small and large financial cooperatives, CUNA Mutual is endorsed by the Credit Union National Association, Inc. ("CUNA") as the insurance carrier for the credit union movement. It should be noted that although we share "CUNA" in our names, CUNA Mutual and CUNA are separate legal entities with no financial or ownership ties between them.

CUNA Mutual is committed to providing solutions to help credit unions run modern, cooperative financial institutions dedicated to serving their members. Our consumer products are made available through contractual arrangements with credit unions with the overall purpose of supplementing the traditional savings and lending products credit unions make available to their members. Because of our history and close relationship to the credit union system, we understand very clearly the importance of managing credit union members' personal information – a member's trust in a credit union, and the credit union's trust in our ability to serve its members, is fundamental to our common success. For these reasons, we have established business practices to carefully manage any information that is provided to us. We do not release or sell it to third parties for commercial purposes or engage in outbound telemarketing or cold calling.

Our success in supporting the credit union movement is proof that the exchange of information between financial institutions and non-affiliated third parties is not always injurious or offensive to consumer interests so long as it is managed responsibly with a sensitivity to the privacy expectations consumers rightfully have in their personal information. There are many benefits to consumers through the controlled exchanges of information as demonstrated most recently by the rapid interest consumers have shown in all variations of electronic commerce. We are concerned



that recent privacy initiatives, as embodied in H.R. 10, will eliminate or, at minimum, chill these opportunities in an attempt to curb abusive and irresponsible data management practices.

With the above as background, these comments are directed to the privacy provisions in H.R. 10 from the point of view of an insurance and financial services company that is dedicated to serving the credit union system. We believe H.R. 10's privacy provisions are tilted to favor large financial institutions with affiliated corporate structures at the expense of protecting consumer interests. We are also concerned that the notice and disclosure burdens fall disproportionately on small financial institutions which will ultimately reduce the variety of products made available in the marketplace. These shortcomings can be corrected without sacrificing consumer privacy protections and the overall objectives of H.R. 10 by addressing four provisions within the privacy amendment. Our recommendations are as follows:

**1. Amend the definition of "affiliate" to recognize the cooperative tradition of the credit union movement which serves as an alternative to the "affiliate" structure as envisioned in H.R. 10.**

Credit unions do not have the benefits of an affiliated corporate structure and therefore the notice and disclosure obligations fall disproportionately on the cooperative system when compared to larger, affiliated corporations. Sixty-one percent (61%) of credit unions across the country are small financial institutions with less than \$10 million dollars of assets. Many of these credit unions do not have the ability to efficiently administer the various disclosures imposed upon them if the H.R. 10 privacy provisions are ultimately adopted.

We think this is unfair given the flexibility granted to large affiliated company structures and we fear that many small credit unions will discontinue providing products and services through third party relationships simply because the burden of administering the disclosures will be too great. The result would be an unfortunate anti-consumer consequence of H.R. 10's privacy protections felt the hardest by many small credit unions and their members located in urban and rural areas traditionally ignored by larger financial institutions. Consumers will see fewer products in the market and less incentive to turn to their credit unions for such services.

Credit unions and consumers would be treated more fairly if "affiliate" was defined to recognize the cooperative tradition of the credit union movement. Credit unions do not typically have affiliated organizations beyond the limited number of credit union service organizations ("CUSOs") that are wholly owned by one credit union. The majority of credit unions' third-party relationships for the promotion and sale of financial products, particularly insurance products, are with companies that are mutually and cooperatively owned by many credit unions. This is true for CUNA Mutual as well as other entities organized across the country designed to serve the particular needs of the credit union system. The cooperative nature of individual credit unions has made it logical for credit union leaders to turn within the credit union system for insurance, mortgage, data processing and other services that complement products offered by credit unions and meet operational needs credit unions have in conducting their business.

This cooperative tradition is an important characteristic of the credit union system which has resulted in a web of non-affiliated third party relationships that are comparable to an "affiliate" company structure. The relationships among mutually owned entities serve the same purpose as those found in an "affiliated" structure. Accordingly, we propose to amend the definition of affiliate found in §509(6) as follows:

"AFFILIATE – The term "affiliate" shall mean

- (1) any company that controls, is controlled by, or is under common control with another company; and
- (2) shall include any mutually or cooperatively owned entities, and their affiliates, which have entered into a formal contractual agreement to make products and services available to one or more cooperatives or their members.

This definition retains the original concept of requiring an affiliate to have a relationship with an entity that has the capacity to control its operation while also recognizing the role of the cooperative system in relying upon mutually owned entities to serve its needs in the same capacity as within an "affiliated" structure.

## 2. Establish similar rules for sharing account information among affiliates and with third parties.

Rules for sharing account information should be uniformly applied to affiliated and third party relationships. The broad prohibition in H.R. 10, §502(d) against the release of account numbers to third parties creates significant disadvantages for credit unions and other financial institutions that can not benefit from an "affiliated" structure which includes affiliated telemarketing or mass mailing entities. Consumers will also be restricted from making electronic purchases of products and services if account numbers are not permitted to be released to facilitate customer-authorized sales.

CUNA Mutual supports permitting account information sharing so long as there are strong privacy protections requiring the financial institution and third party to enter into a contractual agreement which includes specific consumer confidentiality provisions, prohibits the third party from initiating any payments against the accounts absent the consumer's authorization and restricts the re-sale of customer information to a non-affiliated third party. The flat ban of H.R. 10, §502(d) is overly restrictive and disproportionately affects small financial institutions which must contract with non-affiliated third parties to expand their product and service offerings to their customers. It also eliminates efficiencies obtained by using account number as a single personal identifier to remove list redundancies and thereby avoid sending consumers multiple duplicate mailings.

We believe limited and purposeful exchanges of information can avoid causing injury to privacy concerns while also benefiting consumers if §502(d) is revised as follows:

A financial institution shall not disclose an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in

telemarketing, direct mail marketing or other marketing through electronic mail to the consumer unless such release is subject to a joint agreement in which (1) any data exchange will be protected by a data encryption or other security device; (2) a provision prohibits the resale of the information; and (3) the consumer's express authorization is required to use the account number to execute a transaction.

3. **Amend the definition of "Joint Agreement" to eliminate conflict with NCUA regulations and state insurance law.**

Under H.R. 10, §509(10), a "joint agreement" is defined as a formal written contract pursuant to which two or more financial institutions jointly offer, endorse, or sponsor a financial product or service and any payments between the parties **are based on business or profit generated** (bold italics added for emphasis). We recommend deleting "are based on business or profit generated" because this language directly conflicts with NCUA Rule Part 721 which restricts federal credit union compensation to administrative expense reimbursements (under NCUA regulations, Rule 721 restricts the amount of compensation a federal credit union may receive from insurance sales and prohibits a federal credit union from receiving income, other than administrative expense reimbursements, from all other third party services made available to members).

The current language also conflicts with state insurance laws which prohibit profit sharing between an insurance company or agent and a non-licensed entity. The definition will have the operative effect of requiring credit unions to become licensed in order to benefit from the "joint agreement" exception found in §502(c). However, under many states' laws, credit unions are not eligible to be licensed and therefore, the benefit of §502(c) is unavailable to these financial institutions.

We believe these significant problems likely result from drafting oversights and can be easily resolved **without any substantive change** to the intent of the meaning of "joint agreement" by simply deleting the reference to "**business or profit generated.**" For these reasons, we recommend that Section 509(10) be revised as follows:

(10) JOINT AGREEMENT. – The term "joint agreement" means a formal written contract pursuant to which two or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

4. **Prohibit Grouping of Consumers That Reveals Personally Identifiable Information.**

Section 509(4) includes within the definition of nonpublic personal information "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that *is derived* using any personally identifiable information other than publicly available information" (highlighting and italics added for emphasis). This definition permits affiliated entities to exchange personally identifiable information for market segmentation modeling purposes without disclosure but places credit unions at a disadvantage simply because the benefits of an affiliate structure are not available in the credit union system.

This imbalance can be corrected if the definition of "affiliate" as proposed above is adopted. Absent that change, §509(b)(C) should be amended to focus on whether a consumer's personal information is identifiable or revealed, as opposed to, whether the list, per se, was derived in part from personal information. Alternative language to Section 509(b)(C) is as follows:

(C) Notwithstanding subparagraph (B), such term shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that identifies or reveals the consumer's personally identifiable information.

#### Summary

H.R. 10's privacy amendments moved very quickly through the House and we question whether law makers have had the time to digest the impact these important provisions will have on financial services. Certainly the provisions have brought the credit union movement into the debate even though we have stayed away from Congressional financial modernization efforts. Now that we are in the process, CUNA Mutual and the credit unions we serve seek to ensure that the disclosure requirements are applied fairly to large and small financial institutions.

In closing, we hope that you find these comments helpful. CUNA Mutual believes that the privacy provisions can be amended to permit reasonably protected exchanges of information without sacrificing consumer privacy. We are optimistic that you will agree and support the changes proposed above.



1717  
 Pennsylvania  
 Avenue, N.W.,  
 Suite 500  
 Washington,  
 D.C. 20006

202-974-1000

info@efscouncil.org

Organizers  
 Countrywide Home Loans, Inc.  
 Intuit Inc.  
 GE Capital Mortgage Corporation  
 Microsoft Corporation

Contact: Jeremiah S. Buckley  
 Counsel  
 (202) 974-1010  
 info@efscouncil.org

**Testimony Submitted by the  
 Electronic Financial Services Council  
 to the Financial Institutions Subcommittee of the  
 House Committee on Banking and Financial Services**

July 20, 1999

Thank you for the opportunity to present testimony regarding issues of financial privacy. Your hearings, Madam Chairwoman, will provide a forum for a comprehensive discussion and analysis on how best to proceed with any privacy legislation.

The Electronic Financial Services Council was established in January of 1999. Its mission is to meet consumer needs for easier access to financial products and services by updating laws and regulations to facilitate electronic commerce. The Council seeks to promote legislation and regulations designed to ensure that electronic commerce continues to revolutionize the availability and delivery of financial services, including mortgage loans, insurance products, investment products, consumer loans and on-line banking.

Membership in the Council is open to businesses regularly engaged in offering, originating, servicing, investing in or facilitating the delivery of financial services through electronic commerce. The Council does not restrict its membership based on a company's charter or license, but seeks to bring together leading companies from various sectors within the financial services industry which share the goal of promoting electronic commerce.

While this testimony presents the views of the Council, individual members may on some issues adopt positions differing from those expressed herein.

**Perspectives on Financial Privacy**

As companies providing financial services both on and offline, members of the Council are sensitive to the need to protect the privacy of customer information as is shown by the business policies and practices voluntarily adopted by its Council members. The availability of privacy protections increasingly is becoming a competitive feature in the offering of financial products through electronic commerce.



In fashioning any privacy policy, both the private sector and the government need to consider the extent to which the collection and use of individual information has direct benefits to consumers. In the financial services industry, the collection, analysis and use of individual customer information lowers the cost of credit and other financial services to consumers in numerous ways:

- It enables the development and use of credit scoring models and automated underwriting systems.
- It facilitates secondary market sales.
- It assists anti-fraud efforts.
- It facilitates the development of new products tailored to consumer needs.
- It allows marketing to be targeted to consumer preferences rather than being wastefully broadcast.

As technology improves, the uses of individual customer information will increasingly influence the creation and delivery of innovative financial services helping to produce better and more responsive services, and making their delivery more effective and responsive to consumer preferences and needs. In our efforts to protect the privacy of individual consumer data, we should be careful not to adopt standards which impair the beneficial uses of data regarding consumer preferences.

As noted in the recent Federal Trade Commission Report on online privacy (July 13, 1999), the flexibility inherent in a market-driven, market-enforced system should not be overlooked. Companies that do not adequately respect consumer privacy concerns as those concerns develop may be expected to lose market share. It has been the experience of our members that those companies that respond quickly and effectively to consumer demands for privacy are more likely to prosper. In a world where consumer privacy expectations are continually evolving, one can make a strong case that the best system for dealing with consumer privacy concerns is a market-driven one like that developing in the online world.

In addition to market forces, it should be noted that specific statutes already in place related to unfair and deceptive practices give state attorneys general and the FTC the ability to deal with abuses or the failure of a company to comply with its stated privacy policy, and they are doing so.



Although we believe that market forces are addressing privacy concerns and will continue to bring about enhancements in the privacy protections provided by financial services firms to the public, we recognize the desire expressed by the House to adopt national standards. In this regard, if Congress chooses to legislate with respect to privacy standards, it would be desirable that such legislation take the form of a uniform national privacy standard. Such a standard would be particularly appropriate in a borderless environment such as the Internet. Even in the absence of a uniform national standard, however, we would ask that any legislation adopted by the Congress be clear and effective, and to that end we would like to suggest some areas which we believe might benefit from clarification.

#### **Comments on H.R. 10's Financial Privacy Provisions**

This hearing provides the first opportunity to comment on the provisions on financial privacy contained in H.R. 10, the "Financial Services Act of 1999." Because these provisions represent the first statement of Congressional intent with respect to financial privacy regulation, we believe that a careful review of the specific provisions of this proposal will greatly assist in developing and refining a record of such Congressional intent. Your foresight in calling these hearings, Madam Chairwoman, is to be commended. You have provided the first Committee forum for expression of views by the public on this important issue.

#### *Scope of Coverage of the Privacy Provisions*

##### **1. Definition of Financial Institution**

H.R. 10's definition of "financial institution" would cover all institutions that engage in financial activities or activities "incidental" to financial activities, as defined by H.R. 10. Is the term "financial institution" intended to be restricted to companies which are chartered or licensed to provide financial services or is it intended to cover any business which may engage in an activity in which a financial services holding company is permitted to engage? For example, the Comptroller of the Currency recently ruled that a bank may act as a retail website host because the provision of such service is deemed to be the "business of banking." Would all website hosts be deemed to be "financial institutions" for the purposes of the privacy provision of H.R. 10?



If it is the intent of Congress to regulate "financial institutions" as that word is commonly understood, the term probably should be defined to include entities which are chartered or licensed by a state or the federal government to provide financial services to the public. This definition would be broad enough to cover not only the traditional, chartered providers of financial services such as banks, insurance companies and securities firms, but also mortgage brokers, small loan companies and others who are licensed to provide financial services to the public. The scope of the definition should include any company receiving non-public, personal financial information from a financial institution, but would not sweep in any company, whether affiliated with a financial institution or not, that does not receive non-public, personal financial information from a financial institution.

In the alternative, if it is the intent of Congress that any person or entity receiving "nonpublic personal information" should be covered by the privacy provisions of H.R. 10, then that should be made clear and there would be no need to introduce the concept of "financial institution" into the privacy amendment. Such an approach would, of course, encompass a broad range of business entities who receive information that may be characterized as "nonpublic personal information." This would put a high premium on defining very precisely what constitutes "nonpublic personal information," and it would be important that all persons required to comply with H.R. 10's privacy provisions be given an opportunity to comment on the effect of the legislation on their operations.

## 2. Definition of Nonpublic Personal Information

The privacy subtitle defines "nonpublic personal information" to include personally identifiable financial information that is:

- provided to a financial institution by a consumer,
- resulting from any transaction with the consumer, or
- "otherwise obtained by the financial institution."

The third category could encompass information obtained by a financial institution outside the context of any customer relationship. Although publicly available information is exempt from regulation, the legislation leaves it to the regulators to define what constitutes publicly available information.





The legislation also leaves to the regulatory process a precise definition of what constitutes personally identifiable financial information. Because this concept is so central to legislative intent, it would be desirable to give these words more precise meaning. One way to do so would be to exclude from the definition information which is "otherwise obtained by the financial institution," thus confining the protected information to information relating to a person's finances supplied to a financial institution by a customer or generated by the financial institution in connection with a transaction with the customer, including the fact that the customer has established an account or other relationship with the financial institution. This would exclude information on potential customers which is obtained by a financial institution outside of the context of any customer relationship.

In addition, Section 509(4)(C) of the legislation states that the term "nonpublic personal information" shall include any . . . "grouping of consumers (and publicly available information pertaining to them) that is *derived* from using personally identifiable information other than publicly available information" (emphasis added). Can nonaffiliated companies aggregate individual data into a larger shared inter-company database (for purposes of analysis only) without receiving consent? This provision could make the business of aggregating and analyzing information, which is essential to the effective use of information, cumbersome and expensive outside of a single financial services institution.

### 3. Retroactive Impact

H.R. 10 does not discuss what restrictions, if any, apply to information collected prior to the enactment of the bill's privacy protections. It would seem to apply to all "nonpublic personal information" which may have been obtained by any means by a "financial institution." While it might be feasible to disclose privacy policies and offer an opt out to consumers on a going forward basis, the burden of offering an opt out to present and former customers before sharing, for example, information "derived" from "nonpublic personal information" could hamper any effective use of historical data regarding consumer preferences and performance. If this information is made inaccessible or difficult to use, the law could have the effect of frustrating important research needed for financial product development and enhancement of the delivery of financial services. We doubt that this is the intent of Congress, but clarification on this point would seem to be appropriate.



#### 4. "Opt Out" Consent Requirement

Any consent requirement related to consumer data sharing could generate litigation unless legal requirements are very precisely defined. For example, questions may arise as to whether the consent was "informed?" Was the disclosure complete? Must companies seek a general consent or can they limit the proposed use of data subject to consent by describing uses? Can consent be revoked?

#### 5. Timing of Privacy Notice

The bill provides that the consumer must receive information concerning the financial institution's privacy policy when the customer relationship "is established." This is a hard thing to pinpoint especially in an electronic context or in the more familiar telemarketing context. Would the relationship be "established" when you visit a website, when you use the Internet to shop for financial information, or when you provide nonpublic personal information?

#### **Conclusion**

..

The action of the House in early July to include privacy provisions in H.R. 10 reflects strong public demand that consumer privacy be protected by legislation. Because the members of the Council have adopted privacy policies along the lines of those which the House has provided for in the privacy amendment to H.R. 10, we understand the motivation for these provisions. However, we believe that it is important that Congress provide clear definitions regarding what companies are covered and what they must do to comply.



**NATIONAL COUNCIL OF INVESTIGATION & SECURITY SERVICES, INC.**  
 THE NATIONAL VOICE OF THE PRIVATE INVESTIGATION & SECURITY INDUSTRY

**BOARD MEMBERS**

*President*  
 John E. Slagowski

*First Vice President*  
 John G. Tsagaris

*Second Vice President*  
 Kenneth E. Romine

*Third Vice President*  
 Sydney J. Huckvale

*Secretary*  
 Lynette H. Rivla

*Treasurer*  
*Chairman of the Board*  
 Daniel R. Westbrook

*Region I*  
 Roy Buckan  
 Don C. Johnson

*Region II*  
 John Doyle  
 Bruce Hulme

*Region III*  
 Buddy Bombel  
 Brian McGuinness

*Region IV*  
 Tom Davidson  
 Joe A. Stennetz

*Region V*  
 Eugene Ferraro  
 Robert Heales

*Region VI*  
 Bertram Falbaum

*Members at Large*  
 Lloyd Davis  
 A. Dale Wunderlich

**EXECUTIVE DIRECTOR**  
 Sharon Hike

**NCISS OFFICE**

*Headquarters*  
 611 Pennsylvania Avenue, S.E.  
 Suite 2686  
 Washington, D.C. 20003-4303

*Administration*  
 938 21st Street  
 Sacramento, CA 95814  
 800 445 8408  
 916 441 2616  
 Fax 916 441 2617  
 E-Mail: [nciss@aol.com](mailto:nciss@aol.com)  
[www.nciss.com](http://www.nciss.com)

Statement of Eddy L. McClain

Chairman of Krout & Schneider, Inc.

for

National Council of Investigation & Security Services, Inc.

before the

Subcommittee on Financial Institutions & Consumer Credit

July 20, 1999

Good morning. My name is Eddy McClain. I am the Chairman of Krout and Schneider, Inc, a private investigative firm located in California. The firm has been in business for 72 years and I've been employed there for 39 years. I am appearing this morning on behalf of the National Council of Investigation and Security Services (NCISS) representing both investigative and protective service companies and many State associations throughout the United States. I previously served as Chairman and President of NCISS and am currently a member of the Board of Directors.

### **Judicial System Threatened by Information Restrictions**

The investigative community is well aware of the public's concern with privacy. We share those concerns. No one should have unfettered access to personal financial, medical or other private information without a legitimate need for the information. However, we fear that in its zeal to respond to the public's concern over privacy, Congress is creating a mosaic of restrictions on those who serve the judicial system, which will

- ◆ hamper law enforcement;
- ◆ substantially increase inventory losses;
- ◆ increase fraud on the elderly and others;
- ◆ provide a protective shield for workplace sexual predators;
- ◆ permit debtors to hide assets from the courts;
- ◆ increase theft of intellectual property; and
- ◆ jeopardize employee safety.

### **Financial Privacy Act to Shield Irresponsible Debtors and Criminals**

The privacy debate over HR 10, the Financial Services Modernization Act, dealt mostly with issues relating to the ability of financial firms to share customer data with either their affiliates or outside data miners. But the most far-reaching provision, having the most significant effect on the public, restricts our ability to conduct lawful investigations to determine where an individual may be hiding assets. These restrictions will reward those individuals who mislead the courts about where their assets are located. It will mean that some victims of fraud or automobile accidents will not be able to effect a recovery. This well-meaning legislation will be a cruel hoax on many citizens who go to court, spend thousands of dollars on legal fees to obtain a lawful judgment and then end up with nothing to show for their time and expense. And although this Committee attempted to assist those seeking to obtain child support payments, the provision has been made meaningless by changes added in the Rules Committee vehicle.

It would not be necessary to gut the privacy provisions of HR 10 and permit "pretexting" willy nilly in order to avoid some of these problems I've cited. Our association believes that licensed investigators and other professionals, including attorneys, ought to be able to walk in the front door and openly ask for information about accounts of individuals in pursuit of fraud investigations. Using traditional investigative techniques, which sometimes do include some deception, we ought to be able to pursue debtors and others who hide assets.

We don't propose that this should include deceiving bank employees. But as written, HR 10 doesn't allow any deception to obtain information from an individual about where he or she banks. How does the Committee recommend finding out where assets are hidden by individuals who are willing to lie to the courts?

#### **Drivers License and Postal Restrictions**

Private investigators are also facing further restrictions being considered by the 106th Congress outside of financial privacy legislation. Now pending on the Senate floor as part of the Transportation Appropriations bill is a provision which would deny state departments of motor vehicles the right to provide "personal information" about individuals to anyone without express permission of the individual. This would effectively overturn the Drivers Privacy Protection Act provisions which were the result of Congressional hearings and which expressly permits licensed investigators to obtain such information under appropriate circumstances. At the same time, the US Post Office is no longer making change of address information available to investigators except under very limited circumstances related to service of process.

#### **Fair Credit Reporting Act Amendments Outlaw Many Investigations**

The restrictions on investigators by HR 10, the US Post Office, and the Transportation Appropriations bill are serious but an even greater threat is the impact of the 1996 amendments to the Fair Credit Reporting Act. Under the Fair Credit Reporting Act, any employer using an outside agent to investigate alleged illegal conduct in the workplace must inform the suspect employee he or she is under investigation and obtain permission to conduct the inquiry. This is not an idle concern, voiced by private investigators under a tortured reading of the statute. It is the opinion of the Federal Trade Commission attorneys who are charged with carrying out the provisions of the Act. I'm attaching a memorandum prepared by an attorney who testified on behalf of NCISS at the FTC and Federal Reserve Board privacy hearings, explaining how the provisions of the Act lead to this absurd result. Also attached is correspondence from FTC staff demonstrating that this notice requirement applies specifically to employer investigations of sexual harassment complaints. Can you imagine how many women will complain to their employers about boorish or predatory behavior when they learn that everything they say will be turned over to the accused?

### **Unintended Consequences Undermine Workplace Protections**

For the last several decades, Congress has enacted statutes designed to protect employees from a number of harms. The Occupational Health and Safety Act and the various civil rights statutes were enacted to provide a safe workplace and one in which all citizens have an equal opportunity to succeed in the American workforce. But now, in the name of privacy, Congress is eliminating the tools, which are essential to enforce those statutes. Employers are required to provide a safe workplace by OSHA, and Title VII requires them to investigate allegations of sexual harassment. Yet the amended Fair Credit Reporting Act makes it virtually impossible for a concerned employer to comply with the law.

### **Confluence of Legislation Undermines Law**

The combination of the restrictions I've outlined above will result in increasing numbers of violations of law. Those who seek to avoid meeting their obligations as determined by a court of law will be able to do so with impunity, because they will not have to seek out offshore havens—they can simply bank across town. Workplace drug dealers and substance abusers can flourish on the job without fear of apprehension, endangering the safety of co-workers. Those who choose to steal from their employers will be far more likely to avoid apprehension because they will be warned at the earliest stages of investigation (if the employer even attempts such a futile inquiry). And those individuals who abuse women at work will have nothing to fear, because no witnesses will come forward.

### **Law Enforcement Exemptions and a Safe Work Environment**

Congress routinely exempts law enforcement agencies from compliance with laws which touch on privacy issues, but the fact of the matter is that the authorities have neither the time or the resources to investigate any but the very largest white collar business cases involving such crimes as embezzlement, employee theft and drug abuse in the workplace. In many cases, the sole way in which a case can be brought forth to prosecution is through the efforts of private law enforcement such as corporate security officials or State-licensed private investigators. Congress needs to remember that private security in the United States is three times the size of public law enforcement in personnel and budget. In stopping white collar crime, public law enforcement officials normally rely on private security and State-licensed private investigators to gather evidence and prepare cases for prosecution. The honest workers of America are entitled to a safe place to work free of drugs, crime and harassment. Employers must have the tools to create and maintain this environment.

**What Can Be Done**

The Fair Credit Reporting Act, must be amended to permit employers to hire licensed private investigators or attorneys to conduct investigations covering drug use, violence, sexual harassment and other violations of law without triggering the complex reporting requirements of the Act. We have attached suggested amendment language.

We also are hopeful that those of you who will be serving as Conferees on HR 10 will be willing to review the specific language of the bill and permit licensed investigators to conduct legitimate inquiries to locate assets.

Thank you for your kind consideration.

## PROPOSED FCRA AMENDMENT

ADD AT THE END OF SECTION 603(D) (2) (A) (15 USC 1681a(d) (2) (A) :

(iv) report prepared by an agent or employee of a consumer's employer solely for the purpose of investigating allegations of drug use or sales, violence, sexual harassment, employment discrimination, job safety or health violations, criminal activity including theft, embezzlement, sabotage, arson, patient or elder abuse, child abuse, or other violations of law, in the employer's workplace.

Explanation of amendment:

This amendment would exclude from the definition of "consumer report" under the FCRA investigative reports prepared for employers in response to allegations of criminal or other illegal conduct in the workplace.

American workers have a right to a safe and secure working environment, free of violence, sexual harassment, drug use, physically dangerous conditions, or other criminal or illegal conduct. In the same vein, American employers have a legal and moral responsibility to investigate allegations that employees are violating these rights of their co-workers by engaging in criminal or illegal activity. As currently drafted and expansively interpreted by the Federal Trade Commission, the Fair Credit Reporting Act (FCRA) constitutes a serious obstacle to employers who seek to respond effectively to threats to the safety and security of their workplace.

The operative term in the FCRA which currently sweeps too broadly is "consumer report." Section 603(d) of the FCRA defines a "consumer report" to include "any written, oral or other communication of any information ... bearing on a consumer's ... character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for ... employment purposes." "Employment purposes" in turn, is defined to include not only the initial employment decision but also decisions about promoting, reassigning or retaining a current employee.

Under this expansive definition, an employer who receives a credible allegation that a current employee is, for example, selling or using drugs in the workplace, faces a difficult legal dilemma. The wisest course of action would be to retain the services of a qualified investigator to look into the allegation in an effort to prove it or disprove it, thus providing the basis for an appropriate response by the employer. By doing so, however, the employer is, under the FCRA, commissioning the creation of a "consumer report," since he is seeking information about the suspect employee's "personal characteristics or mode of living" and doing so for "employment purposes," such as deciding whether or not to suspend or fire the employee. These facts trigger a number of obligations under the FCRA, which are almost certain to compromise the effectiveness of the investigation.

First, under section 604(b) (2) (A) of the FCRA, the employer cannot "cause a consumer report to be procured for employment purposes" unless he has previously disclosed this fact to the employee and obtained his written authorization. In other words, the employer cannot even begin to investigate



an allegation until he first discloses the investigation to the employee and obtains his permission to carry it out. In most cases, giving the employee this veto power will destroy any chance of carrying out a thorough investigation that will get at the truth. Either the employee will simply refuse to authorize the investigation, or, if the allegation is well founded, there is a serious risk that the employee will destroy evidence, intimidate potential witnesses, or take other actions that make the workplace more, not less, dangerous for his fellow employees.

Second, even if this hurdle is surmounted, the employer faces another obstacle if the investigation turns up information that would dictate suspending, transferring, or firing the employee in question. Under section 604 (b) (3) (A) of the FCRA, before taking any adverse action against the employee "based in whole or in part" on the investigative report, the employer must give the employee a copy of the entire report. "Adverse action" is broadly defined, in section 602(k) of the FCRA, to include "any ... decision for employment purposes that adversely affects any current or prospective employee." Thus, even in a case in which an investigation turns up compelling evidence that an employee poses an immediate threat of physical violence, sexual harassment, or other serious risk to his fellow employees, the employer cannot, without violating the FCRA, suspend the dangerous employee or take other urgently needed action, without first disclosing the entire investigative report to the dangerous employee. Nothing in the FCRA even authorizes the employer to edit the report - for example, to maintain the anonymity of adverse witnesses whose safety or lives might be at stake - before turning it over to the employee in question.

These crippling restrictions on the ability of employers to fulfill their obligations to provide a safe and violence-free workplace seem to be unintended consequences of FCRA amendments adopted by Congress in 1996. Recent advisory opinions rendered by FTC staff attorneys reinforce the sweeping impact of the 1996 amendments. These opinions have insisted, for example, that the broad definition of "employment purposes" be "interpreted liberally," and that the requirement to provide the report to the employee in question before any adverse action is taken must be strictly complied with, "even where the information contained in the report ... would automatically disqualify the individual from employment or lead to an adverse employment action." FTC staff opinions have also pointed out that the new FCRA strictures apply even outside the scope of traditional employment relationships; thus, even a homeowner checking out references on a prospective home repair contractor could be required to obtain the contractor's authorization before doing so, and to disclose the results of such a check to the contractor before declining to engage him or her.

Employers - or even individual homeowners - who violate the strictures created in the 1996 amendments could find themselves on the wrong end of federal civil litigation charging violations of the FCRA, in which compensatory (or pre-set statutory) and punitive damages would be sought, and in which the court could also order the employer to pay for the plaintiff's attorneys. In other words, an employee who is suspended or fired for committing criminal acts on the job, including assaults, rapes, drug dealing, or theft, or for engaging in other illegal activity such as sexual harassment, racial or religious discrimination, or workplace safety violations, could sue the employer because the employee had not been given the opportunity to veto any investigation of alleged misconduct, or because the full investigative report had not been disclosed to him before the firing

or suspension. In such a case, the fact that all the allegations were true, and that the employer had to act in order to maintain a safe workplace for all its other employees, would not constitute any defense to the claim that the FCRA had been violated. While it is too soon to expect to see such verdicts arise under the 1996 FCRA amendments, the plain language of the amendments, and the interpretation already being given them by FTC staff attorneys, invite such an outcome.

The proposed amendment would prevent these harmful and unintended consequences by excluding from the definition of "consumer report" a report prepared by or for an employer solely for the purpose of investigating allegations of serious criminal violations in the workplace, and used only for that purpose. In commissioning such a report by a qualified independent investigator, or by the employer's own security staff, the employer would not be causing the creation of a "consumer report" for FCRA purposes, and thus the strictures of section 604(b) regarding prior approval by, and disclosure to, the employee would not apply.

The amendment would not, of course, prevent an employee who has suffered an adverse action from seeking to learn the complete basis for such action by means other than the FCRA. Nor would it affect in any way that employee's ability to seek redress for an unjustified action, whether through the grievance and arbitration provisions of a collective bargaining agreement, or through any civil cause of action that may be available under the particular circumstances. All the amendment would do is to relieve employers of the dilemma they currently face when confronted with substantial allegations of serious wrongdoing in the workplace: either to act to protect the safety and security of the entire workforce, while exposing themselves to a federal lawsuit under the FCRA; or to abide by the FCRA amendments, without regard to the consequences for the co-workers of a violent, harassing, or otherwise dangerous employee.

Related article in *Lawyers Weekly USA*:

**Employers, Lawyers Who Investigate Harassment Liable Under Credit Act?**

Employers and the law firms or consultants they hire to investigate sexual harassment complaints may be sued by the people they investigate under the federal Fair Credit Reporting Act, according to an advisory letter issued by a staff attorney for the Federal Trade Commission, the agency charged with enforcing the Act.

*Lawyers Weekly USA* Issue Date: May 31, 1999

Cite this Article 99 LWUSA 481

---

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

Division of Financial Practices

April 5, 1999

Judi A. Vail, Esq.  
1111 Main Street, Suite 604  
Vancouver, Washington 98660

Re: Sexual Harassment Investigations and the Fair Credit Reporting Act;  
Sections 603(e), 603(f), 603(k)(1)(B)(ii), and 604(b)(3)(A) of the Fair Credit  
Reporting Act.

Dear Ms. Vail:

This is in response to your letter posing two questions concerning the application of the Fair Credit Reporting Act (FCRA) to sexual harassment investigations. You note, by way of context for your inquiries, that the Civil Rights Act of 1964 (Title VII) prohibits discrimination in employment on the basis of race, color, religion, sex or national origin, and that under Title VII an employer has specific obligations, including the obligation to investigate allegations of sexual harassment in the workplace. If harassment is found to have occurred, appropriate corrective or disciplinary action may be taken. We agree with your assessment that such action could reasonably be defined as an adverse employment decision under Section 603(k)(1)(B)(ii) of the FCRA. That section provides that "adverse action" means "a denial of employment or any other decision for employment purposes that adversely affects any current . . . employee."

*1. Application of Section 603(f) or 606 to outside organizations that regularly engage in assisting employers with investigations for a fee if the scope of their investigation does not exceed the employer's workforce or company documents. (Would investigatory information compiled solely from employees and documents within the workplace be defined as a consumer report or investigative consumer report?)*

The relevant inquiry here is not whether the scope of the investigation goes beyond the

employer's workforce or internal documents. Section 603(f) of the FCRA defines a consumer reporting agency (CRA) as any person which, for monetary fees, "assembles or evaluates" credit information or other information on consumers for the purpose of regularly furnishing "consumer reports" to third parties using any means or facility of interstate commerce. A "consumer report" is, in turn, defined in Section 603(d)(1) as a report containing information bearing on an individual's "character, general reputation, personal characteristics, or mode of living" that is used or expected to be used for the purpose of serving as a factor in establishing the consumer's eligibility for, among other things, employment. From the information in your letter, it seems reasonably clear that the outside organizations utilized by employers to assist in their investigations of harassment claims "assemble or evaluate" information. See the fuller discussion of this issue under point one in the enclosed staff opinion letter (*LeBlanc*, 6/9/98).

Thus, once an employer turns to an outside organization for assistance in investigation of harassment claims in the manner outlined in your letter, the assisting entity is a CRA because it furnishes "consumer reports" to a "third party" (the employer). For purposes of determining whether the entity is a CRA, the FCRA does not distinguish whether the information on consumers is obtained from "internal" records or from outside the employer's workplace. The source and scope of information *does* enter into a determination of whether the information is a "consumer report" or an "investigative consumer report."

An "investigative consumer report" is defined in Section 603(e) of the FCRA as "a consumer report . . . in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with other with who he is acquainted or who may have knowledge concerning any such items of information." I have enclosed a staff letter (*Hinkle*, 7/9/98) that discusses the considerations involved in analyzing the application of this section. From the limited facts outlined in your letter, it would appear that the reports prepared by outside organizations performing harassment investigations for employers are most likely "investigative consumer reports" within the meaning of the FCRA. As your letter recognizes, employers who utilize consumer reports or investigative consumer reports have certain obligations under the FCRA to notify employees and/or supply a copy of the report to the employee. (See generally *Hawkey*, 12/18/97; copy attached.)

2. *When a consumer or investigative consumer report is released pursuant to Sections 604(b)(3), 615(a) or 606(a)(1)(B) by the employer or consumer reporting agency, to what degree may the information be redacted?*

Information cannot be redacted in those instances in which the FCRA requires that the consumer be provided a copy of a consumer report (Section 604(b)(3)(A)). I enclose a copy of a prior staff opinion letter (*Hahn*, 7/8/98) which explicates this requirement more fully. I also note that the staff has taken the position that an employer who uses investigative consumer reports must comply fully with the provision of the FCRA that apply generally to "consumer reports" (such as Sections 604(b) and 615(a)),<sup>(1)</sup> as well as the provisions that apply specifically to investigative consumer reports (Section 606). (*Beaudette*, 6/9/98; copy attached.)

I hope that this information is helpful to you. The views expressed herein are the views of

the Commission staff and are advisory in nature. They do not necessarily reflect the views of the Commission or of any particular Commissioner.

Very truly yours,

Christopher W. Keller  
Attorney

---

1. You refer to a staff letter (*Weisberg*, 6/27/97), that responded affirmatively to an inquiry as to whether an employer would comply with the requirement in Section 604(b)(3) that it make certain disclosures to the consumer "before" taking any adverse action, if it waited five days to take the action. That letter specifically stated that "the facts of any particular employment situation" controls the appropriate waiting period, which would likely be much shorter in the case of an employer who was taking required action to remedy sexual harassment.



# **A P P E N D I X**

July 21, 1999

# Congresswoman

# Marge Roukema

Fifth District - New Jersey

2469 Rayburn House Office Building/Washington, D.C. 20515 (202) 225-4465

Contact:  
J. Craig Shearman  
(202) 225-4465

Release:  
July 21, 1999

## Roukema: Comprehensive Approach Needed for Financial Privacy

*Following is the opening statement of House Financial Institutions Subcommittee Chairwoman Marge Roukema, R-N.J.-5th, as prepared for delivery at today's hearing on financial privacy issues. Today is the second of two days of hearings.*

Good morning. Today is the second day of hearings by the Subcommittee on the issue of customer financial and medical privacy. As I mentioned yesterday, we addressed the privacy issue in great detail in H.R. 10. There are several significant new privacy protections in H.R. 10 — required privacy policies, mandatory "opt out" for consumers on information sharing with third parties, a prohibition on sharing account and credit card information with marketers, and the outlawing of pretext calling. Quite frankly, I think we have made a very good start in H.R. 10 on privacy protections.

Yesterday we heard from three panels of witnesses. These witnesses included academics and other privacy experts, representatives of our smaller financial institutions, credit bureaus and marketers as well as the consumer groups. The hearing covered lots of ground.

Several interesting points were made:

- Virtually all witnesses warned Congress to move carefully in legislating any further privacy protections past what is currently in H.R. 10.
- The majority of witnesses advised against an "opt in" approach at this time.
- Consumers have the right to know who is collecting their information and how that information is to be used. Therefore, to be effective, privacy policies must be clear and easy to understand.
- There was agreement that to be meaningful the customer "opt out" process must be clear and straightforward.
- Small financial institutions use third parties for many common, everyday business practices — such as check printing and data processing — which must be protected.

Many issues remain:

- Should customers be permitted to "opt out" of information sharing with affiliates?
- Several witnesses made the point that the new economy and e-commerce is driven by the availability and use of information — both public and private. What effect would an "opt in" requirement have on the new economy?
- In addition, is it possible that with good disclosure of privacy policies we may be able to eliminate the debate over "opt in" and "opt out"?
- With respect to Section 351 and Medical Privacy, do we need to make it clear that the Secretary of HHS retains authority to promulgate comprehensive medical privacy rules even if H.R. 10 becomes law?
- What other changes, if any, are necessary to tighten up the Ganske medical privacy provisions in Section 351 to make sure consumer medical records are not shared without consumer consent.

The Subcommittee will be looking at these and other issues today. We are committed to looking at all these privacy issues comprehensively. I yield now to the distinguished Ranking Member, Mr. Vento.





Questions in Writing of Congressman Bruce F. Vento  
for the Witnesses at the Financial Institutions and Consumer Credit Hearings on  
EMERGING FINANCIAL PRIVACY ISSUES:  
July 21, 1999

For Richard Fischer

1. Your testimony suggests that the marketplace works. For whom? Are you suggesting that the status quo is protecting individual's privacy?
2. What evidence do you have that sharing information reduces fees and rates to consumers?
3. Can you give some examples of how sharing information has enabled financial institutions to develop and offer consumers an "astonishing array" of financial products and services?
4. Can you give me an example or two (other than those excluded from coverage under H.R. 10) of how information-sharing restrictions would harm consumers by restricting availability of products and services they want or request.
5. Did H.R. 10's privacy provisions leave out any financial institutions that should be covered?
6. Your testimony suggests that FCRA provides all the protection that consumers need for financial privacy. How would you address the serious consumer concerns about transactional and experience data NOT covered by FCRA?
7. Do you agree that control of the portrait painted by a person's financial information belongs to the consumer, not the financial institution that processes the transaction?



Questions in Writing of Congressman Bruce F. Vento  
for the Witnesses at the Financial Institutions and Consumer Credit Hearings on  
EMERGING FINANCIAL PRIVACY ISSUES:  
July 21, 1999

For Treasury's Under Secretary Gary Gensler:

1. What would be an appropriate transition or phase-in period for applying new privacy policy disclosures and new restrictions on sharing of customer data?
2. Would it be useful for the financial institutions regulators to jointly pursue workshops on privacy issues?
3. Is the self regulatory approach of the FTC satisfactory for protecting Internet privacy? Would such a framework work for financial institutions? Does the Administration favor self regulation for financial institutions web sites?
4. Does H.R. 10 as passed the House, or a future limitation on sharing of information among affiliates constrict competitiveness of financial industries vis a vis other non-covered industries? How do we look for more universality or a level playing field on this issue?
5. Does the Federal Trade Commission has adequate staff levels to be a super regulator for privacy? Would that be appropriate in terms of the functional regulation balance that has been sought through H.R. 10?
6. If we were consider limiting information sharing for the purposes of marketing, how would you define marketing? Are there other secondary uses of information that might not be covered by this?
7. In the July 20, 1999, hearing, some of the witnesses discussed allowing sharing for "related purposes". What do you think of this idea? Is it workable? What might be a good definition of "related purpose"?
8. You state in your written testimony (page 5) that "Eventually, we may wish to look beyond financial privacy". Why wait? Does this waiting constrain our financial services sector?



9. Do you think an annual disclosure of privacy policies is too costly? Why or why not?
10. Should we specifically prohibit the affiliating of financial holding companies with telemarketers?
11. If the Conference were to strike Title III, the medical privacy provisions, as some have suggested, why wouldn't that leave an opening for privacy violations between insurance and other affiliates? The deadline for HHS to issue rules is Feb. 2000, right? Do you anticipate that will be on time? Could it be delayed by obstructionists?
12. How are the comprehensive medical privacy plans of other Committees in Congress or the rules being contemplated by the Department of HHS planning to deal with the affiliations of banks and life insurance or property and casualty insurance or other insurance firms (that are not health insurance firms), as provided for under H.R. 10? Will the regulations as directed under HIPAA be as direct and as strong as necessary to preserve individual medical privacy?
13. Should we consider a straight prohibition of medical information sharing under H.R. 10's structure, until the HHS rules are in force?
14. Some medical information needs to be shared for treatment, payment and core business functions. What data is actually used to process these activities?
15. What kind of notice and authorization is "okay" and what kind provides an opportunity to unduly pressure consumers to release information they do not released?
16. Are there instances where authorization shouldn't be required for research activities?
17. Do you think we should amend the FCRA to include transaction and experience data?
18. Do you agree that control of the portrait painted by a person's financial information belongs to the consumer, not the financial institution that process the transactions?



June 28, 1999

The Honorable Tom Bliley  
House Committee on Commerce  
2409 Rayburn House Office Building  
Washington DC 20515

Dear Chairman Bliley,

The undersigned organizations of the Consumer Coalition for Health Privacy are writing to express our deep concern about Title III, Subtitle D (The Confidentiality of Health and Medical Information) in H.R. 10, which addresses the confidentiality of health and medical information. We understand that the *intent* of this language, as offered by Congressman Ganske, was to limit the sharing of information between financial industries and their affiliates. The provision, however, would do exactly the opposite — it would facilitate the broad sharing of sensitive medical information. In order to provide a modicum of protection to health care consumers, this section should be amended so that it is clear that people must be notified, and must give permission, before their health information is shared between affiliates.

The mission of the Consumer Coalition for Health Privacy is to educate and empower health care consumers to have a prominent and informed voice on health privacy issues at the state, federal and local levels. Members of the coalition include consumer, patient, disability, civil liberties and professional organizations committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research. The Coalition is an initiative of the Health Privacy Project at Georgetown University.

There is currently no comprehensive federal law that protects the privacy of medical records. However, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Secretary of Health and Human Services to promulgate regulations if Congress fails to enact such legislation by August 1999. Both the House and the Senate have been moving forward to meet this deadline.

It should be emphasized that the language in H.R. 10 does not meet the requirements of the HIPAA mandate, and that a financial services bill is not the appropriate venue to deal with medical privacy in a *comprehensive* manner. We do believe, however, that in so far as H.R. 10 authorizes the sharing of information between affiliates, it is appropriate to address medical privacy in this specific context. In particular, there needs to be a specific prohibition on the sharing of medical information without notice and consent. People should retain decision-making authority over their medical information. In addition, the current language must be clarified to ensure that stronger state laws will be allowed to stand.

The merging of these two very different industries — the financial and health insurance industries — raises many questions about the ethics of sharing this information that was once separate, proprietary data. The American people have an expectation that this information will be kept separate and private. A health insurance company, for example, should not be able to share information with a bank, or vice-versa, without a person's permission. To allow entities to freely share this information will erode consumer confidence and trust in both industries.

We look forward to working with you to resolve this issue. Please call Janlori Goldman, Health Privacy Project Director, at 202-687-0880 if you have any questions

Sincerely,

AIDS Action  
American Association of Occupational Health Nurses  
American Counseling Association  
American Federation of State, County, and Municipal Employees  
American Medical Association  
American Nurses Association  
Center for Women Policy Studies  
Children & Adults with Attention-Deficit/Hyperactivity Disorder  
Legal Action Center  
Myositis Association  
National Association of Alcoholism and Drug Abuse Counselors  
National Association of People with AIDS  
National Association of Social Workers  
National Mental Health Association  
National Organization for Rare Disorders  
National Partnership for Women & Families  
National Senior Citizens Law Center  
Planned Parenthood Federation of America, Inc.

**Treasury Under Secretary ~~Gary Gensler~~**  
**Subcommittee on Financial Institutions and Consumer Credit**  
**Committee on Banking and Financial Services**  
**United States House of Representatives**

Madam Chair, ranking Member Vento, and members of the Committee, I am pleased to have this opportunity to present the Administration's views on the protection of personal financial information. These issues are of great importance to the President and the entire Administration, and we look forward to working with Congress to provide American consumers the financial privacy protections that they deserve.

Privacy has been a cherished right to Americans since the founding of our nation. Originally, the idea was predominantly one of privacy from governmental interference: privacy in one's home and one's person. The citizenry's fear of governmental intrusions on privacy was rooted partly in American history -- our rejection of tyranny -- but also in practicality. Businesses had neither the means nor the incentive to invade one's privacy.

But over time, the notion of privacy has evolved. The right is no less cherished, but the threats to it are new. When, a century ago, Louis Brandeis famously enunciated privacy as a "right to be let alone," he was referring to privacy from the press.

Today many Americans increasingly feel their privacy threatened by those with whom they do business. In particular, financial institutions and others are able to consolidate information about spending and investing habits. Americans want the ability to earn, invest, and spend their money without having to expose their lives to those who process their transactions --

just as they would not expect a letter carrier to read their mail. Americans deserve that right, and financial services firms wishing to maintain their trust would benefit by embracing it.

For much of our history, consumers were justifiably confident about their financial privacy. Most of their day to day transactions were conducted in cash. They obtained financial services from local firms. Records were kept on paper ledgers rather than in computers. A small town banker, a local securities broker, or an insurance agent knew the customer's financial circumstances and tolerance for risk, to best anticipate the customer's financial needs. Yet customers were confident that the banker, broker or insurance agent would not share that information. Doing so would have been considered a breach of personal trust. That confidence is understandably on the wane today.

The first cracks in that confidence began to appear in the late 1960s, as unprecedented amounts of credit information were collected in new, national databases. Congressional hearings revealed that many credit files contained inaccurate and damaging information, and that consumers often had no way to correct errors that could lead to a denial of credit, employment, or insurance.

The resulting Fair Credit Reporting Act was the first federal law directed at financial privacy. The Act limited the purposes for which credit report information could be distributed, and granted individuals access to their credit histories and the ability to correct errors. Amendments to the Act in 1996 recognized that customers should have notice and the ability to opt out of certain information transfers. Taken together, these were significant privacy protections for their times.

Much has changed, however, since the Fair Credit Reporting Act was passed in response to the mainframe computers of the 1960s. We are in the midst of three important and significant changes in the financial services sector: a technological revolution, industry consolidation, and a move away from cash towards electronic transactions.

First, today's ordinary desktop computer is significantly more powerful than the mainframe of 30 years ago. Vast amounts of information can be stored, sorted, manipulated, and analyzed at lower and lower costs. Advances in telecommunications allow for this information to be sent virtually anywhere on the globe in a fraction of a second. Financial services firms are collectively spending billions of dollars per year to further enhance their technologies.

A second key change is the growing integration and consolidation of financial services providers. Interstate banking and branching has allowed banks to grow larger than ever before, and the removal of regulatory restraints has allowed banking organizations to offer more insurance and securities services. Even those smaller banks that have avoided consolidation often broaden their services by contracting with other financial services providers. At the same time, insurance companies are offering products that compete with bank products, and investment banks are in the lending business.

These developments have brought considerable benefits to consumers, in the form of operating efficiencies, new products, and better prices for customers. The desire of large, integrated financial services firms to profit from their scale and cross-sell their products, however, has created a powerful incentive to treat consumer data as a business asset. Consolidation and technology also have allowed the relationship between financial institutions and their customers to become increasingly impersonal. Fewer customers walk into branches to deal with a personal banker, as more customers drive up to ATMs or log onto the Internet.

Third, there is an increasing use of electronic means of payments and receipts. Americans increasing use of credit cards, debit cards and (more recently) electronic bill payment in lieu of cash now allows financial services companies to collect a far greater amount of information. Direct deposit now means that a bank knows not only what you spend but how much you earn, and from whom.

A generation ago, financial privacy meant keeping private your salary, your bank balances, and your net worth. Today, financial privacy means keeping secret your entire way of life. The typical credit report in 1970 would have shown only that a customer had received a total of, say, \$5,000 of credit, and had repaid it on time. The credit card records of 1999, by contrast, can list each and every purchase ever made by that customer, sorted by date, location, and other details. Furthermore, if credit card companies work together with merchants, then the level of detail can become even more refined -- each dish ordered at a restaurant or each book title bought at a store.

Taken together, these three trends -- a technological revolution, industry consolidation, and the movement from a cash to electronic payment and receipt system -- are the means, motive, and opportunity for financial services firms to mine consumer information for profit. Our challenge, therefore, is to protect the privacy of consumers while preserving the benefits of competition and innovation.

On May 4, the President outlined the Administration's "Financial Privacy and Consumer Protection in the 21<sup>st</sup> Century" initiative. Protecting financial privacy led the list of key principles for consumer protection.

- First, the President recommended enactment of legislation to provide consumers notice and choice before their financial information is shared or sold -- the right to say "no." Central to this policy is the idea that control of the self-portrait painted by one's financial information belongs to the consumer, not the financial institution that processes the transactions.
- Second, the President stated that consumers should not have to worry that the results of their latest physical exam will be used to deny them a home mortgage or credit card. The President therefore recommended legislation that would impose special restrictions on sharing medical information within financial conglomerates and with third parties,



consistent with the Administration's overall plan for protecting medical privacy. The President made clear in his State of the Union Address his intention to work with Congress to pass a strong, comprehensive medical record privacy bill this year. He has consistently encouraged legislation that would expand our authority to protect the privacy of medical information.

- Third, the President called for giving back to regulators authority to monitor compliance with privacy protections. Under the Fair Credit Reporting Act, for example, banking regulators were in 1996 prohibited from examining banks for compliance with this statute, as they do for other consumer protection statutes. Surely there is no compelling reason for treating privacy less seriously than other statutory consumer protections.

When the President announced this agenda in May, some may have viewed his proposals as ambitious. Only two months later, however, the policy of notice and choice is gaining momentum. Leadership by the President and members of this Committee and of the House has sparked a debate on this issue that has educated policy makers and produced dramatic results. Most recently, the House of Representatives passed with overwhelming bipartisan support a bill providing notice and choice before personal financial information can be shared with third parties. The House provided the enforcement mechanisms sought by the President. It also generally prohibited the use of so-called "pretext calling" -- albeit with an unwarranted exception that would allow investigators to commit fraud in child support cases, while a subpoena would be the best approach.

Acceptance of the idea of notice and choice is an important step in protecting financial privacy. Consumer choice over third party sharing, however, should be the floor, not the ceiling. We should move forward to consider how consumers can exercise choice over sharing of transaction and experience information within financial conglomerates -- especially conglomerates which, under H.R. 10 and S. 900, would be able to engage not just in financial activities, but also activities incidental and complementary to such financial activities. We should prevent exceptions from swallowing the rule by prohibiting re-use of shared data beyond the purpose for which it was shared. We should further ensure that any new federal legislation add to -- as we believe H.R. 10 does, but should do so more clearly -- rather than preempt existing protections in federal and state law. And we should consider how to make any privacy protection regime workable, all the while keeping in mind the significant economic benefits that information sharing can bring to consumers.

With that in mind, I will address five basic issues that we believe the Congress ought to consider as it moves forward with financial privacy legislation: what information such legislation should cover; what notice is appropriate; what choice is appropriate; what exceptions may be appropriate; and how any privacy regime is to be administered.

Madam Chair, you also requested that I discuss various privacy issues relating to the privacy practices of state governments and the federal government, and of the Treasury

Department itself. I am attaching as an appendix a discussion of those issues not addressed in my testimony.

### Scope

The first issue is what financial information should be protected. Under the Fair Credit Reporting Act, there are currently no limits on sharing information about consumers' transactions and experience. Thus, financial institutions currently are able to treat what a person buys with checks and credit cards as information belonging to the institution, and are free to sell it.

The Administration believes that this transaction and experience data must be protected, regardless of the type of financial institution at which it is held. Checks written on a checking account should share the same protections as checks written on a money market account. H.R. 10 adopts this sound approach.

We must consider, though, a future where financial information may be consolidated -- and potentially mined -- at non-financial firms. Many of us already provide a list of our assets to Internet web sites, where daily performance can be monitored. Consumers might be surprised if a list of stocks held at an Internet brokerage site were protected as confidential, but a list of stocks entered at another type of web site could be freely sold without notice or consent.

Eventually, we may wish to look beyond financial privacy. Like financial institutions, booksellers and other retailers can build considerable databases and can sell them without customer knowledge or consent. Your on-line bookseller may not only know what books you read, but what books you considered buying, where you vacation, what music you listen to. The Administration continues to support efforts at self-regulation. Industry efforts over the past year have been impressive, but they still have a long way to go. We will want to continue scrutiny of these non-financial areas.

### Notice

Notice is fundamental to privacy protection. The Administration believes that every financial institution should establish and disclose a privacy policy that encompasses information sharing with both affiliates and third parties. Disclosure of an institution's information practices is a precondition to consumers choosing how their information will be used, or choosing to do business elsewhere.

The Administration believes that a meaningful notice should be provided before a customer opens an account and at least annually thereafter. The contents of the notice should be sufficient to inform the customer of the uses that will be made of their information and to whom it will be transferred.

That said, the exact contents of a notice may be best left to a rulemaking process where public comment can be solicited.

### Choice

The next issue is that of choice -- under what circumstances customers should be able to restrict the uses a company makes of their data. The Administration believes that consumers should have the choice to opt out of -- that is, say "no" to -- the use of their data by both third parties and affiliates.

Although the uses of affiliate sharing generally tend to relate more to the consumer's original expectations than third-party sharing, this will not always be the case. Under both pending financial modernization bills, affiliates of banks will be permitted to engage in any financial activity, any activity incidental to financial activities, and to some extent in any activity complementary to such activities. Unless the language is clarified, commercial companies held pursuant to merchant banking and joint ventures -- perhaps even telemarketers -- could be considered affiliates. I would also note that restricting only third party sharing would tend to confer a competitive advantage on large banks, which have many affiliations, as opposed to small banks, which tend to use third parties to service customers.

Congress has embraced notice and choice -- for both affiliates and third parties -- in the Fair Credit Reporting Act. The FCRA has given consumers the right to notice and the opportunity to opt out before a company shares certain credit information with an affiliate. Financial firms have proven the practicality of notice and choice through the implementation of the FCRA. Most recently, U.S. Bancorp, in response to a suit brought by the Minnesota Attorney General, has agreed to notice and opt out before transaction and experience data can be shared with affiliates for direct marketing purposes and with unaffiliated third parties for purposes of marketing financial products or services of the unaffiliated third party. The settlement prohibits sharing information with third parties for purposes of marketing non-financial products.

Nonetheless, some have contended that customers need not have choice over information sharing because they possess the ultimate choice: the ability to take their business elsewhere. We believe that customers are less able to "vote with their feet" on financial privacy than may first appear. Changing one's bank or broker is not a simple matter. It requires a considerable investment of effort and time, as one checking account must be run off as another is created, as direct deposit orders must be reissued, as checks must be reprinted, as new codes must be memorized, as stocks must be transferred. It is a change that most of us make only when we are extremely dissatisfied with our current circumstances.

For that reason, the Administration believes that choice must be guaranteed by law. In most cases, we support the notice of "opt out" choice -- that the sharing may occur so long as the customer is given notice and the opportunity to object. In some cases, with particularly sensitive

information such as medical information, an "opt in" may be appropriate. We also believe that these choices should not be circumvented by allowing a financial institution or an affiliate to do the marketing itself, on behalf of the third party.

Choice would allow consumers to make their own decisions as to the potential tradeoff between their financial privacy and the various marketing opportunities and other potential benefits of information sharing. This is a very personal decision which is most appropriately left to an individual.

### Exceptions

While the Administration is firmly for choice, we also believe that there is a need for balance. There are some types of information sharing where customer choice may not be appropriate -- where allowing customers to opt out of information sharing is counterproductive or too costly. The most obvious case is sharing of information with appropriate law enforcement authorities. Another example is the sharing of information in order to facilitate the processing of individual transactions -- clearing checks, for example.

Other types of information sharing present difficult tradeoffs. In approaching any exceptions and the general policy of choice, we think three questions are appropriate:

- First, what is the consumer's reasonable expectation of privacy? This in turn largely depends on the type and sensitivity of the information. Most people expect that their checks will be processed efficiently -- even if by third parties -- but not that anyone processing the data will be able to learn how they live their lives. They also don't expect that information to be sold without their consent.
- Second, what is the purpose of the transfer? Does it directly benefit the consumer or mostly just the company? Is the company using the information to directly serve the customer, or is the company primarily using or sharing the customer's information for another purpose?
- Third, what are the costs of allowing choice? Does it significantly (i) disrupt the functioning of the enterprise, (ii) raise costs to consumers, or (iii) disrupt markets?

Any decision should be based on a balance of these factors. The Administration strongly believes that in most cases the balance counsels for choice, whether the sharing be with a third party or an affiliate. We also support strict limits on re-use of information shared pursuant to any exception, to the extent that such use exceeds the excepted use.

Perhaps the clearest case for choice is in the area of medical privacy. Although a company may have economic incentives to share medical information, no consumer expects that in consenting to a physical examination for an insurance policy, he or she is endangering an

ability to obtain credit or employment. For that reason, the Administration favors strong restrictions on the ability of any company, including insurance companies, to share medical information. We strongly oppose, however, the medical privacy provisions of H.R. 10. These provisions contain significant exceptions that would, for example, allow re-use of medical information by companies with whom the information is shared, preempt state law, and allow an insurance company to ship information to other companies under the rubric of "marketing research" in circumstances that neither current practice nor future regulations would likely permit.

The provisions also would create uncertainty about the authority of the Department of Health and Human Services to establish stronger protections for customers of financial services companies. Notably, the provisions in H.R. 10 apply to "insurers," who are central to the functioning of the medical system. Such a broad scope would significantly undermine efforts to craft meaningful, comprehensive medical privacy legislation, and would erode existing protections. The Administration strongly urges that these provisions be stricken from the bill in conference.

The sale of marketing information to a third party -- or using such information on behalf of a third party -- also appears to be a clear case where no exception to notice and choice is appropriate. A consumer doing business with a financial institution would not expect the information generated through that relationship be sold for unrelated, especially non-financial, purposes. In such a case, the financial institution would be selling the information primarily for its own profit, not the customer's benefit. Due to advances in technology, maintenance of a "do not market" list has become more easily achievable.

In some cases, though, the case for an exception may be stronger. Financial services firms may wish to provide customers a consolidated account statement including accounts from different affiliates within the organization. Here, the case for an exception from "opt out" appears appropriate. Customers could reasonably expect to have their financial information presented to them in a comprehensive way; the consolidated statement is done for the convenience of the customer, who is able to correct any errors; and the cost of requiring separate mailings for each account could be considerable.

Other cases present more difficult tradeoffs. For example, with respect to risk management, one could conclude that a customer who has defaulted on one loan from a financial organization should not reasonably expect to be able to shield that information from an affiliate considering a second loan. Allowing the information to be shared protects the depository institution from loss, and should result in lower prices for creditworthy borrowers. The same also could be said of information on the timeliness of a customer's payments to the institution -- assuming that such an exception is implemented in a way that ensures that the customer receives notice that such information sharing is occurring and has access to and the ability to correct such information.

The idea that a sister bank could, however, deny a loan because a consumer's credit card reveals risk-taking *behavior* -- say, the recent purchase of a skate board or a sports car -- is far more troublesome. Thus, any information about where a consumer is spending money, or the purposes for which the consumer is obtaining credit, should remain subject to notice and opt out. How we live our lives, what we believe, the choices we make -- all of these very personal pieces of information should not be shared without our consent.

#### The Need for Regulatory Flexibility

Each of the issues we have just discussed is complicated, and the answers may well change as technology and business practices advance. The complexity and uncertainty of the task at hand suggest two further points.

First, we should allow many of the details to be worked out by the regulators that know the financial services industry best, after taking into account public comment. The agencies that examine financial services firms and follow industry trends should be responsible for writing and enforcing privacy rules applicable to the firms that they regulate.

Second, a transition period would be appropriate so that financial institutions can reprogram their systems to take account of customer choices.

#### **Conclusion**

Thank you for allowing me to appear today on an issue of such importance to the Administration. I welcome your questions.

**Appendix to Testimony**  
**Before the Subcommittee on Financial Institutions and Consumer Credit**  
**The Committee on Banking and Financial Services**  
**July 21, 1999**

The following discussion of privacy policy issues complements the written testimony. It addresses federal government privacy policies and federal government web site privacy policies.

**Government privacy policies:**

The Privacy Act of 1974 establishes a set of fair information practices for the federal government's handling of personal information in systems of records. These principles include: written consent as the baseline for disclosure of personal information; notice of the specific purposes for which that information will be used; and access by individuals to their records and the ability to correct mistakes in those records. The Privacy Act does contain some exceptions, such as for certain law enforcement uses.

The Administration has no current proposals to update the Privacy Act, or the Right to Financial Privacy Act, which protects customer records maintained by certain financial institutions from improper disclosure to officials or agencies of the federal government.

This year the President established the position of the Chief Counselor for Privacy at OMB, underscoring the Administration's commitment to examining where progress can be made to improve federal government privacy policies while achieving other important government goals. The Chief Counselor will be engaged in a "privacy dialogue" with state and local governments, as Vice President Gore announced last July 31. This dialogue will include considering the appropriate balance between the privacy of personal information collected by governments, the

right of individuals to access public records, First Amendment values, and Department of Motor Vehicle information.

With respect to the IRS, the agency launched a major effort in late 1997 to eliminate unauthorized access and inspection of taxpayer records. Because the law requires the Service to terminate employees who are found to have engaged in unauthorized access, IRS focused its planning on deterring, preventing and detecting privacy violations, and on administering penalties for unauthorized access. This effort included an extensive training and education program aimed at establishing a single basic principle for all employees: do not look at, access, scan or otherwise gather information from any return or return information that you have no official need to see. IRS is constantly evaluating the success of these efforts and considering additional strategies as it learns from its experience.

**Privacy on federal government web sites:**

All federal agencies have web sites and every federal web site must comply with the Privacy Act.

Federal agencies' web site privacy policies are diverse and are tailored to the information practices of each site. The Office of Management and Budget has provided guidance to agencies for developing their web sites. Jacob Lew, Director, Office of Management and Budget, issued a memorandum to agencies directing them to post privacy policies no later than September 1, 1999. OMB has also issued guidance on good practices for agency web sites. As of July 15, 1999, all Cabinet departments have privacy policies clearly posted on their home pages.

Treasury's web site privacy policy is conspicuously displayed as part of the home page ([www.Treas.gov](http://www.Treas.gov)). The Main Treasury web site does not use "cookies" (that is, a file placed on a visitor's hard drive that allows the web site to monitor the individual's use of the site) to collect information about citizens' visits to the web site. Treasury Bureaus have been notified that Main Treasury's web site should be used as a model. The Financial Management Service uses temporary cookies to maintain a connection with the user to insure the user receives a response, for example to comments, but the cookie is immediately deleted when the user leaves the site.





UNDER SECRETARY

DEPARTMENT OF THE TREASURY  
WASHINGTON  
November 1, 1999

The Honorable Bruce F. Vento  
U.S. House of Representatives  
Washington, D.C. 20515-2304

Dear Congressman Vento:

I appreciated the opportunity to speak about the privacy of personal financial information before the Subcommittee on Financial Institutions and Consumer Credit on July 21. It gave me an opportunity to provide some detail about the Administration's support for including strong privacy protections in financial modernization legislation. Enclosed you will find responses to your written questions, which were submitted to me by House Banking Committee Staff Director Cole, to whom I have sent a copy.

I would be pleased to respond to any further questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "GG", written over the word "Sincerely,".

Gary Gensler  
Under Secretary for Domestic Finance

### Response to Questions on Financial Privacy

**Question 1.** What would be an appropriate transition or phase-in period for applying new privacy policy disclosures and new restrictions on sharing of customer data?

**Answer:** *H.R. 10 requires the Federal banking agencies, the NCUA, the Secretary of the Treasury, and the SEC, after consulting with the FTC and state insurance authorities, to issue final regulations within 6 months after the date of enactment. The bill provides that the privacy provisions in the Subtitle take effect 6 months after the date that the final regulations are issued, unless the regulations specify a later date.*

*We believe the bill appropriately allows the agencies to determine the length of the phase-in period. The agencies should seek public comment on the appropriate effective date as well as on the substance of the rule.*

**Question 2.** Would it be useful for the financial institutions' regulators to jointly pursue workshops on privacy issues?

**Answer:** *Last year, the Treasury asked the financial services regulators to establish an interagency group to coordinate efforts related to privacy issues. The group includes representatives from the OCC, OTS, Federal Reserve System, FDIC, FTC, the Conference of State Bank Supervisors and the Treasury. The regulatory authorities already pursue these issues with their regulated entities -- for example, by issuing guidance -- as the need arises. We have raised the issue of joint workshops with the group, and it is under consideration by members.*

**Question 3.** Is the self-regulatory approach of the FTC satisfactory for protecting Internet privacy? Would such a framework work for financial institutions? Does the Administration favor self-regulation for financial institutions web sites?

**Answer:** *Americans traditionally have been concerned with the privacy of their financial records. Recent developments have intensified this concern.*

*We are in the midst of three important and significant changes in the financial services sector: a technological revolution, industry consolidation, and a move away from cash towards electronic transactions. Given these changes, we believe that the time has come for Congress to act with respect to financial privacy -- just as Congress has already acted to protect phone and video rental records.*

*The Administration would expect that whatever statutory and regulatory protections are provided to customers of financial institutions would apply regardless of whether a customer communicates with his particular institution electronically or in person.*

**Question 4:** Does H.R. 10 as passed [by the] House, or a future limitation on sharing of information among affiliates, constrict competitiveness of financial industries vis a vis other non-covered industries? How do we look for more universality or a level playing field on this issue?

**Answer:** *H.R. 10 applies broadly across all providers of financial services, not just to those already regulated. In addition, it seeks to protect the privacy of consumers while preserving the needs of businesses. This balance is embodied in a series of exceptions to notice and choice in the House bill.*

**Question 5:** Does the Federal Trade Commission [have] adequate staff levels to be a super regulator for privacy? Would that be appropriate in terms of the functional regulation balance that has been sought through H.R. 10?

**Answer:** *We support the system of regulation set forth in H.R. 10. That system would require the federal banking agencies, the NCUA, the Secretary of the Treasury, and the SEC to jointly prescribe regulations after consulting with the FTC and representatives of State insurance authorities designated by the National Association of Insurance Commissioners. The rules prescribed would be enforced by the federal functional regulators and the FTC only with respect to financial institutions subject to their jurisdiction.*

**Question 6:** If we were [to] consider limiting information sharing for the purposes of marketing, how would you define marketing? Are there other secondary uses of information that might not be covered by this?

**Answer:** *A restriction on information sharing only for marketing purposes may be too narrow. Customers should be able to exercise choice about whether confidential financial information is shared generally. We believe that Americans should have the opportunity to participate in the modern means of electronic payments and receipts without subjecting themselves to behavioral profiling. Our buying patterns and preferences, our assets and liabilities, earnings history and net worth, our accidents and losses, are among our most personal information. This information describes who we are as individuals. Many Americans would not expect such information to be recorded, consolidated, and used to make decisions about them without their knowledge and consent.*

**Question 7:** In the July 20, 1999, hearing, some of the witnesses discussed allowing sharing for related purposes. What do you think of this idea? Is it workable? What might be a good definition of related purposes?

**Answer:** *If firms provide notice and choice, H.R. 10 does permit sharing for related purposes. We think this is the appropriate balance.*

**Question 8:** You state in your written testimony (page 5) that: Eventually, we may wish to look beyond financial privacy. Why wait? Does this waiting constrain our financial services sector?

**Answer:** *Americans have especially high expectations for the privacy and confidentiality of their personal financial information. Given the rapid developments in technology, consolidation and electronic payments, it is important to act now to protect this particularly sensitive information. We have an opportunity through H.R. 10 to establish privacy protections that would be applied broadly across all providers of financial services.*

*To ensure that any privacy protection regime is workable, it needs to balance the consumer's need for privacy with the need to maintain efficient banking and payments systems. The House bill does this through a series of exceptions to notice and choice.*

**Question 9:** Do you think an annual disclosure of privacy policies is too costly? Why or why not?

**Answer:** *Disclosure of an institution's information practices is a precondition for informed consumer choice. The Administration believes that a meaningful notice should be provided before a customer opens an account and that annual disclosure of privacy policies is reasonable.*

**Question 10:** Should we specifically prohibit the affiliating of financial holding companies with telemarketers?

**Answer:** *The Administration believes protection of personal financial information is important to Americans, and is focusing on financial privacy issues generally, not telemarketing. That is why we believe that customers should be able to exercise choice about whether confidential financial information is shared among affiliates as well as unaffiliated firms.*

**Questions 11:** If the Conference were to strike Title III, the medical privacy provisions, as some have suggested, why wouldn't that leave an opening for privacy violations between insurance and other affiliates? The deadline for HHS to issue rules is February 2000, right? Do you anticipate that will be on time? Could it be delayed by obstructionists?

**Answer:** *As the President announced in early September, the Administration believes that Congress should enact comprehensive legislation protecting the privacy of medical records this year. In the event that Congress does not act, HHS is prepared to issue regulations this Fall.*

**Question 12:** How are the comprehensive medical privacy plans of other Committees in Congress or the rules being contemplated by the Department of HHS planning to deal with the affiliations of banks and life insurance or property and casualty insurance or other insurance firms (that are not health insurance firms), as provided for under H.R. 10? Will the regulations as directed under HIPAA be as direct and as strong as necessary to preserve individual medical privacy?

**Answer:** *As the President announced in early September, the Administration believes that Congress should enact comprehensive legislation protecting the privacy of medical records this year. Such legislation would be more comprehensive than the regulations being prepared under HIPAA authority.*

**Question 13:** Should we consider a straight prohibition of medical information sharing under H.R. 10's structure, until the HHS rules are in force?

**Answer:** *As noted above, the Administration believes that Congress should address medical privacy issues on a comprehensive basis, through stand-alone legislation.*

**Question 14:** Some medical information needs to be shared for treatment, payment, and core business functions. What data is actually used to process these activities?

**Answer:** *The types of personally identifiable information, or data, that may be necessary to carry out treatment, payment and core business functions will vary depending on the specific purpose for which the information is being collected. For example, in order to have an insurer pay a claim, it will need the patient's name, plan ID number, date, diagnosis, and treatment (which may include tests conducted, and the results of those tests). To develop a course of treatment, a physician will need to know the plan limits, detailed information about the patient's current health status and medical history. Any or all information from the patient's medical record(s) and their administrative or billing records may also be needed.*

**Question 15:** What kind of notice and authorization is "okay" and what kind provides an opportunity to unduly pressure consumers to release information they do not [want] released?

**Answer:** *Notices regarding financial information should be meaningful. In general, they should be clear and conspicuous, periodic as noted in Question 9, sufficient to inform the customers of the uses that will be made of their information and to whom it will be transferred, and provide consumers the choice to opt out of the use of their data by both third parties and affiliates.*

**Question 16:** Are there instances where authorization shouldn't be required for research activities?

**Answer:** *"Research" is not defined in H.R. 10. Without an understanding of the type of research involved, it is not possible to determine whether it may be appropriate to permit the transfer of any medical information without patient consent.*

*As the President announced in early September, the Administration believes that Congress should enact comprehensive legislation protecting the privacy of medical records this year. This is the place to address the appropriate authorizations for medical research.*

**Question 17:** Do you think we should amend the FCRA to include transaction and experience data?

**Answer:** *We believe that the privacy of transaction and experience information should be protected. H.R. 10 does this in a free-standing statute which we think is a sufficient approach.*

**Question 18:** Do you agree that control of the portrait painted by a person's financial information belongs to the consumer, not the financial institution that process[es] the transactions?

**Answer:** *I think that consumers should have control over how their financial information is used. Americans want the ability to earn, invest, and spend their money without having to expose their lives to those who process their transactions. Just as they would not expect a letter carrier to read their mail or record their correspondents, they do not expect a bank processing a check to record, store, and evaluate their personal behavior.*

Statement of  
Edward M. Gramlich  
Member  
Board of Governors of the Federal Reserve System  
before the  
Subcommittee on Financial Institutions and Consumer Credit  
of the Committee on Banking and Financial Services  
U.S. House of Representatives  
July 21, 1999

Thank you, Madame Chairwoman. You and the Subcommittee are to be commended for efforts to resolve the issue of customer financial privacy. This is a vitally important issue in our increasingly information-dependent economy.

Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy. The more information about needs and preferences that is available, the more accurately and efficiently will the economy meet these needs and preferences. But though the availability of information promotes economic efficiency, there is also a long-recognized value in permitting individuals to maintain a zone of privacy. This value must be weighed against the benefits of economic efficiency that accrue from a broad dissemination of information.

To date, this issue has been largely handled in the marketplace, where the competitive value to companies of the use of customer information has been traded off against the competitive value of providing customer privacy, but there could be a public dimension as well. The growth of information-sharing technology has raised some important public policy issues that must be dealt with by the Congress.

The collision between economic interests in the value of customer information and individual privacy interests is an inevitable consequence of the growth in information technology. As information technology increases the flexibility of production processes to meet changes in product demands, the value of information about existing and probable demands also increases. Increases in productivity will contribute most efficiently to increases in standards of living when that productivity is focused on the goods and services consumers desire most. In order to identify existing customers' preferences, as well as potential customers and their preferences, firms will seek information about the tastes of their own customers.



The current debate over the privacy of customer financial information concerns information that banking and other financial institutions derive from their relationships with their customers. This information may include information submitted by a customer to a bank in order to obtain a loan or deposit service; information concerning transactions between a customer and a bank, such as individual deposits, check payments or payments on loans; as well as information obtained by the bank from third parties, such as information from a credit report. The economic value of this customer financial information to the bank is unquestionable. It is necessary to the conduct of transactions and also helps the bank evaluate the credit risk of its customers. This information also has value to others who may wish to sell goods or services to the bank's customers, and therefore has value to the bank as a marketable asset.

In the area of financial information, however, it is clear that many consumers believe that an implicit contract exists between the financial institution and the customer that requires the financial institution to keep certain transactional information confidential. Control of information about ourselves is one of the fundamental means by which we, as individuals, manage our relationships with each other. The feeling that financial information should be private has deep historic roots, and bankers and bank customers have long viewed their business relationship as involving a high degree of trust. The maintenance of this trust is essential to ensuring the confidence in our financial institutions that is so essential to their operations.

As market processes evolve, there is evidence that consumers have come to value both economic efficiency and privacy. On one side, individual consumers often overcome their reluctance to share particular items of information with third parties if they benefit from the sharing of that information. Many consumers participate in programs that assist retailers in

collecting detailed information about their own purchases in exchange for modest price discounts. Similarly, the sharing of credit histories for certain purposes is so widely accepted that sometimes creditors have been criticized by customers for failing to share information that would help these customers improve their credit histories.

At the same time, proposals or programs for using information about individuals have been abruptly dropped because of public responses. In Washington, D.C., two sellers of prescription medications stopped sharing prescription data with a third party. Several states backed away from programs of sharing driver's license photographs with a private company. Federal banking regulators dropped a proposal to require banks to establish "Know Your Customer" programs. In each of these cases, the strength of individual privacy preferences was underestimated, and public reaction forced a response more consistent with these preferences.

It is also possible that the increased ease of collecting and sharing information is allowing the practices of information users to evolve more rapidly than individuals' ability to respond. Given the rapid evolution of current market practice and the paucity of public information about these practices, the ability of individual bank customers to influence these developments through their market choices may not be adequate.

Already our judicial system is reaching for the appropriate balance between the economic value of customer financial information and the customer's privacy interest. The judicial system has long recognized the value of customer information: the courts have considered customer lists to be intellectual property protectable as trade secrets for most of this century. This suggests that customer account information may also be considered to be the intellectual property of the bank. In a related context, the Supreme Court has flatly characterized documents relating to a

customer's account as "the business records of banks" to which the customer "can assert neither ownership nor possession." Although ownership of property, including intellectual property, ordinarily includes the power to use or transfer the property, a number of state courts have limited banks' ownership rights in customer information, recognizing the value of the privacy of financial transactions to individuals. Despite the fact that most banking relationships are based on a debtor-creditor relationship, which entails considerably less responsibility for the counterparty's interests than a fiduciary relationship, these courts have found an implied contractual duty on the part of banks to maintain the confidentiality of customer information.

This environment presents the Congress with a series of important questions. Are banking practices involving customer information developing so quickly that customers will be unable to respond to those practices effectively? If so, can market processes be made more efficient without materially lessening privacy protections? If not, must the Congress itself strike the appropriate balance between these competing interests?

The Congress has already deemed it necessary to address specifically the uses of consumer financial information in the Fair Credit Reporting Act (FCRA). This Act governs the exchange of customer data by and with consumer reporting agencies. In connection with the enactment and amendment of the FCRA, the Congress grappled with some of the issues related to sharing customer information between affiliates. After significant debate, the Congress balanced the issues of consumer privacy and economic efficiency by allowing institutions to share information related solely to the institution's transactions or experiences with the customer, but to require that each customer be provided with the right to opt-out of sharing between affiliates of any other type of customer information. In addition, the Electronic Fund Transfer

Act requires a financial institution holding certain accounts to inform consumers of the circumstances under which information will be made available to affiliates and third parties. Similarly, several states have construed constitutional provisions or enacted general or industry-specific statutes to establish financial privacy rights.

Moreover, the Congress has given the banking agencies powers that may be exercised to address abuses in this area. These include the banking agencies' general enforcement powers over unsafe and unsound practices under the Federal Deposit Insurance Act and the Federal Reserve's ability to adopt rules addressing unfair or deceptive acts or practices under the Federal Trade Commission Improvement Act. Although we believe that information sharing between banks and third parties is fairly common, to date we have received relatively few complaints and have not found the need to institute any enforcement actions on privacy grounds.

The Congress is now considering whether to place additional limitations on banks and other financial institutions' disclosures of customer information, as would be done by the privacy provisions of H.R. 10. By adding these additional limitations--such as providing customers the right to "opt out" and thereby limiting the sharing of the institution's own experiences and other transactional information with third parties--it would be placing an increased value on privacy protections for bank customers. In making this decision, it is important that the tradeoff between economic efficiency and privacy be addressed with the fullest possible understanding of the competing interests. In particular, there should be recognition of the importance of consistency across markets--to ensure that any limitations imposed on one industry, such as financial services, do not place that industry at a competitive disadvantage.

If the Congress were to enact the privacy provisions of Sections 501 through 510 of H.R. 10 as drafted, we believe that the exceptions would permit routine payment transactions and supervisory activities to continue. However, the Committee may wish to consult others as to the efficacy of other exceptions to the disclosure limitations. There may be some room to clarify the drafting, and we would be happy to offer suggestions to that end. In addition, the time period for adopting or implementing regulations is ambitious. Thought might be given to extending the implementation period to at least a year.

Finally, your letter of invitation raised issues with respect to the Board's own privacy policy and to our experience with the Right to Financial Privacy Act and the Privacy Act. Significantly, these questions relate to governmental, as opposed to private, access to data about individuals. The Board's privacy policy statement was adopted in June and can be accessed from the Board's "home page" and several other locations on the Board's web site ([www.federalreserve.gov](http://www.federalreserve.gov)). At its web site, the Board collects information concerning the frequency and volume of visits to the site. It does not collect information that identifies individuals, nor does it use "cookies" (i.e. entries placed in the individual's computer to allow monitoring of the individual's use of a web site). The Board does not see an obvious need for revision of the Right to Financial Privacy Act at this time, though there is a need for its continued review. We would want to make a more thorough study of the issue before recommending any specific changes.

Governor Gramlich subsequently submitted the following in response to written questions received from Congressman Vento following the July 21, 1999, hearing:

**1. How has the FRB exercised its interpretative authority under the Fair Credit Reporting Act?**

Our staff regularly provides informal, oral interpretations in response to public inquiries. We are also in the final stages of preparing formal, written interpretations that address significant issues raised by the FCRA amendments that took effect in September 1997. These issues include, for example, the content and timing of the "opt-out notice." This is the notice that an institution must provide to a consumer (unless the institution wishes to incur the obligations of a consumer reporting agency) before sharing certain types of information about the consumer with the institution's affiliates.

We have consulted about our interpretations with the FDIC, NCUA, OCC, and OTS, as the FCRA requires. We have also coordinated with the FTC in order to promote consistency in the guidance applicable to depository and non-depository institutions.

We expect to issue our interpretations for public comment in the next month or two. The FTC will issue identical interpretations at the same time.

**2. Do you think an annual disclosure of privacy policies is too costly? Why or why not?**

The costs that an annual disclosure requirement for privacy policies would impose on financial institutions is difficult to estimate with any precision. In part, this is because some institutions may already make, or contemplate making, such disclosures for their own purposes. Consequently, the regulatory requirement would not impose significant additional costs on these institutions. Nevertheless, the disclosure requirement would be likely to impose additional costs on a significant number of financial institutions, costs that would not be imposed on non-financial institutions that may also share customer information for marketing purposes.

**3. Does H.R. 10 as passed by the House, or a future limitation on sharing information among affiliates, constrict competitiveness of financial industries vis a vis other non-covered industries? How do we look for more universality or a level playing field on this issue?**

In my testimony, I noted the importance of consistency in privacy requirements across markets to ensure that limitations on one industry, such as financial services, do not place that industry at a competitive disadvantage. As drafted, H.R. 10 would impose costs on financial institutions, not only through the requirement to disclose their privacy policies,

but also by denying them the economic value of sharing information with unaffiliated third parties for marketing purposes. If financial institutions choose to share information for these purposes, H.R. 10 would require financial institutions to keep track of those customers who have "opted out" of having information about them shared, thereby incurring additional costs. These costs are not imposed by H.R. 10 on retail sellers or other non-financial institutions. In addition to the competitive issue, addressing privacy issues on an industry-by-industry basis leaves gaps in the privacy protections for individuals.

With respect to extending the limitations on H.R. 10 to sharing with affiliates, H.R. 10 reflects a judgment that relationships among affiliated financial companies foster greater efficiency than relationships between unaffiliated companies. Thus, extending the limitations on sharing customer information to sharing with affiliates may impose costs that could be disproportionately higher than the costs due to the limitations on sharing with unaffiliated third parties.

In order to attain a greater universality or a level playing field on this issue, it would be necessary to establish standards that applied to all collection and sharing of similar information.

- 4. Please discuss EFTA's privacy protection (disclosure of circumstances where institutions will disclose consumer information to third parties) and your understanding of compliance, enforcement, and consumer satisfaction with this law and regulation.**

The Board's Regulation E, which implements the EFTA, requires a financial institution to disclose its information-sharing policy. This disclosure is part of the initial disclosures given to consumers when they open an account to or from which electronic fund transfers (EFTs) may be made. An institution must describe the circumstances under which any information about the account--not just information about EFTs--will be disclosed to third parties. The commentary to the regulation states that the term "third parties" specifically includes affiliates.

We routinely examine state member banks for compliance with the disclosure requirements of Regulation E. We also closely monitor consumer complaints in this area; to date, we have not received any complaints or inquiries about this disclosure.

- 5. How do you envision the role of the regulator in enforcing the privacy provisions of H.R. 10 once enacted into law?**

We would expect to play several roles: developing regulations, and possibly interpretations of those regulations; conducting regular compliance examinations of state member banks; and undertaking enforcement action when appropriate. Thus, our activities

under sections 502-505 and 509-510 would generally resemble what we do under the other consumer-protection laws we administer. (In accordance with section 505(b), our activities under section 501(b) would generally resemble those under section 39 of the Federal Deposit Insurance Act.)

There would be some differences, however, including:

- Broader scope of issues for regulatory resolution. The consumer-protection laws we administer generally do not leave open for regulatory resolution basic issues of coordination with other statutes. Sections 502-505 and 509-510, however, do leave such issues open—for example, how these sections relate to the FCRA and to state consumer-privacy laws. We would have to resolve these issues by regulation in the event those sections are enacted in their present form.
- Joint rulemaking. The federal banking agencies sometimes issue regulations on a joint basis as contemplated in H.R. 10, but in the consumer-protection context it is more typical for the Congress to direct the Board alone to issue regulations. Joint rule-making could slow down materially responses to market-driven changes in industry practice, to changes in technology, and to changing consumer concerns.





BOARD OF GOVERNORS  
OF THE  
FEDERAL RESERVE SYSTEM  
WASHINGTON, D. C. 20551

August 9, 1999

EDWARD M. GRAMLICH  
MEMBER OF THE BOARD

The Honorable Marge Roukema  
Chairwoman  
Subcommittee on Financial Institutions  
and Consumer Credit  
Committee on Banking and Financial Services  
House of Representatives  
Washington, D.C. 20515

Dear Madam Chairwoman:

Thank you for your letter of July 29, 1999, concerning my July 21, 1999, testimony before your Subcommittee on the issue of privacy in the financial services industry. In your letter, you asked whether I had specific concerns about legislation that would provide an opt-out of: (1) information sharing with affiliates for the purpose of marketing or (2) information sharing with affiliates for any purpose?

As I noted in my testimony, the value of permitting individuals to maintain a zone of privacy must be weighed against the benefits of economic efficiency that accrue from a broad dissemination of information. Some have argued that consumers will perceive no difference between sharing of information with third parties and sharing information with affiliates. While it is difficult to evaluate consumer perceptions without meaningful data, it is clear that H. R. 10 reflects a judgment that relationships among affiliated financial companies foster greater economic efficiency than relationships between unaffiliated companies. Clearly judgments as to the economic efficiency that would flow from affiliations would affect the balance between economic efficiency and privacy.

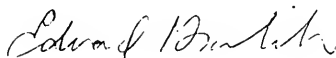
In this context, the sharing of information with affiliates is likely to differ from the sharing of information with third parties in the following respects:

- the benefits to both the service providers and their customers of cross marketing of related financial services are likely to be greater than in cross marketing involving unaffiliated companies;
- the efficiencies in the delivery of related financial services by affiliated companies, such as combined statements, or single contact point customer service, are likely to be greater than in the case of unaffiliated companies;

- the benefits of consolidated risk management by affiliated companies, including credit risk and fraud prevention -- purposes that are important to the safety and soundness of insured depositories -- are likely to be greater than in the case of unaffiliated companies; and
- information shared among affiliates may be more readily controlled and protected than information shared with unaffiliated companies.

Thus, Congress could reasonably conclude that the same types of privacy protections that might be considered appropriate between unaffiliated companies are not appropriate between affiliated financial services companies. At a minimum, an extension of an opt-out to affiliate sharing should include a clear exception for credit risk management purposes and may warrant other exceptions to address the products or groups of products that are offered jointly by affiliates.

Sincerely,



TESTIMONY OF  
JOHN D. HAWKE, JR.  
COMPTROLLER OF THE CURRENCY  
before the  
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
of the  
COMMITTEE ON BANKING AND FINANCIAL SERVICES  
U.S. HOUSE OF REPRESENTATIVES  
July 21, 1999

Statement required by 12 U.S.C. 250:

The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

## Introduction

Madam Chairwoman, Congressman Vento, and Members of the Subcommittee, thank you for the opportunity to testify about an issue that has enormous ramifications for the banking industry and the customers they serve -- financial privacy. I commend you, Madam Chairwoman, for holding this timely hearing on an issue that is generating increasing public attention and concern.

Fundamental to the relationship between banks and their customers is the trust that customers place in their banks to uphold the confidentiality of that relationship. In fact, the banking industry has had a long history of safeguarding customer confidentiality. A 1961 court case aptly described this tradition stating, "It is inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors' accounts. Inviolable secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors."<sup>1</sup>

Today, however, this tradition is under pressure from technological advances and from the demands of a competitive marketplace that have placed a premium on the availability of personal information -- often at the expense of personal privacy. Resistance to this pressure is of enormous importance, for if banks fail to honor customer expectations that personal information will be kept private and confidential, they will impair the most priceless asset of their banking franchise -- their customers' trust. Thus, privacy is not just an important consumer issue; it is an issue with implications for the long term vitality and stability of the banking system.

Banking is an information-driven industry. Bankers have always relied on access to personal financial information to make fundamental judgments about consumers' qualifications for financial products and services. Information exchanges thus serve a useful and critical market function that benefits consumers and financial institutions alike, in facilitating credit, investment, insurance and other financial transactions.

Recent advances in technology that permit the efficient collection, storage, analysis and dissemination of vast stores of information, coupled with the changing structure of the financial services industry and the development of efficient new delivery systems, have increased the market value of customer information. Passage of financial modernization legislation will further change the financial services landscape, permitting diverse financial companies to affiliate and to pool their customers' personal information. While financial conglomerates may profit from the cross marketing opportunities occasioned by an expansion of powers and the "warehousing" and "mining" of personal data, and while consumers may benefit from the availability of a broader array of custom-tailored products and services, there is a serious risk that these developments may come at a price to individual privacy.

---

<sup>1</sup>Peterson v. Idaho First National Bank, 367 P.2d 284,290 (Idaho 1961).

Until very recently, consumers knew little about the information-sharing practices of the companies that they patronized. As these practices become more widely known, however, the public appears ready to react against real or perceived abuses in the treatment of their personal information. When that information relates to financial or medical circumstances, customers are even less tolerant of perceived violations of privacy. Bank customers in particular, expect their banks to protect the confidentiality of their transactions.

A review of existing privacy laws and banking practices reveals that more can be done to assure the public about the responsible uses of financial information. H.R. 10, as passed by the House, adopts a measured approach that provides consumers with notice and choice about the information-sharing practices of financial institutions, without impeding the flow of information essential to doing business. This common sense approach is a positive step in assuring consumers that their information will be handled appropriately and in providing consumers with increased control over their personal information. Customers are likely to expect more, however, and the challenge is how best to meet their reasonable expectations of privacy without defeating the potential benefits available from advances in technology and the new corporate affiliations that would be made possible by H.R. 10.

My testimony today will expand upon these concepts and address the questions posed by the Chairwoman's letter of invitation.

#### **Privacy Laws**

The letter of invitation asked about existing laws and regulations that protect financial privacy. Although the United States does not have a comprehensive, universal privacy law, there are a number of legal provisions that help to ensure that consumer financial information will be treated as confidential.

On the federal level, the most significant of these laws is the Fair Credit Reporting Act ("FCRA"), which prohibits "consumer reporting agencies" from sharing information about consumers with third parties unless the third party has a "permissible purpose." The Act enumerates with some precision just what these permissible purposes are: they include using customer information (1) in connection with a credit transaction or insurance underwriting involving the consumer, (2) in other situations in which the third party has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer, (3) for employment purposes, such as hiring, (4) in connection with "prescreened" transactions involving a "firm offer of credit or insurance," assuming the consumer has not elected to be excluded from such offers, and (5) where the consumer has

given written permission for the information to be shared.

These restrictions sharply curtail the circumstances in which the major credit bureaus and other central repositories can share the consumer financial information in their databases. They cannot, to note one important example, generally give out confidential information to telemarketing companies prospecting for sales.

Perhaps just as important as these limits on credit bureaus, from the standpoint of consumer financial privacy, are the limits that FCRA places on other business entities, such as banks, securities firms, and insurance companies. Roughly speaking, FCRA defines "consumer reporting agency" as any person or entity that furnishes "consumer reports."<sup>2</sup> Consumer reporting agencies are subject to a number of significant requirements under the Act -- including the information-sharing restrictions described above and related procedural requirements, accuracy standards, consumer access requirements, and dispute resolution procedures.

As a practical matter, unless they wish to become consumer reporting agencies subject to the requirements described above, banks and other financial firms may only share information that is not "consumer report" information, such as (1) information that relates solely to the institution's own transactions or experiences with the consumer, and (2) any other information shared with affiliates, provided that the consumer is first given notice of the proposed affiliate information-sharing and an opportunity to "opt out" -- that is, to object to the sharing of individual information.

Thus, FCRA does *not* provide consumers with the ability to object to or prevent the sharing of so-called "transaction and experience information," which includes a wide range of sensitive information about individuals -- not only loan repayment patterns, but also, for example, information from an insurance affiliate about one's medical insurance claim history. Moreover, this information may be shared with affiliates or with unrelated third parties, regardless of their intended use of the information. In this light, it is not at all surprising that much of the current debate about financial privacy revolves around these provisions relating to "transaction and experience information."

---

<sup>2</sup>The term "consumer report" means any communication of information by a consumer reporting agency that bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or collected for a permissible purpose under FCRA.

Other federal laws concerning financial privacy are much more limited in scope, involving either disclosure of information-sharing practices or governmental access to information. In particular, the Electronic Fund Transfer Act and its implementing regulation, the Federal Reserve Board's Regulation E, require financial institutions to provide deposit account customers a general disclosure about when, in the ordinary course of business, the institution will share information about the consumer's account with affiliates or other third parties. These provisions require only disclosures, however, and do not impose any substantive limits on the actual sharing of information or enable consumers to opt out of such sharing.

The letter of invitation also inquired specifically about the Privacy Act of 1974 ("Privacy Act") and the Right to Financial Privacy Act ("RFPA"). These laws provide controls over the federal government's collection, use, and disclosure of consumer financial information. Among other requirements, the Privacy Act permits a federal agency to maintain in its records "only such information about an individual as is relevant and necessary" to accomplish a required agency purpose, and, with certain exceptions, prohibits the agency from sharing that information with another agency or person without the consent of the individual in question. Thus, unless an exception applies, the federal government may share this information only if the individual "opts in."

In May 1998, the President issued an executive order directing all federal agencies to review their records and information systems to ensure compliance with the Privacy Act. The OCC promptly took appropriate actions to fulfill this mandate, including an inquiry to all employees to identify new or modified systems of records that might be covered by the Act. We will ensure both that new and existing records systems are fully compliant with the Privacy Act.

RFPA deals specifically with federal government access to customer financial records at a financial institution. RFPA limits such access -- as well as any further sharing of the information within the federal government -- to specifically enumerated situations. As is the case with the Privacy Act, these exceptions generally represent a careful balancing of privacy interests with important bank supervisory, law enforcement, and other governmental functions. In response to your question, Madam Chairwoman, although I have no evidence that these laws are not effectively accomplishing their limited purposes, they deal with potential privacy intrusions by the federal government, and do not cover the private sector or even state governmental units.

State laws also provide some measure of protection for consumer financial information.

As an initial matter, many states have enacted counterparts to the FCRA and EFTA, the primary federal laws discussed above relating to private sector financial privacy. The federal laws in question generally provide that state laws on the same subject matter will not be preempted unless inconsistent with the federal provisions -- and then only to the extent of the inconsistency. Thus, the state and federal laws often comfortably coexist. There are important exceptions to this principle, however, the most important of which may be that any state law regarding the sharing of information with affiliates -- whether "transaction and experience information" or other information -- is specifically preempted by the FCRA until 2004. Thus, state law cannot provide *greater* protections for consumers than the FCRA in this regard.

In discussing state law, it also should be noted that common law principles -- particularly a fiduciary duty of confidentiality owed by banks to their customers -- may provide additional protections. As with state statutory law, however, these judicially recognized protections vary widely by jurisdiction, and do not provide equal protections to all U.S. consumers.

The letter also specifically asked about the OCC's regulatory authority with respect to financial privacy. While we cannot promulgate regulations or issue authoritative interpretations for any of the laws discussed above, the OCC, like the other federal banking agencies, has the authority to remedy violations of any federal or state law or regulation with respect to the entities we supervise. This authority is granted in section 8 of the Federal Deposit Insurance Act, and includes both the authority to order that the bank cease and desist from violating any such law or regulation and, in certain circumstances, to order reimbursement for harms.

I must note, however, that with respect to the FCRA -- perhaps the most important federal law relating to financial privacy -- our enforcement authority has been severely hampered by 1996 amendments that curtailed our ability to examine national banks for compliance with the Act. In particular, we may examine a bank only in response to a complaint or if we "otherwise have knowledge" of a violation. No other consumer protection statute we enforce similarly limits our ability to examine banks for compliance.

### **OCC Privacy Initiatives and Bank Practices**

Over the past year, the OCC has issued three advisory letters to national banks focussing on different elements of privacy -- security of confidential customer information,



compliance with existing legal requirements for consumer notice and choice regarding information sharing, and measures to address customer concerns about national banks' privacy practices in the Internet environment. Attached to my testimony are copies of these advisory letters.

*Pretext Calling.* The first advisory letter, issued in August 1998, alerted banks to a deceptive practice that victimizes both the banks and their customers. The subject of that advisory was "pretext phone calling," a practice whereby account information brokers, posing as bank customers, gain improper access to confidential account information. In addition to warning banks about this practice, the advisory letter encourages them to establish clear guidelines, procedures, and internal controls to reduce the chances of unwitting and unauthorized disclosures of customer information by bank employees.

The OCC was initially alerted to pretext calling through its participation in an interagency bank fraud working group. In response, the OCC jointly prepared the advisory with the other banking and law enforcement agencies in the working group. Additionally, the OCC has previously testified before this Committee in support of legislation aimed at curbing pretext calling. We generally support those provisions in H.R. 10, although we do have concerns about the enforcement authority.

*FCRA Affiliate Information Sharing.* The second advisory letter issued in March 1999 addressed banks' obligations under the FCRA to notify customers about affiliate information sharing and to provide customers with an opportunity to opt out of that sharing. The advisory letter discusses the most effective practices for meeting these requirements that the OCC observed among national banks. In doing so, the advisory features examples of notices that make bank information handling practices more readily understandable and transparent to customers and procedures that provide convenient opt-out mechanisms.

This advisory was the product of the OCC's Privacy Working Group, an interdisciplinary team that includes senior level OCC officials, which was established to inform the Comptroller about financial privacy issues and to coordinate agency policy and initiatives. In assessing general industry privacy practices, working group members discovered that some bank FCRA affiliate sharing notices were often buried in fine print in multipage agreements and provided customers with little useful information about the bank's information sharing practices. Other notices, however, were clear, simple, and precise and provided information sufficient to allow bank customers to make informed choices about the sharing of their information. It is those notices we highlight in the guidance.

*Internet Privacy Policies.* Our third advisory, issued in May 1999, informed banks about effective practices for developing privacy policies, in general, and prominently posting those policies on bank Web sites. The advisory letter provides examples of the various mechanisms banks have employed to make their privacy policies easy to spot and easy to understand by Web site visitors. Additionally, the advisory discusses effective procedures used by large and small banks to establish privacy policies, encourage employee understanding of and compliance with stated policies, and address privacy-related inquiries and complaints from customers.

The OCC issued this guidance in response to a comprehensive survey conducted by the FTC last year that found a general failure of Web sites, including those operated by financial institutions, to post any disclosures about their information handling practices. The OCC believes it is especially important for banks to reassure customers about the safeguarding of their personal information when information is communicated in an online environment. The advisory is intended to sensitize banks to some of the challenges posed by the Internet to consumer privacy and to give constructive examples for meeting these challenges.

### **OCC Privacy Policy**

The OCC takes privacy issues seriously in its own operations. Last year we adopted a comprehensive new privacy policy, which was posted on our Web site in October 1998. The OCC's privacy policy is conspicuously listed on the opening page of our Web site.

Pursuant to our privacy policy, we do not collect or store information about members of the public who call or write the agency or visit our Web site, unless they identify themselves and ask for a response to an inquiry or request. We do, however, collect and store certain non-personal information about visitors to our Internet site when they log on to read or download information, such as OCC bulletins, alerts or press releases, and this is disclosed in our privacy policy. We use this information simply to help us stay abreast of technical upgrades that can make our site more accessible to visitors, and to record the date and time of all visits to our site.<sup>3</sup> We do not attach "cookies" to the browsers of our visitors.

---

<sup>3</sup>Specifically, we record: The name of the domain from which a visitor accesses the Internet (for example, aol.com or princeton.edu); the Internet address of the Web site from which the visitor linked directly to our site, if any (for example, www.fdic.gov, if the visitor linked to the OCC from the FDIC Web site, or www.yahoo.com, if the OCC Web site was located using the Yahoo search

If visitors identify themselves when they contact us, appropriate agency employees may see this information. We adhere to the following principles in handling information provided by members of the general public:

- We use personally identifying information only for the purpose for which it is originally collected.
- We maintain personally identifying information in secure computer systems and we limit employee access to those with a business reason to see it.
- We do not disclose personally identifying information to anyone outside the OCC, except where compelled by law or in connection with a criminal investigation.

### Public Policy Responses

Maintaining the public's confidence in the banking system has long been a critically important national policy objective. In furtherance of that objective, we have a program of federal deposit insurance and a comprehensive system of bank licensing, supervision, and regulation. Another critical factor in upholding public confidence in the banking system has been the assurance that banks will honor customers' expectations that information provided or maintained in connection with their financial transactions will be kept in confidence. Traditionally, national banks have earned the public's trust in this regard by honoring those expectations.

However, developments in the marketplace are affecting the public's concerns about privacy in ways that were not contemplated until fairly recently. Indeed, these concerns have evolved since the enactment of the laws dealing with the collection and use of financial information that I previously mentioned. These developments, and the consequent evolution of public concerns, explain why we are engaged in this public policy debate on privacy.

One reason for the increased public concern about privacy is the explosion of information technology. Today, personal information about individuals can be accessed, reviewed, combined, rearranged, and transferred with just a few key strokes. Information about a person's financial or medical condition, buying habits, and other characteristics -- down to the most personal level -- can be used to create profiles for marketing or for developing new products. As a result of changes in technology, information is an increasingly valuable commodity.

---

engine); the type of Web browsing software used to view our site; and the date and time the visitor accessed our site.

Financial institutions have generally safeguarded customer information -- not only to preserve the trust and goodwill of their customers -- but also to protect what the institutions consider to be proprietary information. However, it is now possible to create huge databases that can be easily shared among affiliates due to improvements in technology. And with the development of speedy electronic marketing and delivery systems, institutions are using customer information for purposes other than those for which it was originally provided or maintained. Centralized customer databases within new financial conglomerates offer the promise of increased business opportunities, lower costs, and improved financial products and services for consumers. Information technology now enables combined financial services companies to offer one-stop shopping to customers and to adapt products to their customers' changing financial needs over the course of a lifetime.

At the same time, however, the commoditization of information, and the pace and magnitude of mergers and affiliations in the financial services industry -- which will be accelerated with financial modernization legislation -- have sharpened privacy concerns. Obviously, affiliations among diverse sectors of the financial services industry offer tremendous opportunities for these companies to operate in complementary ways, achieve efficiencies, and expand through cross-marketing of products to customers. However, these new combinations also fuel both the perception and reality that individuals are losing control over their personal information. When the information is highly sensitive, such as medical and financial information, consumer concern over who has control over its disposition is magnified.

The banking industry has recognized the need to respond to consumer privacy concerns. Banking trade groups are to be commended for developing a common set of privacy principles that explicitly recognize a customer's expectation of privacy, and it appears that an increasing number of banks are adopting this model. Financial institutions clearly have the capacity to react swiftly to concerns about abusive practices, as we have seen recently when several major banks discontinued their practice of selling customer account information to third-party telemarketers. I applaud these banks for their prompt responses when this privacy issue became known.

Let me now turn to the current legislation. The privacy provisions in H.R. 10 embody the important elements of notice and choice -- a concept already contained in the Fair Credit Reporting Act, and one with which financial institutions are very familiar. When administered properly, notice and choice enable consumers to make informed decisions about the disposition of their personal information and maintain control over their information. We have learned through our research as part of the Consumer Electronic Payments Task Force,

and survey data bear this out, that consumers have different levels of sensitivity to privacy. Notice and choice allow those consumers who place a premium on privacy to protect that privacy at the expense of forgoing certain marketing opportunities or even beneficial treatment from their financial institutions in the form of cost savings. On the other hand, consumers without the same desire for privacy, may choose to relax confidentiality in exchange for the benefits that they perceive will result from information sharing. The bottom line is that it is the consumer's choice to give up or retain personal privacy -- not the institution's.

The privacy provisions in H.R. 10 will enhance the notice and choice requirements already existent under FCRA. The existing law limits the sharing of certain information among affiliated companies unless consumers are provided with notice about the sharing and an opportunity to opt out of that sharing. However, as I noted above, the banking agencies are presently hamstrung in their ability to enforce these provisions. H.R. 10 will restore the agencies' examination authority.

Additionally, and equally significant, H.R. 10 will give the banking agencies the authority to implement FCRA by regulation. As previously mentioned, the OCC has seen a number of affiliate sharing opt out notices that are virtually invisible to the consumer and meaningless in their content. Regulatory authority should allow the banking agencies to prescribe meaningful and uniform standards for these notices. Also, since we published the advisory about affiliate information sharing requirements in May, we have received a number of inquiries from banks and their attorneys about the meaning of various ambiguous provisions of the FCRA. The rulemaking authority in H.R. 10 will enable the agencies to deal with the complex -- and evolving -- nature of the issues presented, pursuant to a public notice and comment process, that will permit adjustments to be made, if and when changing circumstances warrant.

The scope of personal information that H.R. 10 protects against disclosure will address a major exception in current law -- transaction and experience information. Under FCRA, companies can freely share the confidential information that they derive from their relationship with their customers, including account type and balances, payment history, credit limits, and amount and date of last payment. In the recent matter involving a bank's transfer to telemarketers of confidential customer information, including credit card and checking account numbers, much of the personal information shared was transaction and experience information. H.R. 10 would expressly prohibit the sharing of account numbers and would require notice and consumer choice with respect to the sharing of the personal information implicated in this case.

In my view, however, a serious question can be raised whether H.R. 10 goes far enough in protecting customer confidence in the confidentiality of their relationships with their bank, and it draws a distinction between information sharing with affiliates and nonaffiliates that may not be relevant for customers. In his May 4th proposal regarding privacy, the President indicated his support for legislation that would give consumers control over the use and sharing of all their financial information, both among affiliates and nonaffiliated third parties. H.R. 10 is a good first step in meeting that goal, but I believe that customers will reasonably expect more. Is it realistic to think that customers will distinguish between situations when their confidential information is transferred to affiliates vs. nonaffiliates of their bank? Would customers believe that the legislation adequately covers their reasonable expectations regarding the use and transfer of their confidential information? If the answers to these questions are in the negative, the failure to provide protection for the sharing of information with affiliates could have a profound effect -- particularly in a world of expanded financial conglomeration -- on the willingness of customers to maintain the kinds of relationships with the banking system they have in the past. While the desire of bankers to take advantage of new cross-marketing opportunities is entirely understandable, I believe that a primary objective of policy makers should be to assure that doing so does not cause fundamental damage the banking system.

### Conclusion

I again thank the Chairwoman and other members of the subcommittee for this opportunity to testify on this important issue. I cannot overstate the importance of addressing consumer expectations about the confidential treatment of financial information to maintaining the public's confidence in the banking system. And I urge that, in crafting an appropriate response to consumer privacy concerns, banks and Congress put themselves in the shoes of a customer and ask, "Will my financial institution use my personal information in a manner consistent with my expectations?" and "Will I have any control over the use of my information?" Whatever legislative formulation ultimately results, American consumers deserve to be able to answer "Yes" to those questions.



# OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Fair Credit Reporting Act

---

**TO:** Chief Executive Officers and Compliance Officers of all National Banks,  
Department and Division Heads, and all Examining Personnel

## SUMMARY AND PURPOSE

Recent amendments to the Fair Credit Reporting Act ("FCRA") have enhanced the ability of various businesses, including banks, to exchange customer information among affiliated companies. At the same time, technological advances permit businesses to collect, store, analyze, and disseminate increasing amounts of customer data. Survey data indicate that consumers are sensitive to how businesses, including banks, maintain, use, and analyze information about them. These customer concerns about the accumulation and use of their personal information are likely to increase with the growing use of the Internet and electronic commerce.

The purpose of this advisory is to provide examples from a sampling of existing bank practices that represent effective approaches for complying with notice requirements under the FCRA regarding the sharing of customer information among affiliated companies. These examples are not examination standards and are not intended to be an exclusive description of the various ways in which banks can meet their existing legal obligations under the FCRA, nor do they impose any new obligations on banks. The examples are illustrative of approaches by some national banks that convey meaningful information to their customers about the treatment of personal data. Thus, national banks may find these examples helpful as they develop their own plans and programs to comply with the FCRA.

## CONTENTS

- Background
    - Fair Credit Reporting Act Amendments of 1996
    - Developments in the Marketplace
  - Effective Practices
    - Content of Affiliate Sharing Notice
- 

Date: March 29, 1999

What type of information is shared  
 With whom is the information shared  
 Purpose for the sharing  
 Presentation of Notice  
 Convenience of Customer Opt Out

## BACKGROUND

### Fair Credit Reporting Act Amendments of 1996

In 1996, Congress adopted amendments to the FCRA that, among other things, permit the efficient flow of customer information among affiliated companies.<sup>1</sup> The amendments expanded the opportunity for companies "related by common ownership or affiliated by corporate control" to share, without restriction, transaction and experience information — information that relates solely to an entity's own transactions or experiences with its customers.<sup>2</sup> This information could include, for example, a customer's outstanding balance, whether the customer is delinquent in paying bills,<sup>3</sup> and the length of time a customer has held a credit card.<sup>4</sup> The law accomplishes this by exempting transaction and experience information from the definition of a consumer report.<sup>5</sup> Further, the amendments exempt from the definition of a consumer report, the communication among affiliated companies of *other* information about a consumer (that is,

<sup>1</sup> The Economic Growth and Regulatory Paperwork Reduction Act of 1996 substantially amended the Fair Credit Reporting Act effective September 30, 1997.

<sup>2</sup> 15 U.S.C. § 1681a (d)(2)(A)(ii).

<sup>3</sup> See *DiGianni v. Stern's*, 26 F.3d 346, 348-49 (2nd Cir. 1994), *cert. denied*, 513 U.S. 897 (1994); *Smith v. First National Bank of Atlanta*, 837 F.2d 1575, 1578 (11th Cir. 1988), *cert. denied*, 488 U.S. 821 (1988); *Rush v. Macy's New York, Inc.*, 775 F.2d 1554, 1556-57 (11th Cir. 1985). See also FTC Official Staff Commentary §603(d) item 7A(1) and (3) (May 1990).

<sup>4</sup> FTC FCRA Staff Opinion: Kane-Novak (September 9, 1998).

<sup>5</sup> 15 U.S.C. § 1681a(d)(2)(A)(ii). Generally, a "consumer report" is any communication, by a "consumer reporting agency," of any information that bears on a consumer's credit-worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is collected or used (or expected to be collected or used) as a factor in establishing the consumer's eligibility for credit, insurance, employment, or any other purpose permissible under the Act. *Id.* 1681a(d)(1). Reports limited to the consumer's name and address, with no connotations to credit worthiness or other characteristics, do not constitute a "consumer report." FTC Official Staff Commentary at § 603(d) item 4F.

The law also permits the sharing of transaction and experience information with unaffiliated third parties by exempting such information from the definition of a consumer report. 15 U.S.C. § 1681a(d)(2)(A)(I).

Date: March 29, 1999



information in addition to transaction and experience information that would ordinarily be considered a consumer report), if certain conditions are met: (1) it is clearly and conspicuously disclosed to the consumer that information may be shared among affiliated companies; and, (2) the consumer is given the opportunity, prior to the time that the information is communicated, to direct that such information not be communicated among the entities.<sup>6</sup> This provision permits a bank to freely share customer information, such as consumer reports or information from a credit application, among affiliated companies if these conditions are satisfied.<sup>7</sup>

Failure to comply with these conditions for affiliate information sharing can result in liability (including, administrative enforcement and/or civil action) and can make a bank a consumer reporting agency under the FCRA. A consumer reporting agency is subject to various legal obligations to maintain and safeguard consumer information, including limitations on the purposes for which information can be sold or distributed.<sup>8</sup> Consumer reporting agencies are also required to provide consumers an opportunity to review information maintained about them, as well as to establish particular error resolution procedures and consumer complaint mechanisms.<sup>9</sup> Therefore, a bank that wishes to share customer information with its affiliates, that is not limited to transaction and experience information and that otherwise meets the definition of "consumer report," without the burden of complying with these requirements on consumer reporting agencies, must adhere to the FCRA opt-out conditions.

---

<sup>6</sup> 15 U.S.C. § 1681a(d)(2)(A)(iii).

<sup>7</sup> See Federal Reserve Regulatory Service, Questions and Answers about the Fair Credit Reporting Act, The Financial Institution as a Consumer Reporting Agency, FRRS 6-1605. See also FTC FCRA Staff Opinion: Kane-Novak, *supra*.

<sup>8</sup> 15 U.S.C. § 1681b.

<sup>9</sup> Consumer reporting agencies are required to provide consumers access to all information, except credit scores, maintained in the consumer's file upon request. 15 U.S.C. § 1681g(a)(1). In the event a consumer questions the accuracy or completeness of any information in the consumer's file, the reporting agency must conduct a reinvestigation. 15 U.S.C. § 1681i.

While banks may be subject to federal or state laws in other areas of consumer privacy,<sup>10</sup> those state laws that prohibit or limit the types of information affiliates may share are expressly preempted by FCRA until the year 2004.<sup>11</sup>

### Developments in the Marketplace

Technological innovations and industry consolidation are increasing the magnitude and scope of information sharing in the financial services sector. Improvements in data processing and communications technology now allow more efficient storage, analysis, and rapid dissemination of vast amounts of information. Mergers among companies with the same or diverse lines of business are resulting in companies with the ability to assemble and use large databases of customer information. These developments create new opportunities for banks to use information to custom design products and services to match their customers' needs and preferences. Bank customers benefit from the improved quality of tailor-made goods and services, as well as the increased speed of obtaining financial services. But, while these developments may increase the quantity and quality of many bank services, the expanded use of customer information has also heightened consumer concerns about confidentiality and personal privacy.

Banks have a particular stake in addressing the privacy concerns of customers. Maintaining customer trust that the relationship will remain confidential is an essential component of banking relationships, and banks continually rely on the willingness of customers to provide extensive confidential information. Survey evidence indicates that much of the public's suspicion and concern about the privacy issue generally derives from a lack of knowledge about how a business handles consumer information.<sup>12</sup> The affiliate information sharing notice mandated by the FCRA can provide a convenient vehicle for banks to educate their customers about their information practices, and gives customers an opportunity to control the flow of their information.<sup>13</sup>

---

<sup>10</sup> For example, the Electronic Funds Transfer Act and its implementing regulation, Regulation E, require a bank to provide its customers a description of the circumstances in the institution's "ordinary course of business" in which it will disclose information about the consumer's account to third parties. 15 U.S.C. § 1693c(a)(9); 12 C.F.R. 205.7(b)(9). This disclosure must address all information concerning the account that may be provided to third parties and whether it will be provided to affiliates. See FRB Official Staff Commentary 205.7(b)(9)-1.

<sup>11</sup> 15 U.S.C. § 1681t (b) and (d)(2). State laws that were preempted by the FCRA do not automatically return in force after the sunset date. Each state must enact new legislation. *Id.* § 1681t (d)(2).

<sup>12</sup> See Business Week/Harris Poll, "A Little Privacy, Please" Business Week, March 16, 1998.

<sup>13</sup> A recent survey of consumers indicated that 61 percent of the public believe that it is acceptable for companies to do profile marketing generally. The figure increases to 83 percent with prior notice about information uses and an opportunity to opt-out. See survey sponsored by Privacy & American Business, conducted by Louis

## EFFECTIVE PRACTICES

This section discusses examples of existing bank practices for complying with the affiliate information sharing notice provisions of the FCRA and addresses the contents of the notice, the appearance and prominence of the notice, and the convenience of a customer's opportunity to opt out. While the FCRA does not impose specific requirements for the placement or content of the notice, the following examples illustrate how some banks have used these notices to make their information handling practices more readily understandable to their customers. Likewise, the FCRA does not dictate that consumers be accorded convenient methods to opt out of information sharing. However, we have selected examples of existing practices to highlight how some banks, consistent with the spirit of the law, have made the opt out process easier for their customers to use.

### Content of Affiliate Sharing Notice<sup>14</sup>

#### *What type of information is shared*

A simple and concise description of the types of information that a bank intends to share among affiliates enables customers to make informed choices about whether to opt out of affiliate information sharing. For example, a number of banks inform their customers, when it is the case, that they share consumer reports in addition to other types of information, such as information from a customer's application, unless a customer opts out, rather than simply tell their customers they intend to share "other information" — the terminology employed by the statute. Some banks provide additional disclosures to make their information sharing practices more transparent to their customers. For instance, some banks explain that they share the following types of information with affiliates: identification information (such as name and address), transaction and experience information (such as loan repayment history), and other personal information (such as information obtained from an application or consumer report). The banks explain that, unlike transaction and experience information that they may share among affiliates by law, customers may direct that certain other personal information (*i.e.*, information contained in an application, information from consumer reports) not be similarly shared.

#### *With whom is the information shared*

---

Harris and Associates and Dr. Alan F. Westin, "Privacy, E-Commerce, and Financial Transactions" (November 1998).

<sup>14</sup> Some banks have selected a question and answer format to convey information about their usage of customer data. This is one method for conveying basic information to customers in a clear and easily understood format.

---

Date: March 29, 1999

Some banks inform customers of the names of their affiliated companies with which information will be shared and/or a description of their lines of business. In situations involving numerous affiliates, a generally stated description of the types of business they conduct is used instead. Other banks provide their customers with an expressly stated representative sample of the names or lines of business of their affiliates. (Banks that identify their affiliates by name or business type should be aware of the potential need to update their notices if there is a change in circumstances.) In describing their affiliates, some banks choose to use a term other than "affiliate" to avoid potential customer confusion, such as "members of the corporate family."

#### *Purpose for the sharing*

Notices may also contain basic information about the reasons why the bank shares personal data. Some banks describe specific ways in which information sharing benefits their customers. For example, certain banks explain that by knowing that a particular individual owns a home, the bank can direct that consumer to a home equity loan to finance a purchase because of the favorable tax consequences, rather than an unsecured installment loan. Other purposes for information sharing may be to reduce the customer's burden in having to provide duplicative information each time the customer applies for a new product or service from an affiliated company, or to identify customers for better pricing on products or services. Banks sometimes disclose these types of specific benefits in addition to more general disclosures that sharing customers' information enables a bank to design or improve products and services, such as new types of account or investment services. These types of disclosures also provide the bank a good opportunity to promote and distinguish its customer service.

#### **Presentation of Notice**

There are various ways that banks make FCRA notices clear and conspicuous to customers. Some banks provide customers with the notice in a stand alone document.<sup>15</sup> Other banks have chosen to include the notice in a document containing additional information, such as an account agreement. Banks can employ a number of devices to highlight the notice, including (1) putting a box around it, (2) putting it in bold type, (3) putting it in type that is larger than other portions of the text, (4) putting the notice in a different color than other portions of the agreement, (5) captioning the notice to call attention to its contents, (6) underlining the notice, or (7) doing a combination of several of these steps. As part of its FCRA notice, one bank provides a telephone number its customers can call with questions about information sharing and opt out.

#### **Convenience of Customer Opt Out**

---

<sup>15</sup> Banks must not only provide this notice to new customers, but must also provide notice to existing customers. Some banks have sent separate mailings, such as postcards, to their customers to provide the requisite notice. Other banks have sent this notice to existing customers in their regular customer statements.

For bank customers who are concerned about maintaining the privacy of their personal information, being furnished with a convenient mechanism for opting out of affiliate information sharing is a value-added service. Banks have many options to provide customers convenient opportunities to opt out of information sharing, including providing their customers with detachable opt out forms as part of the affiliate information sharing notice or self-addressed opt out postcards. Additionally, some banks allow for opt out by telephone or by electronic means (for instance, by personal computer via the bank's Web site)<sup>16</sup>. One bank provides a check-off box in a prominent position on its credit applications -- within the box containing the signature line -- that customers can mark to elect to opt out of information sharing.

## CONCLUSION

Banks that share particular personal information with their affiliates may use the notice requirements of the FCRA as an opportunity to inform their customers about their information handling practices and further provide their customers with convenient mechanisms for opting out of such sharing. At a time of growing public sensitivity and concern about the proper treatment of personal information, this type of meaningful communication may enhance customer confidence and trust in their financial institutions.

## FURTHER INFORMATION

For further information or questions relating to this advisory, please contact Amy Friend, Assistant Chief Counsel, (202)874-5200.

---

Julie L. Williams  
Chief Counsel

---

<sup>16</sup>If a bank chooses to permit opt out by means other than in writing, the bank should create a record of the opt out.

---

Date: March 29, 1999



## OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

**TO:** Chief Executive Officers of all National Banks, Department and Division Heads, and all Examining Personnel

### PURPOSE

This guidance provides national banks with examples of effective practices for informing consumers who access bank Internet sites about bank privacy policies for the collection and use of personal information. The guidance also discusses examples of effective practices for the development of bank privacy policies and for ensuring adherence to those policies.

### BACKGROUND

Banks increasingly are using the Internet as a medium for communicating with their customers, and, to a lesser extent, as a vehicle for enabling their customers to conduct financial transactions. The success of banks in expanding the amount and type of business they and their customers conduct on line will depend largely on customer acceptance of this medium for making financial transactions. Survey data indicate that consumers are sensitive to how businesses, including banks, maintain, use, and analyze information about them. These consumer concerns about the accumulation and use of their personal information are likely to increase with the growing use of the Internet and electronic commerce.

Because a fundamental component of the bank/customer relationship is a customer's trust in the institution to respect the privacy and confidentiality of that relationship, it becomes even more important for banks to reassure customers about the safeguarding of their personal information when it is communicated in a remote, on-line environment. Indeed, informing customers about bank policies for handling of personal information may well increase consumer confidence in transacting business electronically. [Note: A recent Harris-Westin survey found that the majority of Internet users who purchased goods or services on line said that it was very important for businesses to post notices on their Web sites explaining how they will use the personal information customers provide when making purchases over the Internet. Further, the survey found that of consumers not likely to access the Internet in the next year, greater privacy protection was the factor that would most likely convince them to use the Internet. *E-Commerce and Privacy: What Net Users Want*, a survey conducted by Louis Harris and Associates, Inc. and Dr. Alan F. Westin, June 1998.] The Internet, thus, presents banks with both new business opportunities and new challenges for addressing legitimate expectations of customers about the privacy and security of their personal information.

---

Date: July 20, 1999



# OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

A number of institutions have recognized the growing importance of privacy to their customers and have developed, implemented, and communicated privacy policies. [Note: A number of the banking trade associations -- the American Bankers Association, the Consumer Bankers Association, the Banking Industry Technology Secretariat of the Banker's Roundtable, American's Community Bankers, and the Independent Community Bankers of America -- have adopted a core set of banking industry privacy policies. These industry-wide policies have been used by many banks as a starting point for developing privacy policies tailored to their individual corporate practices.] Generally, these policies encompass one or more of the following five areas: (1) notice to consumers about the institution's information practices; (2) consumer choice about the disposition of personal information; (3) accuracy of personal information maintained by the institution; (4) security measures to protect consumers' personal information; and (5) mechanisms to handle consumer questions or complaints about the handling of personal information. [Note: For a discussion of widely accepted principles concerning fair information practices see *Privacy Online: A Report to Congress*, Federal Trade Commission, June 1998 (posted at [www.ftc.gov/reports/privacy3](http://www.ftc.gov/reports/privacy3)).] This guidance provides examples from a sampling of these existing bank practices that represent effective approaches for the development and implementation of privacy policies and their posting on bank World Wide Web (Web) sites.

Although this guidance is targeted at banks that operate Web sites, the examples of practices and procedures for developing and implementing privacy policies are pertinent to any national bank considering establishing or revising a privacy policy and related procedures. Thus, national banks may find these examples helpful as they develop their own privacy policies and implementation procedures. These examples are not examination standards, do not impose new regulatory requirements on banks, and are not intended to be an exclusive description of the various ways banks can devise and communicate effective privacy policies.

## EXISTING LEGAL REQUIREMENTS

Financial institutions, historically, have taken special care to protect the privacy and security of confidential customer information and have long been subject to a number of federal and state laws that govern the handling of such customer information. These laws and regulations may

---

Date: July 20, 1999



# OCC ADVISORY LETTER

Comptroller of the Currency  
Administrator of National Banks

Subject: Guidance to National Banks on Web Site Privacy Statements

apply to aspects of the operation of bank Web sites. [Note: Banks offering PC banking were reminded to be familiar with applicable privacy rules that could restrict their ability to share information with third parties that they obtain from their customers. See Technology Risk Management: PC Banking, OCC Bulletin 98-38, August 24, 1998. The OCC also recently issued an Advisory Letter alerting bankers to the practice of "pretext phone calling," which is a means of gaining access to customers' confidential account information by organizations and individuals who call themselves "account information brokers." This letter was also intended to enhance institutions' awareness regarding the confidentiality and sensitivity of customer information generally, and identify some appropriate measures for the safeguarding of such information. See OCC Advisory Letter 98-11.] For example, banks operating Web sites that permit customers to transfer funds electronically into and out of their accounts [Note: An "account" for the purposes of the Electronic Funds Transfer Act (EFTA) is defined as a demand deposit, savings deposit or other consumer asset account held directly or indirectly by a financial institution, established primarily for personal, family or household purposes. 15 U.S.C. §1693a(2); 12 C.F.R. 205.2(b)(1).] must inform these customers, among other things, about the situations in which the bank, in the "ordinary course of business," will disclose information about the customers' accounts to third parties. [Note: *Id.* §1693c(a)(9); 12 C.F.R. 205.7(b)(9). This disclosure must describe the circumstances in which any information concerning the account may be provided to third parties, including affiliates. See FRB Official Staff Commentary 205.7(b)(9)-1.

Banks may make this disclosure by mail, or, for a discussion of how banks may satisfy the EFTA's disclosure requirements by electronic means, see the interim rule currently in effect at 12 C.F.R. 205.4(c)(2), 63 Fed. Reg. 14528 (March 25, 1998).

Additionally, if a bank permits customers to apply for credit over its Web site, the Fair Credit Reporting Act's conditions for sharing certain customer information outside of the bank may apply. [Note: The Fair Credit Reporting Act (FCRA) provides that certain consumer information that is shared among affiliates is not a "consumer report" if there is clear and conspicuous notice to the consumer that the information may be shared and the consumer is given an opportunity to direct that the information not be shared ("opt out" notice). 12 U.S.C. §1681a(d)(2)(A)(iii). For a further discussion about the FCRA, the different types of consumer information that it covers, and examples of effective practices for satisfying the notice and opt out requirements related to sharing of information among affiliates, see OCC Advisory Letter 99-3.

Date: July 20, 1999





## OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

### EFFECTIVE PRACTICES

This section discusses examples of existing bank practices that the OCC considers effective means for communicating a bank's privacy policies, developing a bank's policies for handling customer information, and ensuring adherence to stated policies.

#### Communication of Privacy Principles

The most effective disclosures of privacy principles are clear, prominent, and easy to understand. In general, effective disclosures avoid communicating complicated information in a complex and technical way. Many banks that post privacy notices on their Web sites acknowledge their customers' privacy expectations and indicate how the bank will safeguard and handle personal information. In many instances, banks inform their customers that the bank takes measures to limit employee access to confidential information and to maintain accurate and up-to-date consumer records. Some banks also describe the general circumstances under which the bank will share information with third parties. Some banks explain that customers have a choice about how their information is shared and provide a convenient way to "opt out" of mail or telephone solicitations. Additionally, some Web site privacy policies explain the bank's collection and usage of customer information that is unique to the online environment, such as "cookies."

[Note: A "cookie" is a piece of information that a Web site stores on a visitor's Web browser that is retrieved when the visitor logs onto the site again.] To ensure that these stated principles are readily understood, some banks have supplemented their privacy principles with a series of questions and answers about the handling of customer information. [Note: Many banks use their Web sites as the only medium for communicating their privacy policies to customers. Some banks, however, provide customers with written copies of their privacy policies as a stand alone document or in conjunction with other written materials.]

Banks have used a number of different devices to feature their privacy statements prominently. Banks with effective communication practices have posted privacy policies at specific locations on their Web sites where they may be most meaningful to the consumer. For instance, a bank that permits customers to submit on-line credit applications displays its privacy policy at the point at which the customer is asked to submit personal information. Many banks place "hypertext" links or "hotlinks" to privacy statements on their Internet home pages and/or on Web site transactional pages (e.g., on-line banking or small business pages) that automatically present disclosures to customers when the option is selected. Several banks place links to their privacy policies in the footer of each of their Web site pages.

---

Date: July 20, 1999



# OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

## **Developing an Effective Privacy Policy**

Banks with effective privacy policies also take steps to ensure that their internal policies and procedures are consistent with and support stated privacy promises.

### *Senior Management Involvement*

Effective policies and procedures often involve senior management's knowledge of, and involvement in, the planning process. Senior management can provide a broad perspective on the issues, dedicate appropriate resources to accomplish the task, and create the necessary culture to ensure that privacy matters are addressed comprehensively and consistently across the organization. In a number of banks, the teams or personnel responsible for developing privacy policies and procedures report directly to senior officials.

### *Interdisciplinary Working Groups*

A number of banks, particularly large banks, have formed privacy working groups, teams, or task forces consisting of members from various departments in the bank (e.g., legal, marketing, compliance, retail, systems, security, and human resources) to either update or develop their privacy policies and procedures for handling customer information. The multi-disciplinary team approach has enabled banks to centralize efforts, while ensuring that diverse interests and perspectives in the company are represented. One institution that used the team approach to develop an institution-wide privacy policy is relying on individual business units to develop appropriate implementation plans to support the policy. Some smaller institutions, however, with different business considerations and personnel resources have found that an interdisciplinary team was not needed to develop privacy policies. In these cases, senior management appointed a particular division or employee to develop policies and procedures.

---

Date: July 20, 1999



## OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

### *Review of Existing Procedures and Systems*

Often the individuals or groups responsible for establishing policies and procedures reviewed existing systems, operations, and other internal policies to better understand current information practices, to assess risks associated with information handling, and to avoid promulgating privacy promises that could not be met. Additionally, reviews have involved an assessment of which, and the extent to which, existing systems and practices needed to be modified to accommodate a bank's new or revised privacy policy. [Note: Because of changes in bank systems, operations, and technology, banks expect these reviews will need to be ongoing or periodic.]

### *Review of Relationships with Third Parties*

In addition to reviewing internal procedures and practices, many banks have reviewed their relationships with unaffiliated third parties to assess their adherence to the bank's privacy policies. Several banks that provide customer information to unaffiliated third parties for joint marketing purposes or operational support, such as data processing, have required the third party to execute a confidentiality agreement and agree to limit the use of information. Some banks also monitor these third parties for compliance with their agreements and/or give their customers prior opportunity to opt out of the information sharing where feasible (e.g., joint marketing).

### **Enhancing the Effectiveness of the Bank's Privacy Policy**

Banks with effective privacy policies take measures to enhance their employees' understanding of compliance with such policies. These banks have supported their policies with employee training and compliance mechanisms.

### *Internal Communication and Training*

Banks with effective privacy policies take steps to ensure that their policies are understood by bank personnel involved in the handling of confidential customer information. These banks widely communicate the policies among appropriate bank employees and support them with employee training. For example, banks have informed their employees about their privacy policies through employee handbooks, codes of ethics, articles in company newspapers, Intranet postings, individual mailings from senior management, or the distribution of policy guidance. Some banks have supplemented communications with various forms of training -- live sessions,

---

Date: July 20, 1999



## OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

handbooks or videos. Many banks require employee acknowledgment of training, *i.e.*, the staff must formally acknowledge their understanding of privacy/confidentiality policies, by signing a form. Where the bank's privacy policies have been incorporated into the bank's code of ethics, officers and employees have been required to certify their own compliance (annually or periodically) with the ethics code.

### *Compliance*

A number of banks have established programs or procedures to enhance compliance with their privacy policies. Some banks require individual business unit compliance officers to establish appropriate compliance plans and/or require periodic self assessments by business lines to determine the adequacy of their adherence to procedures and internal controls. Others determine the adequacy of compliance through internal audits (the frequency of which is determined by the risk associated with the individual lines of business), or use audits to supplement the activities of business line managers or compliance officers. Depending on the size of the institution or the nature of the activity at issue, some institutions rely on periodic reviews rather than formal audits to monitor compliance with privacy policies.

Most banks have procedures designed to deter employee violations of their policies. An employee's failure to comply with a bank's privacy policy is often subject to the same disciplinary actions as any other breach of bank policy -- including termination where appropriate. These personnel procedures have been provided for in banks' ethics codes, codes of conduct, or human resource policies.

Additionally many banks have established mechanisms for handling consumer privacy complaints and inquiries. Some banks provide for a central point of contact within the bank to handle customer privacy issues. For instance, some banks provide an e-mail link on their Web sites for privacy related questions or complaints. Another bank has appointed an ombudsman to handle customer privacy complaints. Still, another bank catalogues privacy complaints, and depending on their nature, routes them to different centralized locations for handling. Each business line is expected to appoint a privacy officer and track and correct privacy complaints in another bank. Some banks have determined that, because of their size or the nature of the activities they conduct, they can use established mechanisms or procedures within the bank designed to deal with customer complaints, generally, to handle customer privacy related complaints.

---

Date: July 20, 1999



## OCC ADVISORY LETTER

---

Comptroller of the Currency  
Administrator of National Banks

---

Subject: Guidance to National Banks on Web Site Privacy Statements

---

### CONCLUSION

At a time of growing public sensitivity and concern about the treatment of personal information, bank privacy policies may enhance customer confidence and trust in their financial institutions. When posted on bank Web sites, privacy policies may increase customer acceptance of the Internet as a medium for conducting financial transactions. The most effective privacy policies found on bank Web sites are those that are posted prominently, contain clear and readily understandable disclosures about the handling of customer information, and are supported by consistent internal procedures and methods to enhance compliance by bank personnel.

### FURTHER INFORMATION

For further information or questions relating to this advisory, please contact Amy Friend, assistant chief counsel at (202) 874-5200.

---

Julie L. Williams  
Chief Counsel

---

Date: July 20, 1999

**Question 1:** At the July 20, 1999 hearing, one of the academic witnesses recommended that the OCC pursue workshops like the FTC has done on privacy to improve industry practices, etc... Do you think that would be a helpful thing? Have you discussed this kind of option OR are your efforts focused more on Best Practice activities as an example?

**Response:** We think both approaches can be helpful in this area. On October 19, 1998, the OCC conducted a forum on consumer privacy with the participation of industry leaders, public interest representatives, academic experts and government representatives. The forum sought to facilitate a dialogue about privacy issues confronting the banking industry and their customers, specifically focused on public awareness and concerns about privacy, use of customer information, and security of customer information. The discussion produced practical information that the agency used in formulating "effective practices" guidance in the privacy area.

Since the forum, the OCC has issued two privacy-related advisories. The first such guidance was issued on March 29, 1999 and identified effective practices among national banks for complying with the affiliate sharing notice and opt out requirements of the Fair Credit Reporting Act. The second guidance, dated May 4, 1999 advised banks about effective practices for establishing and posting privacy policies on Internet Web sites.

The agency considers consumer privacy a significant customer service issue that has great importance for the future of the banking industry. Accordingly, the OCC will consider workshops, forums, and guidance, as well as other appropriate mechanisms, as avenues for continuing to communicate with the industry about ways to improve customer privacy.

**Question 2:** How important, if at all, are privacy policies that institutions can be held accountable to in law today?

**Response:** Currently, there are no legal requirements that banks establish privacy policies. However, the OCC, as well as other banking regulators have been encouraging banks to review their information handling practices and to develop and adhere to privacy policies. The OCC believes it is important for banks to address their customers' expectations about privacy and inform them about the bank's information handling practices as a means of preserving customer trust. Our May 4, 1999 guidance informs banks that it is particularly important to post privacy policies on Web sites where communication and transactions between banks and their customers are remote. Reassuring bank customers about the safe and proper handling of their information, especially when asking them to transmit information online, is likely to be important to the acceptance, and therefore growth, of Internet banking. The OCC has asserted that "enlightened" self regulation is in the interest of banks as well as their customers.

Additionally, international events are shaping the debate in this country on privacy and placing a spotlight on self regulation. Last year the European Union Directive on privacy went into effect, requiring that countries outside of the EU have adequate privacy protections in order to handle data on EU residents. Unlike European countries that have comprehensive privacy laws, the U.S. has a patchwork of state and federal laws that have been adopted on a sectoral

basis. Self regulation has become an important factor in compensating for gaps in privacy protection, and self regulatory regimes are now being studied by the EU to assess the adequacy of U.S. privacy measures.

The OCC is currently considering ways to hold banks accountable for their stated privacy policies. Recently, the FTC brought an unfair and deceptive practices action against a company operating on the Internet for handling customer information in contravention of the company's posted privacy policy. The FTC Act that prohibits unfair and deceptive practices similarly applies to banks, but the FTC has no authority to take actions against banks. The banking regulators may enforce the FTC Act by enforcing regulations promulgated by the Federal Reserve Board that specify unfair and deceptive practices by banks. To date, however, the FRB has not issued any such regulations in the privacy area.

Privacy policies may also be enforceable under state statutes or common law. One state, Minnesota, has sought to hold a bank accountable for its privacy policy under the state's consumer fraud and false advertising statutes. The case was settled and the bank agreed to change its privacy policy and information sharing practices. As part of that settlement agreement, the bank may share personal customer information with affiliates for direct marketing purposes (telemarketing or targeted mail solicitations) and with nonaffiliated third parties for marketing financial products and services only if the bank's customers are given notice of the information sharing and an opportunity to opt out. Pursuant to the settlement agreement, the bank must submit its revised privacy policy and opt out notices to the OCC for approval.

**Question 3:** What kinds of complaints does the OCC receive specific to consumer financial privacy? Have they been rising recently?

**Response:** The OCC receives privacy related complaints from consumers involving issues such as sale of customer information, identity theft, and bank usage of fingerprinting or retinal scans to identify nonbank customers. While the number of privacy related complaints are small relative to the consumer complaints we receive, generally, there has been an increase in recent months in the number of complaints related to the sale of customer information.

**Question 4:** What are your views on the affirmative responsibility to respect privacy provisions in H.R. 10?

**Response:** Section 501(a) states, "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." In furtherance thereof, section 501(b) requires specific agencies, including the federal banking agencies, to establish appropriate standards for the institutions they regulate relating to administrative, technical and physical safeguards of customer information.

The OCC supports the articulation of an affirmative obligation on the part of financial institutions to safeguard customer privacy, provided that it is coupled with sufficient guidance about how to comply with this obligation. If compliance with the standards articulated by the agencies pursuant to 501(b) is sufficient to meet this obligation (in addition to the specific requirements set out in subsequent sections), and we believe that such an interpretation is warranted, then the scope of the affirmative duty is clear. If, however, the affirmative duty is not tied to meeting the standards established by the agencies and, as a result, subjects financial institutions to lawsuits for failure to meet an ill defined obligation, the OCC would object to such a far reaching provision.

**Question 5:** You have questioned some financial institution lenders for not reporting information regarding sub-prime borrowers. Will your concerns be exacerbated by H.R. 10?

**Response:** The OCC does not believe that H.R. 10 will have any effect on the issue of credit reporting by sub-prime lenders.

**Question 6:** Do you think we should amend the FCRA to include transaction and experience data?

**Response:** The FCRA covers entities that are considered to be "consumer reporting agencies" because they regularly assemble or evaluate particular information in order to disseminate consumer reports. A consumer report is a written, oral, or other form of communication of information that bears on a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living..." A report containing a person's own "transactions or experiences" with consumers is exempt from the definition of a consumer report. As you can see from these definitions, the FCRA covers entities beyond financial institutions. Accordingly, removing the transaction and experience information exemption from the definition of a consumer report will have an impact on entities that exceed the expertise of this agency.

The approach taken by the House in H.R. 10 will effectively regulate transaction and experience information, among other types of consumer information, when financial institutions want to disclose the information to unaffiliated third parties. Under the H.R. 10 approach, the sharing of this type of information will not render a financial institution a consumer reporting agency, (which would be the likely consequence if the FCRA were amended to cover transaction and experience information), but the failure to adhere to the notice and opt out requirements of H.R. 10 could trigger administrative enforcement. The bill provides that the federal banking agencies may use the enforcement powers under section 8 of the Federal Deposit Insurance Act which include cease and desist orders, as well as the ability to assess civil money penalties.

**Question 7:** On page 6 of your testimony, you note that you have concerns about the enforcement authority under the pretext calling provisions. Can you expound?



**Response:** Section 522 of H.R. 10 vests the FTC with enforcement authority. The scope of this authority is unclear. Section 522(a) states that the FTC shall enforce the provisions in the same manner and with the same power and authority as the Commission has under the Fair Debt Collection Practices Act (FDCPA). The FDCPA vests the Commission with all the functions and powers available under the FTC Act, including the power to enforce the FDCPA as if the violation had been a violation of a trade regulation rule. The FDCPA, however, specifically commits enforcement authority to the banking agencies with respect to banking institutions.

The pretext calling provisions do not similarly grant enforcement authority to the banking agencies. Moreover, section 522(b) requires the FTC to notify the federal banking agencies whenever the Commission initiates an investigation with respect to a financial institution subject to regulation by the banking agencies. Therefore, these provisions mean either that the FTC has authority to take enforcement action against banks (authority not given to the FTC elsewhere in law), or that the FTC can investigate banks, but not bring enforcement actions, and therefore no entity has the authority to take actions against an offending bank.

The OCC would like this provision clarified to vest investigative and enforcement authority with the federal banking agencies in matters that involve the institutions that we regulate consistent with the FDCPA, as well as other federal consumer protection statutes, and the FTC Act.

**Question 8:** How do you envision the role of the regulator in enforcing the privacy provisions of H.R. 10 once enacted into law?

**Response:** H.R. 10 establishes an appropriate role for the agencies in the following ways. It directs the financial institution regulators to promulgate regulations to carry out the purposes of the privacy provisions, and further gives the agencies enforcement authority pursuant to section 8 of the FDI Act, discussed in response to Question 6, above. Additionally, H.R. 10 requires the banking regulators to promulgate regulations under the FCRA, and further restores the full scope of the agencies' examination authority under the FCRA. Currently, the banking agencies may examine a bank for compliance with the FCRA only if the agency receives a consumer complaint that involves an FCRA violation or the agency "otherwise has knowledge" of a violation. With this restored examination authority, the agencies can include privacy-related compliance review as part of their regularly scheduled compliance examinations and take appropriate action where violations are found.



UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

---

**PREPARED STATEMENT OF THE  
FEDERAL TRADE COMMISSION**

**Before the**

**SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
COMMITTEE ON BANKING AND FINANCIAL SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES**

**on**

**FINANCIAL PRIVACY, THE FAIR  
CREDIT REPORTING ACT, AND H.R. 10**

**July 21, 1999**

## I. INTRODUCTION

Chairwoman Roukema and members of the Subcommittee, I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on H.R. 10, the Fair Credit Reporting Act ("FCRA") and financial privacy.<sup>1</sup> The Commission supports the work of the Committee in striving to provide financial privacy protections for consumers and supports such provisions currently in H.R. 10.

We live in a burgeoning information economy. The personal computer revolution of the 1980s, and the explosive growth of interactive technologies in the 1990s, have made it possible for businesses to collect, aggregate, store, and market personal information in ways unthinkable only a generation ago. The commercial use of this information can have great benefits for consumers and industry, by allowing more cost-effective marketing systems. At the same time, it raises concerns because of the speed and ease with which vast amounts of sensitive information can be aggregated and disseminated.

It is not surprising to learn that, of all the types of information collected about them, American consumers view their financial information as extremely sensitive, indeed as sensitive as their medical histories.<sup>2</sup> Congress has long recognized this fact in enacting laws to protect financial information, such as the FCRA and the Right to Financial Privacy Act. As custodians

---

<sup>1</sup> The Commission voted 3-1 to issue this testimony, with Commissioner Swindle concurring in part and dissenting in part. His statement is to be attached to the testimony.

My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or the other Commissioners.

<sup>2</sup> Testimony of Alan F. Westin on "Electronic Payment Systems, Electronic Commerce, and Consumer Privacy" before the Subcommittee on Financial Institutions and Consumer Credit, House Committee on Banking and Financial Services, at 4 (September 18, 1997).

of sensitive financial information, financial institutions must take their customers' privacy concerns into account. The Commission has extensive experience dealing with privacy and consumer protection issues, including those related to the financial services industry, and I am pleased to present the Commission's perspective in this complex area.

## II. THE COMMISSION'S CONSUMER PROTECTION MISSION

The FTC is a law enforcement agency whose mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.<sup>3</sup> The Commission's authority over banks, other depository institutions and insurers is limited to the extent they are regulated by federal bank or state insurance regulatory agencies.<sup>4</sup> The FTCA generally provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce and with the authority to gather information about such entities.<sup>5</sup> The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices.<sup>6</sup> Recently, for example, the

---

<sup>3</sup> 15 U.S.C. § 45(a).

<sup>4</sup> Moreover, the Commission's authority to conduct studies and prepare reports relating to the business of insurance is limited. 15 U.S.C. § 46(a).

<sup>5</sup> 15 U.S.C. §§ 45(a), 46(a).

<sup>6</sup> These include, for example, the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices.

Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime and authorized the Commission to serve as a central clearinghouse to receive complaints from, and provide information to, victims of identity theft.<sup>7</sup>

The Commission has extensive experience in addressing consumer protection issues that arise in the financial services industry, involving, for example, the use of credit cards, lending practices, and debt collection.<sup>8</sup> Similarly, the Commission has been deeply involved in addressing online privacy issues,<sup>9</sup> including consultation to Congress and the federal banking

---

<sup>7</sup> Public Law No. 105-318, 112 Stat. 3007, amending 18 U.S.C. § 1028 (1998). Specifically, the Act requires the Commission to establish procedures to (1) log the receipt of complaints by victims of identity theft; (2) provide these victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.

<sup>8</sup> Commission cases involve claims of, for example, aiding and abetting a merchant engaged in unfair and deceptive activities, Citicorp Credit Services, Inc., 116 F.T.C. 87 (1993), discrimination based on race and national origin in mortgage lending, United States v. Shawmut Mortgage Co., 3:93CV-2453AVC (D. Conn. Dec. 13, 1993), failure to provide required notices of adverse actions to credit applicants, United States v. J.C. Penney Co., CV964696 (E.D.N.Y. Oct. 8, 1996), and engaging in unfair and deceptive practices in its collection of credit card debts after the filing of consumer bankruptcy, Sears, Roebuck and Co., C-3786, 1998 FTC LEXIS 21 (Feb. 27, 1998); Montgomery Ward Corp., C-3839 (Dec. 11, 1998); May Department Stores Co., File No. 972-3189, 1998 FTC LEXIS 117 (Nov. 2, 1998).

<sup>9</sup> The Commission has held a series of public workshops on privacy since April 1995. It also has examined Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children; issues raised by individual reference ("look up") services, as well as issues relating to unsolicited commercial e-mail. These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. *Self-Regulation and Privacy Online: A Report to Congress* (July 1999); *Privacy Online: A Report to Congress* (June 1998). Further, the Commission staff has issued reports describing various privacy concerns in the electronic marketplace. See, e.g., FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996); FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

The Commission has also brought enforcement actions under Section 5 of the FTCA to address deceptive online information practices. In its first Internet privacy case, GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site. The settlement prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children and requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had

agencies about consumer protection issues involving financial services.<sup>10</sup> Just last week, the Commission presented its views on online privacy issues and the status of self-regulatory efforts before the House Commerce Committee, Subcommittee on Telecommunications, Trade and Consumer Protection. At that time, the Commission also issued its Report to Congress on "Self-Regulation and Privacy Online."<sup>11</sup> Additionally, the Commission regularly provides comments to the Federal Reserve Board regarding the FCRA, and the implementing regulations for the Truth in Lending Act, the Consumer Leasing Act, the Electronic Funds Transfer Act, and the Equal Credit Opportunity Act.<sup>12</sup> Finally, the FTC's Privacy Policy, which has been in place for about two years, is featured on the home page of the website, [www.ftc.gov](http://www.ftc.gov).<sup>13</sup>

---

previously collected personal information an opportunity to have that information deleted. *GeoCities*, Docket No. C-3849 (Feb. 12, 1999) (Final Decision and Order available at <http://www.ftc.gov/os/1999/9902/9823015d&o.htm>). In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. In fact, this information was maintained in identifiable form. The consent agreement would require Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children. *Liberty Financial*, Case No. 9823522 (proposed consent agreement available at <http://www.ftc.gov/os/1999/9905/lbtyord.htm>).

<sup>10</sup> In 1997, the Commission conducted a study of database services, known as "look-up services" or "individual reference services," that make commercially available personal information used to locate and identify individuals. The study examined how such services operate and how they may create detailed profiles on consumers containing financial and other sensitive personal information. The Commission then reported to Congress what it had learned about the individual reference services industry and assessed the viability of a proposed set of industry self-regulatory principles, designed to provide some controls on the disclosure of sensitive personal information. *Individual Reference Services: A Report to Congress* (December 1997).

<sup>11</sup> See *supra* note 9. The Commission's testimony may be found at <http://www.ftc.gov/os/1999/9907/pt071399.htm>

<sup>12</sup> Commission staff also participates in numerous task forces and groups concerned with, for example, fair lending, leasing, subprime lending, electronic commerce, and commerce on the Internet, all of which have an impact on the financial services industry.

<sup>13</sup> With only one mouse click, any one can reach the "Privacy Policy for FTC Website" statement ([www.ftc.gov/ftc/privacy1](http://www.ftc.gov/ftc/privacy1)). It sets forth the limited information retained by the FTC on consumers who visit the site to read or download information, and the use made of any personal information that individuals choose to include when they file complaints. Copies of the home page and Privacy Policy, as viewed by visitors to the Commission website, are attached. We do not attach cookies to visitors' computers.

### III. FAIR CREDIT REPORTING ACT

The Subcommittee has requested that the Commission provide a discussion of its regulatory authority in the area of financial privacy, particularly under the FCRA, and its views on the privacy protections in H.R. 10, recently passed by the House.<sup>14</sup>

The FCRA provides critical privacy protection for consumers by limiting the circulation and use of their personal financial information by private firms, including banks. While this law provides strong protections, it does have limits and exceptions. We are aware that the question of how those limits and exceptions should be addressed has been the focus of considerable debate in the context of H.R. 10.

#### A. Scope of the FCRA

The FCRA primarily governs the accumulation and distribution of information that bears on individuals' creditworthiness by regulating consumer reporting agencies, such as credit bureaus, and establishing important protections for consumers with regard to the privacy of their

---

<sup>14</sup> H.R. 10 also includes important provisions to outlaw the practice of obtaining personal financial information by deceit, or "pretexting." The Commission, as noted in prior testimony, supports civil and criminal sanctions against pretexting. Testimony of Federal Trade Commission, as presented by Commissioner Mozelle W. Thompson on "Obtaining Confidential Financial Information by Pretexting" before the House Committee on Banking, at 13-15 (July 28, 1998). Quite properly, in the Commission's view, H.R. 10 does not require a showing of knowledge or intent as part of civil enforcement actions. Those are standards more properly made part of criminal sanctions. Addition of those requirements in a civil suit would have had the effect of making it harder for the Commission to take civil action against "pretexting" misrepresentations. The Federal Trade Commission Act reaches many aspects of pretexting and does not include knowledge or intent as part of the violation.

In April 1999, the Commission brought a federal court action against James and Regana Rapp, doing business as Touch Tone Information, Inc., involving "pretexting." The complaint alleged that they violated Section 5 of the FTCA when they obtained consumers' private financial information by (1) impersonating bank account holders and making false statements to financial institutions and others to induce the disclosure of consumers' private financial information and (2) selling or disclosing that information, to anyone who requested it, without consumers' knowledge or consent. Federal Trade Commission v. Rapp, No. 99-WM-783 (D. Colo. filed April 21, 1999)(authorized by 3-1 vote, Commissioner Swindle dissenting).

sensitive financial information.<sup>15</sup> The FCRA was enacted, in part, to address privacy concerns associated with the sharing of consumers' financial and credit history contained in consumer credit reports.<sup>16</sup> The FCRA limits the disclosure of consumer reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or similar purposes) and under specified conditions (including certification of the permissible purpose by the user of the report).<sup>17</sup> In these ways, the FCRA operates generally to limit disclosure of consumer reports primarily to instances where a consumer initiates a transaction, such as an application for credit, employment, or insurance.<sup>18</sup> The FCRA also provides consumers with certain rights in connection with the information maintained by consumer reporting agencies.<sup>19</sup>

The FCRA imposes civil liability for both willful and negligent noncompliance by consumer reporting agencies and parties who procure reports from (or furnish information to) such agencies.<sup>20</sup> It grants civil enforcement authority to the Commission, other federal agencies,

---

<sup>15</sup> 15 U.S.C. §§ 1681 et seq. Some states also have their own laws dealing with the same issues. Section 624 of the FCRA specifies certain matters with respect to which the federal law preempts any such state law.

<sup>16</sup> *See, e.g.*, 15 U.S.C. § 1681(a)(4) ("There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.").

<sup>17</sup> 15 U.S.C. § 1681-1681u. The 1996 amendments specifically authorized the practice of creditors and insurers who use credit bureau files to "prescreen" consumers they solicit for their products under specific procedures, most importantly that consumers be notified of the process and be allowed to "opt out" of future credit bureau prescreens. 15 U.S.C. §§ 1681a(m), 1681b(c), 1681b(e), and 1681m(d).

<sup>18</sup> 15 U.S.C. § 1681b.

<sup>19</sup> 15 U.S.C. §§ 1681-1681u. Most importantly, the FCRA requires creditors and other businesses to notify consumers when they take adverse action, in whole or in part, because of a consumer report from a consumer reporting agency (15 U.S.C. § 1681m), and compels consumer reporting agencies to disclose data in their file to consumers upon request (15 U.S.C. § 1681g) and to reinvestigate items disputed by the consumer in good faith. (15 U.S.C. § 1681i).

<sup>20</sup> 15 U.S.C. §§ 1681n-1681o.



and the states, to seek both monetary and injunctive relief for violations of the Act.<sup>21</sup> The potential monetary penalties include, for those who knowingly violate the FCRA, up to \$2,500 per violation in a civil action brought by the Commission in district court,<sup>22</sup> or damages incurred by residents of a state in an action brought by the attorney general (or other official or agency designated by the state) on their behalf.<sup>23</sup> The FCRA also provides for criminal sanctions against parties who infringe on consumer privacy by unlawfully obtaining consumer reports.<sup>24</sup>

The Commission has undertaken FCRA enforcement actions against the three major credit bureaus in the last eight years,<sup>25</sup> including one matter currently pending before the Commission.<sup>26</sup> It has dedicated a portion of its website to the FCRA ([www.ftc.gov/os/statutes/fcra](http://www.ftc.gov/os/statutes/fcra)), where the public can access the statutory text, Commission proceedings relating to the FCRA, consumer education materials, press releases, and the text of over 60 informal FCRA opinion

---

<sup>21</sup> 15 U.S.C. § 1681s.

<sup>22</sup> 15 U.S.C. §1681s(a)(2). The Act creates a private right of action for actual damages proven by a consumer, plus costs and attorneys fees. In the case of willful violations, the court may also award punitive damages to a consumer. 15 U.S.C. § 1681n(a)(2). Any person who procures a consumer report under false pretenses, or knowingly without a permissible purpose, is liable for \$1000 or actual damages (whichever is greater) to both the consumer and to the consumer reporting agency from which the report is procured. 15 U.S.C. § 1681n(b).

<sup>23</sup> 15 U.S.C. § 1681s(c)(1)(B)(i-ii).

<sup>24</sup> "Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses ..." may be fined and imprisoned for up to 2 years. 15 U.S.C. § 1681q. The Computer Fraud and Abuse Act prohibits unauthorized entry into credit bureau files, providing for fine and imprisonment (up to one year for a first offense, up to ten years for a second offense) of a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in . . . a file of a consumer reporting agency on a consumer, as such terms are defined in the [FCRA]." 18 U.S.C. § 1030(a)(2).

<sup>25</sup> Equifax Credit Information Services, Inc., 120 F.T.C. 577 (1995); FTC v. TRW, Inc., 784 F. Supp. 361 (N.D. Tex. 1991).

<sup>26</sup> Matter of Trans Union Corporation, FTC Docket No. 9255. The Commission is currently considering an appeal of an initial decision of Administrative Law Judge James P. Timony, 1998 FTC LEXIS 88 (July 31, 1998).

letters the staff has published since major changes to the statute became effective in September 1997.

#### B. Where the FCRA Does Not Apply

There are two important types of communications among businesses that the FCRA specifically exempts from the full protections that apply to consumer reports. First, a business is free to distribute without limitation information about its own "transactions and experiences" with a customer.<sup>27</sup> Without this exception, the many thousands of firms that report information about their customers each month to credit bureaus might themselves legally be viewed as credit bureaus. Thus, the FCRA does not restrict a financial services (or any other) firm's ability to sell to third parties and affiliates virtually any and all information about its transactions and experiences with its customers, including number and types of accounts, account balances, credit limits, detailed payment history and method of payment – information many, if not most, customers would view as highly sensitive. Allegations in a recent case suggest that at least some financial services firms are selling that type of information.<sup>28</sup> The sale or transfer of such sensitive "transactions and experiences" information, with appropriate exceptions, raises serious privacy concerns.

Second, the 1996 amendments to the FCRA include a provision that permits affiliated companies to share consumer report information free from many of the FCRA's restrictions, so long as a notice and the opportunity to opt-out is provided before such non-transaction and non-

---

<sup>27</sup> Section 603(d) of the FCRA, 15 U.S.C. § 1681a(d)(2)(A)(i) ("The term 'consumer report' . . . does not include any report containing information solely as to transactions or experiences between the consumer and the person making the report.").

<sup>28</sup> Hatch v. US Bank Nat'l Ass'n ND (D.Minn, filed June 9, 1999).

experience information is shared.<sup>29</sup> Most importantly, affiliated companies are permitted to share any information included in a credit report procured by one of the affiliates.<sup>30</sup> Prior to this change, an affiliate that regularly communicated consumer report information to related companies (beyond its own transactions and experiences), which then used this information to make decisions in consumer transactions would have been a consumer reporting agency; the consumer would have had full FCRA rights, including access and dispute rights, as to that information.<sup>31</sup> Under the amendments, that is no longer the result, if notice and the opportunity to opt out are provided. Thus, a consumer who is denied a loan by Company A, based on erroneous consumer information obtained from its Affiliate Companies B and C now has no right to see and correct the information, and has a right to only a limited adverse action notice.<sup>32</sup> Stated more generally, a consumer could be repeatedly denied the benefits of obtaining credit or other services with no right to challenge the accuracy of pooled information kept in the files of a company not involved with the consumer's transaction.

---

<sup>29</sup> 15 U.S.C. § 1681a(d)(2)(A). As noted earlier, the FCRA does not in any way restrict the ability of an entity to share "transaction and experience" information with its affiliates.

<sup>30</sup> Also, the exception allows affiliates to freely share other information beyond their transactions and experiences with the consumer, including information included on a loan application, or information that one of the affiliates has obtained directly from a third party.

<sup>31</sup> Before the affiliate sharing exemption became law, Company A would have been required to notify the consumer he or she had been denied credit because of a consumer report (information other than "transaction or experience" data) received from a consumer reporting agency (Company B). The consumer would have the right to obtain a disclosure of the information maintained in Company B's file, and to dispute it if he or she believed it was inaccurate or incomplete. See footnote 19 above.

<sup>32</sup> Company A would be required only to notify the consumer of the adverse action, and that he or she has a right to make a written request for a statement of the "nature of the information" that caused the action. 15 U.S.C. § 1681m(b)(2).

#### IV. THE PRIVACY PROVISIONS OF H.R. 10

While the Commission generally supports the privacy provisions in H.R. 10, it believes that one specific additional consumer protection should be provided and that the bill's current provisions could be improved in two ways to ensure that legislation adequately protects consumers.

First, we suggest that H.R. 10's privacy protections requiring notice and opt-out before personal financial information is disclosed to nonaffiliated entities be extended to cover the disclosure of such information among *affiliated* companies.<sup>33</sup> This extension makes sense because consumers likely view different companies as separate entities, and are largely unaware of the fact or consequences of common ownership.<sup>34</sup> Thus, the distinction between the disclosure of personal financial information to an affiliated entity versus disclosure to a nonaffiliated one is not likely to be significant to consumers or to affect consumers' privacy interests in the underlying information. In sum, consumers should have the right to know about, and prevent if they so choose, transfers of sensitive personal financial data to *any* third parties, affiliated or non-affiliated.<sup>35</sup>

Next, with respect to two possible improvements to the bill, the Commission is concerned

---

<sup>33</sup> As noted above, the FCRA currently sets out a notice and opt-out mechanism for affiliate sharing of information that is not "transactions and experiences" information. As discussed *infra*, there is a need to clarify that H.R.10 does not undermine the protections currently afforded by the FCRA.

<sup>34</sup> This is particularly true as the barriers are removed between banking and other types of businesses, and as the size of those corporate families expands. In fact, given such expansion and diversification, consumers have no reason to know that the information they give to an insurance company one day may find its way into the files of a bank or securities firm, which happens to be affiliated with that insurance company, the next day.

<sup>35</sup> The Commission supports H.R. 10's notice, choice and security provisions and notes that in other contexts, it also has encouraged consideration of additional fair information practices.

with the broad exception provided for information transmitted "with the consent . . . of the consumer."<sup>36</sup> H.R. 10's notice and opt-out model for the sharing of personal financial information is already premised on the implied consent of the consumer -- if the consumer does not opt out, the consumer has impliedly consented to the information transfer -- so no additional exception for consent should be necessary. If there is a discrete need to obtain consumer consent for the sharing of the information in particular circumstances, such a need should be addressed with a more limited exception. Most importantly, any consent that overrides the privacy protections of this bill should be permitted only where there is clear and conspicuous notice to the consumer of specifically what information sharing will be permitted by their consent and a clear expression from the consumer of that consent.

Finally, the bill should make it clear that its privacy provisions do not limit the FCRA's protections to the extent they apply to financial institution files. H.R. 10's broad definition of "nonpublic personal information," which covers personally identifiable information "obtained by the financial institution,"<sup>37</sup> can include the type of information that would otherwise constitute a credit report; in fact, it could even include credit reports obtained from credit bureaus. Distribution of such information to third parties today should be subject to the full protections of the FCRA, and not just the notice and opt-out regime included in H.R. 10. If construed to supersede the FCRA, the H.R. 10 privacy provisions would be a major retreat in privacy protections for consumers. Credit reports could be distributed to firms that had no permissible purpose to see them if the consumer did not take the affirmative step of stopping that practice.

---

<sup>36</sup> Title V, Subtitle A, Section 502(a)(2).

<sup>37</sup> Title V, Subtitle A, Section 509(4)(A)(iii).

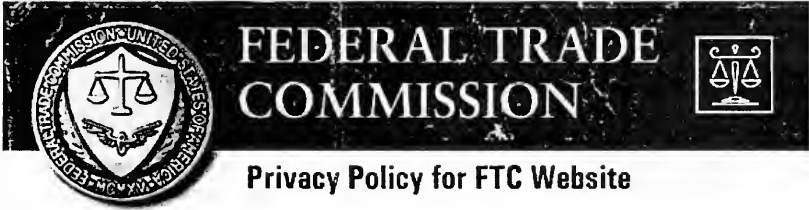
The Commission believes it essential to eliminate the potential for such an interpretation by adding a savings clause indicating that, notwithstanding any provisions of H.R. 10, the full protections of the FCRA continue to apply where applicable.

## V. CONCLUSION

It is clear that financial modernization can bring great benefits to consumers. It is also clear that consumers are extremely concerned about the privacy of their sensitive financial information. At the same time, the provision of financial services is dependent upon efficient, fair and accurate reporting of consumer credit information. A principal goal of the FCRA is to protect consumer privacy, while avoiding negative impacts on industry.<sup>38</sup> The Commission is pleased to serve as a resource as this Subcommittee and others consider how to strike the proper balance between these important competing interests.

---

<sup>38</sup> 15 U.S. C. § 1681(a).



This is how we will handle information we learn about you from your visit to our website. The information we receive depends upon what you do when visiting our site.

If you visit our site to read or download information, such as consumer brochures or press releases:

We collect and store *only* the following information about you: the name of the domain from which you access the Internet (for example, aol.com, if you are connecting from an America Online account, or princeton.edu if you are connecting from Princeton University's domain); the date and time you access our site; and the Internet address of the website from which you linked directly to our site.

We use the information we collect to measure the number of visitors to the different sections of our site, and to help us make our site more useful to visitors.

If you identify yourself by sending an E-mail:

You also may decide to send us personally-identifying information, for example, in an electronic mail message containing a complaint. We use personally-identifying information from consumers in various ways to further our consumer protection and competition activities. Visit **Talk to Us** to learn what can happen to the information you provide us when you send us e-mail.

***We want to be very clear: We will not obtain personally-identifying information about you when you visit our site, unless you choose to provide such information to us.***

[Contact Us](#)
[Search](#)
[Privacy](#)
[Complaint Form](#)
[Site Directory](#)
[Home](#)

Last Updated: Wednesday, June 16, 1999



# FEDERAL TRADE COMMISSION

WORKING FOR CONSUMER PROTECTION  
AND A COMPETITIVE MARKETPLACE

About  
[Privacy](#)



[Who We Are &  
How We Serve You](#)

Our  
[Privacy Policy](#)

## Current News Releases

[FTC Wins Case Against Defendants Engaged in Deceptive Advertising of "Super-Formula" Diet Product](#)

[Tuesday, July 20, 1999  
Children's Online Privacy  
Protection Rule: Public Workshop  
Agenda](#)



[Consumer  
Protection](#)



[Antitrust/  
Competition](#)



[Business  
Guidance](#)



[Economic  
Issues](#)



[Formal Actions,  
Opinions & Activities](#)



[News Releases,  
Publications & Speeches](#)



[Regional  
Offices](#)



[Legal  
Framework](#)

[Contact Us](#)

[Complaint Form](#)

[Search](#)

[IG's Office](#)

[Site Directory](#)

[Related Sites](#)

Last Update: Monday, July 19, 1999



Responses to Questions from Congressman Vento  
 Financial Privacy and H.R. 10  
 September 15, 1999

**Responses to Questions**

*1. Do you have the resources necessary to properly implement the provisions protecting privacy as were passed by the Commerce Committee? Would you need to have additional staffing to appropriately enforce those kinds of provisions?*

The version of H.R. 10 reported by the Commerce Committee named the Federal Trade Commission as the sole enforcer of the Act's privacy provisions. This would considerably expand the scope of this agency's responsibilities, and would be a substantial undertaking. Additional resources would be required, as we would be enforcing new obligations and extending our responsibilities to entities not previously subject to our jurisdiction.

*2. Do you see any shortcomings with the functional regulation approach to privacy protections in H.R. 10?*

The Commission supports the concept of functional regulation, both generally and as it applies to H.R. 10.<sup>1</sup> Functional regulation permits those regulators with the most expertise to regulate activities that fall under their traditional jurisdiction, and helps to ensure a level playing field as companies expand into new areas.

*3. What are your views on the affirmative responsibility to respect privacy provisions in H.R. 10?*

As stated in its testimony before the Subcommittee, the Commission supports the provisions in H.R. 10 that impose an affirmative responsibility to respect consumer privacy, but the Commission believes that these provisions should go even further to protect consumers.<sup>2</sup> Specifically, we indicated that H.R. 10's privacy protections requiring notice and opt-out before personal financial information is disclosed should be extended to cover affiliate sharing of such information, and should not be limited to third party disclosures. Also, as discussed more fully in the written testimony, the Commission believes the privacy provisions could be improved by

---

<sup>1</sup> The Commission presented its views on this topic regarding a previous version of H.R. 10. See Testimony of the Federal Trade Commission on "H.R. 10, The Financial Services Competition Act of 1997" before the Subcommittee on Finance and Hazardous Materials of the House Committee on Commerce, at 4-5 (July 17, 1997).

<sup>2</sup> Commissioner Swindle dissented from this aspect of the Commission's testimony in a separate statement.

Responses to Questions from Congressman Vento  
 Financial Privacy and H.R. 10  
 September 15, 1999

(1) eliminating or refining the broad exception provided for information transmitted with a consumer's "consent," and (2) adding a savings clause indicating that, notwithstanding any provisions of H.R. 10, the full protections of the Fair Credit Reporting Act continue to apply.

*4. The FTC advocates that rather than implementing legislation at this point, self-regulation for the Internet should be given a chance, and that we should promote the idea of educating businesses and creating incentives for them to self-regulate. Can you give any examples of these initiatives? Will this be enough to entice businesses who are not currently interested in self-regulating?*

In recent testimony before the House<sup>3</sup> and Senate,<sup>4</sup> the Commission stated that legislation to address online privacy was not appropriate at this time. The Commission's decision was based, in part, upon its review of a recent report analyzing the fair information practices of commercial Web sites, as well as industry efforts and commitment to fair information practices. For example, the private sector has undertaken several encouraging initiatives to promote self-regulation. Industry leaders like IBM, Disney and Microsoft have announced that they will no longer advertise on Web sites that do not post privacy policies. The emergence of seal programs is another promising development in self regulation. Also, ongoing consumer and business education initiatives will continue to create incentives for self regulation.

I think it likely that such private sector initiatives will encourage additional businesses to adopt fair information practices – either as part of an existing self-regulatory program or on their own. There always will be some businesses that will choose to do nothing. Over the next year, we plan to examine whether widespread adoption of fair information practices takes place online. At the same time, we will examine the quality of those practices. To accomplish these goals, the Commission has announced a series of projects that address consumer online privacy, which includes a "2000 Privacy Survey" of commercial Web sites' information disclosures.

*5. The FTC has stated that "there is considerable distance to go before consumers can feel safe from privacy invasions." If self-regulation is allowed to be the answer to this problem, what*

---

<sup>3</sup> Testimony of the Federal Trade Commission on "Self-Regulation and Privacy Online" before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Committee on Commerce (July 13, 1999). Commissioner Anthony dissented and issued a separate statement. Commissioner Swindle issued a separate concurring statement.

<sup>4</sup> Testimony of the Federal Trade Commission on "Self-Regulation and Privacy Online" before the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation (July 27, 1999). Commissioner Anthony dissented and issued a separate statement. Commissioner Swindle issued a separate concurring statement.

*specific thresholds would have to be met by the industry in order for the FTC to consider consumers "safe"?*

The FTC's 1998 survey of commercial Web sites found that only 14% of sites were providing any disclosures about their information practices. A year later, the 1999 Georgetown Internet Privacy Policy survey found that 66% of sites were providing information practice disclosures. This represents a substantial improvement, and has also helped to raise consumer awareness of online privacy issues.

I am encouraged by these numbers and hope such improvement will continue. Our 2000 Privacy Survey will measure industry's performance on this front. These numbers, however, are only part of the broader picture to provide effective privacy protections for consumers. For this reason, the upcoming survey will entail more than just a quantitative analysis. It also will look at the quality of a Web site's privacy disclosures, and staff is currently assessing standards by which the Commission may evaluate these disclosures.

*6. How does existing technology that promotes seamless transitions – back and forward features for example – on Internet surfing, work for or against privacy of the individuals surfing? How do you address [these issues]? How is information, the cookie stream, being used to market or otherwise monitor consumers?*

The Commission, together with the Department of Commerce, has been reviewing the issue of "online profiling" – the practice of aggregating information about consumers' preferences and interests gathered primarily by tracking their movements online through cookies. The information is then used to deliver targeted online ads to consumers. The Commission and the Commerce Department are planning to hold a public workshop on online profiling in early November. The goal of the workshop is to educate government officials and consumers about online profiling, to discuss the privacy implications raised by the practice, and to encourage self-regulatory efforts to implement fair information practices in this area.

We will also invite members of industry and consumer representatives to submit public comments on a series of questions related to online profiling, to help us better understand the nature of profiling technology, the costs and benefits of online profiling, and current practices with respect to fair information practices. We look forward to sharing with Congress what we learn from these efforts.

*7. How do you envision the role of the regulator in enforcing the privacy provisions of H.R. 10 once enacted into law?*

When enforcing a new law such as the privacy provisions of H.R. 10, I believe the role of the FTC is twofold. First, it is important that we focus our efforts on an educational campaign designed to inform consumers about their new rights and businesses about their new obligations under the law. Second, after allowing for a suitable time for the education efforts, the FTC should bring targeted enforcement actions, where warranted. Additionally, the FTC should play an active role in any relevant rule making undertaken in connection with the privacy provisions.



**TESTIMONY OF**

**ANNETTE L. NAZARETH, DIRECTOR  
DIVISION OF MARKET REGULATION  
U.S. SECURITIES AND EXCHANGE COMMISSION**

**CONCERNING FINANCIAL PRIVACY**

**BEFORE THE SUBCOMMITTEE ON  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
COMMITTEE ON BANKING AND FINANCIAL SERVICES**

**U.S. HOUSE OF REPRESENTATIVES**

**JULY 21, 1999**

**U. S. Securities and Exchange Commission  
450 Fifth Street, N.W.  
Washington, D.C. 20549**

**TESTIMONY OF**

**ANNETTE L. NAZARETH  
DIRECTOR OF MARKET REGULATION  
U.S. SECURITIES AND EXCHANGE COMMISSION**

**CONCERNING FINANCIAL PRIVACY**

**BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS  
AND CONSUMER CREDIT**

**COMMITTEE ON BANKING AND FINANCIAL SERVICES**

**U.S. HOUSE OF REPRESENTATIVES**

**JULY 21, 1999**

Chairwoman Roukema, Congressman Vento, and Members of the Subcommittee:

I am pleased to testify today on behalf of the Securities and Exchange Commission (the "Commission" or "SEC") regarding financial privacy. The Commission supports the legislative efforts that are currently being made to enhance financial privacy. Americans generally expect that their financial transactions -- and their financial information -- to be private. This expectation exists across the broad range of financial services -- not just in the securities business. Meeting this expectation of privacy is one way that providers of financial services demonstrate their own integrity and earn their customers' and clients' confidence. That confidence is essential to the continued success of all financial services providers, including those that the Commission regulates.

## I. Background

Americans always have placed a great deal of importance on privacy. As Justice Brandeis noted many years ago, privacy is “the most comprehensive of all rights and the right most cherished by a free people.”<sup>1</sup>

A number of factors have converged in recent years to bring discussions about the importance of privacy -- and in particular, financial privacy -- to the forefront. The exponential growth in electronic commerce, and in technology, means that more information can be collected than ever before. Moreover, that information can be stored, sorted, and analyzed quickly and cost effectively. The effects of living in the Information Age can be seen throughout our daily lives. Even grocery stores track our purchases in order to target their marketing efforts.

As we all know, privacy concerns are not just domestic. In the international sphere, the European Union’s Directive concerning data protection -- and U.S. efforts to respond to it -- have heightened the need to address concerns about protecting personal data, including financial data.

Financial modernization and the burgeoning merger activity among banks, securities firms, and insurance companies have heightened interest in the need to protect financial privacy. Mergers of large companies can result in huge databases of customer information. We’ve all read the recent media reports of financial institutions sharing -- or

---

<sup>1</sup> Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” 4 Harv. L. Rev. 193 (1890).

even selling -- their personal customer information.<sup>2</sup> Moreover, we recognize the risk that a financial institution may inadvertently disclose financial information just because it lacks adequate controls.<sup>3</sup>

There is, however, another side of this coin. Financial institutions often have a legitimate need to share personal financial information. A good example of this is credit checks. Another example is when a customer does business with two affiliated companies and the companies share information in order to save the customer time and trouble.

So what is the difference between legitimate information sharing and violations of customers' privacy? The key here is the customer's expectations. If a bank customer opens a bank account linked with a securities account offered by the bank's securities affiliate, the customer would reasonably expect for the bank to share information with the

---

<sup>2</sup> On June 9, 1999, the State of Minnesota sued Minneapolis-based U.S. Bancorp for allegedly violating the federal Fair Credit Reporting Act, as well as state consumer fraud and deceptive advertising practices laws for selling customer information to Member Works, Inc., a seller of memberships in discount health programs, in exchange for \$4 million plus 22% of sales.

<sup>3</sup> The practice of "pretexting" (i.e., obtaining private financial information from banks and others under false pretenses) has been on the increase. Pretexting has been used to effect "financial identity theft," which occurs when someone uses the identifying information of another person -- the name, Social Security number, mother's maiden name, or other financial information -- to commit fraud or otherwise engage in other unlawful activities. Using account balances and numbers obtained from a pretexer, an identity thief could deplete a bank account or liquidate a stock portfolio. See "The Federal Trade Commission on Financial Identity Theft," Prepared Statement of Joan Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, before the House Commerce Committee, Telecommunications, Trade and Consumer Protection Subcommittee, and Finance and Hazardous Materials Subcommittee, April 22, 1999.

securities affiliate. The customer might not, however, expect the bank to share this same information with a third party that was marketing other financial services.<sup>4</sup>

In the past, customary business practice came much closer to matching customer expectations. It was just too expensive to gather and transmit data in the pre-computer age. Moreover, many businesses had the incentive to keep their customer information from others. While those incentives are still valid today, consolidation of financial services businesses has made them less critical.

As Congress considers the issues inherent in reforming financial services regulation, it is appropriate for Congress and financial regulators to evaluate how to ensure that the expectations of privacy of financial services customers will be met.

## **II. Privacy and the Securities Regulatory Scheme**

Although the federal securities laws do not contain an express requirement for registered broker-dealers, investment advisers, or investment companies to safeguard the personal financial information of their customers and clients, the Commission has reminded these entities that, as financial professionals, they should protect this

---

<sup>4</sup> Customers also might not expect the bank to share the information with affiliates for marketing purposes. See e.g., In the Matter of NationsSecurities and NationsBank, N.A., Securities Act Release No. 7532 (May 4, 1998). In that case, employees of a bank provided its affiliated broker-dealer with maturing CD lists and lists of likely prospective investors. The broker-dealer's employees also received other bank customer information such as financial statements and account balances. Those broker-dealer employees then used that information to target bank customers for securities purchases, and in so doing, mischaracterized the nature of the investments sold. As a result, many elderly customers were moved from bank CDs to high-risk mutual funds or other unsuitable investments. In settling the Commission's enforcement action for violations of the antifraud provisions of the federal securities laws, the defendants paid a civil penalty of \$4 million.



information.<sup>5</sup> In particular, the Commission has stated that broker-dealers, transfer agents, investment companies and investment advisers should take reasonable precautions to ensure the integrity, confidentiality, and security of personal financial information when it is delivered through electronic means.<sup>6</sup>

In addition to being regulated by the Commission, broker-dealers are regulated by securities self-regulatory organizations ("SROs"). We believe that SROs, which are required to have rules to promote just and equitable principles of trade, have the authority to address privacy concerns. SROs have used this authority to bring disciplinary actions. For example, one SRO censured a registered representative and barred him from the industry for, among other things, improperly disclosing customer account information that was used to withdraw funds from the customer's account without the customer's knowledge. In imposing these sanctions, the SRO found the registered representative's conduct was inconsistent with just and equitable principles of trade.<sup>7</sup> Of course, misuse of customer information may also be an element of fraud.

---

<sup>5</sup> Securities Exchange Act Release No. 37182 (May 9, 1996), 61 FR 24652 (May 15, 1996).

<sup>6</sup> Id.

<sup>7</sup> In re Albert Anthony Dello Russo, New York Stock Exchange Panel Decision 96-23 (March 5, 1996).

### **III. Description of H.R. 10 Proposal**

The privacy provisions in Title V of H.R. 10 are an important first step in rationalizing the current patchwork scheme of privacy protection.<sup>8</sup> In general, these provisions would impose an affirmative and continuing obligation on financial institutions to respect their customers' privacy, and to protect the security and confidentiality of those customers' nonpublic personal information. While the provisions would permit information sharing between affiliates and agents of financial institutions, they would restrict the disclosure of nonpublic personal information to unaffiliated third-parties.

Among other things:

- All financial institutions would be required to disclose their practices and policies with regard to protecting the consumer's non-public personal information. Financial institutions are broadly defined and would include brokers-dealers, investment companies, investment advisers, banks, thrifts, savings and loans, insurance companies, among others.
- All financial institutions would be required to disclose their practices and would be limited. Among other things, consumers would have to be notified, and given the opportunity to opt-out, of the disclosure before the disclosure occurs. Certain disclosures would be exempted from this requirement, including disclosures to third parties that provide services or functions on behalf of financial institutions. Disclosure of customer

---

<sup>8</sup> An appendix discussing current federal and state laws that affect how securities firms handle personal financial information is attached.

financial data to non-affiliated third parties for marketing purposes, however, would be prohibited.

Financial institution regulators would be required to jointly issue rules to implement these provisions.

#### **IV. Comments on H.R. 10's Privacy Proposal**

H.R. 10 is an important step forward in creating a consistent, enforceable privacy protection framework for American investors. We support requiring financial institutions to disclose their privacy policies to their customers and prospective customers. In receiving this notice, investors would have the ability to choose among firms based on their personal priorities.<sup>9</sup> We are also sympathetic to giving customers the ability to decide whether their personal financial information will be shared, even among affiliates, and particularly when it is to be used for marketing purposes.

Any legislative proposal to heighten financial privacy protections needs to balance a number of concerns. First, information sharing may be necessary for a financial services provider to be able to do its job. A broker-dealer, for example, must be able to share elements of its customers' personal financial information with other brokers or clearing agencies in order to clear and settle trades. Information sharing can also be a cost-saving device for financial services providers. As firms consolidate, they enjoy many efficiencies of scale, including the ability to avoid duplicative information gathering. Customers, as well as firms, can benefit from these efficiencies. Customers, however, should know when

---

<sup>9</sup> We presume, however, that any legislation adopted by Congress would include provisions that ensure that any new protections enacted would not interrupt the ability of the Commission or the SROs to obtain the information we need to carry out our regulatory mandates.

their personal information is going to be shared, and they should have a voice in saying how far that information should go.

The Commission also strongly supports an exception for information shared in the context of executing transactions. Elements of apparently seamless securities transactions often involve parties that must share customer information in order to continue to provide the services customers have come to expect. Depending on the size and the structure of the firm involved, these parties may or may not be affiliated. For example, a customer's purchase of shares in a mutual fund may involve a sharing of functions among an investment company, an investment adviser, a fund administrator, a distributor, and a transfer agent. A purchase of an equity security from a broker may involve an introducing broker, a clearing broker, a transfer agent and a depository. Depending on the particular circumstances of a transaction, any of these parties may or may not receive customer information and may or may not be affiliated with the originating organization.

In addition, we note that there are various technical issues contained in H.R. 10's privacy provisions that will need to be addressed if H.R. 10 becomes law. In particular, the SEC and SROs need clear and express authority to enforce the privacy provisions and rules applicable to securities firms. The bill currently is unclear whether enforcement authority is shared with the Comptroller of the Currency and the Office of Thrift Supervision. For broker-dealers that are subsidiaries of national banks and savings associations, respectively, we believe that enforcement authority over the broker-dealer affiliate should be allocated solely to the Commission. Similarly, we believe that the system for joint rulemaking by the federal regulators with a six-month deadline is

unrealistic, given the number of agencies involved in the joint rulemaking, the requirement of consultation with the FTC and state insurance authorities, and the requirements of the Administrative Procedure Act.

**VII. Conclusion**

I appreciate the opportunity to provide this testimony on behalf of the Commission. The issues that you are considering here today are important. While the decisions you make will affect all segments of the financial system -- from large corporations to small investors -- we believe that the key concern is to meet the reasonable expectations of individual investors, policy holders, and bank customers, both in terms of privacy and in terms of efficiency and service. We support the efforts of this Subcommittee to address this important issue. We would be happy to work with you and your staff going forward in addressing issues relating to the SEC, investors and the securities industry generally.

**APPENDIX**

As described below, a limited framework of privacy protection currently exists under both Federal and State laws that applies to securities firms and other financial services firms. We also include a discussion of the European Union (“EU”) Privacy Directive.

**I. Federal Laws Applicable to Securities Firms and Other Financial Institutions**

Outside of the federal securities regulatory scheme, a number of existing laws apply privacy restrictions to certain aspects of the securities industry’s business. At the federal level, Congress has enacted the Identity Theft and Assumption Deterrence Act of 1998 (“ITAD”), the Right to Financial Privacy Act of 1978 (“RFPA”), the Electronic Fund Transfer Act (“EFTA”) (also enacted in 1978), and the Fair Credit Reporting Act of 1970 (“FCRA”). States have also addressed consumers’ right to financial privacy. The scope of privacy rights conferred by these laws, however, is limited.

**The Identity Theft and Assumption Deterrence Act of 1998**

Through the ITAD,<sup>1</sup> Congress amended 18 U.S.C. § 1028(a)(7) to criminalize the knowing and wrongful use or intended use of another’s means of identification to commit a crime. The ITAD defined “means of identification” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual.”<sup>2</sup> Social Security numbers, fingerprints, and electronic addresses are included in the

---

<sup>1</sup> Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

<sup>2</sup> 18 U.S.C. § 1028(d)(3).

definition. In passing this law, Congress attempted to address the privacy concerns specific to the technological information age.

### The Right to Financial Privacy Act

The RFPA<sup>3</sup> was enacted in response to the Supreme Court's decision in United States v. Miller.<sup>4</sup> In Miller, the Court held that a criminal defendant could not raise a Fourth Amendment challenge to the government's improper seizure of records from his bank (e.g., copies of checks, deposit slips, monthly statements), because a bank depositor has no legitimate expectation of privacy in these records.

Enacted to redress the lack of constitutional protection for these records, the RFPA imposes some constraints and procedural requirements on the *federal* government's collection of the financial records of a financial institution's customers. Notably, however, the RFPA restricts only the federal government; it imposes no restrictions on a bank's or securities firm's disclosure or sale of information to state or local governments or to private parties.

The RFPA restricts the federal government's access to a financial institution's customer information without the written consent of the customer or a valid subpoena, summons, search warrant, or formal written request. Except for search warrants, the RFPA also requires that the government give the customer advance notice of its intentions and a chance to challenge the government's access to the records. The RFPA also

---

<sup>3</sup> Pub. L. No. 95-630, tit. XI, 92 Stat. 3641, 3697-3710 (1978) (codified as amended at 12 U.S.C. §§ 3401-22).

<sup>4</sup> 425 U.S. 435 (1976).

prohibits financial institutions from releasing customer information to the government unless the government certifies in writing that it has complied with the RFPA.

### **The Electronic Fund Transfer Act**

The EFTA,<sup>5</sup> enacted in 1978, was another effort to address problems specific to technological advances. The EFTA provides a framework for governing the use of electronic fund transfers. A financial institution must tell its customers, to the extent applicable, under what circumstances it "will in the ordinary course of business disclose information concerning the consumer's account to third persons."<sup>6</sup> Further, similar to the ITAD, this statute imposes criminal liability on any person who knowingly uses, attempts to use, or conspires to use a wrongfully obtained debit instrument. Significantly, however, transactions to purchase or sell securities or commodities through a broker-dealer are exempt from the definition of "electronic fund transfer" and, therefore, are not subject to the requirements of the EFTA.

### **The Fair Credit Reporting Act**

The FCRA was enacted to redress perceived abuses in the credit reporting industry. A 1993 Senate Report described that industry as follows:

The credit reporting industry is centered around consumer reporting agencies, which collect and sell information concerning the credit histories and financial status of 90 percent of all Americans. Much of this information is submitted by credit providers, such as banks and finance companies, which obtain this information from their experience with individual consumers. The agencies also collect items of public record, such as arrests, lawsuits, and legal judgments.

---

<sup>5</sup> Pub. L. No. 95-630, tit. XX, 92 Stat. 3641, 3728-41 (1978) (codified at 15 U.S.C. §§ 1693 to 1693r).

<sup>6</sup> Id. at §1693c(a)(9).



The consumer reporting agencies sell the information from their files to their customers. Customers include retailers, insurance companies, lenders, businesses that sell mailing lists, prospective employers, and government agencies. Thus, a consumer report can be a decisive factor in whether a consumer's application for credit, an apartment, a job, or insurance will be accepted or rejected.<sup>7</sup>

In general, the FCRA imposes restrictions on a consumer reporting agency's provision of consumer reports to others. Entities engaged in this business must meet certain minimum standards designed to ensure that credit reports contain accurate and current information. The FCRA also guarantees consumers access to their credit reports, provides consumers with the right to dispute their credit report (including a mechanism to do so), and imposes penalties for its violation.

The entities and reports covered by the FCRA are, however, narrowly limited. It only applies to "consumer reporting agenc[ies]," and only to their furnishing of "consumer report[s]."<sup>8</sup> Each of these phrases receives a detailed definition in the FCRA. "[C]onsumer reporting agency" generally means "any person which . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."<sup>9</sup> "Consumer report," in turn, is given a lengthy definition, generally covering reports on consumers' creditworthiness.<sup>10</sup> Significantly, however, the phrase does not

---

<sup>7</sup> See S. Rep. No. 103-209, at 1 (1993).

<sup>8</sup> 15 U.S.C. § 1681a(d), (f).

<sup>9</sup> 15 U.S.C. § 1681a(f).

<sup>10</sup> See 15 U.S.C. § 1681a(d).

include any report containing information solely as to transactions or experiences between the consumer and the person making the report. This category is often referred to as “experience information.” Relying on the exception for “experience information” and the definition of “consumer reporting agency,” a number of courts have held that the FCRA is inapplicable to banks providing outside parties with adverse credit information on their customers.

The FCRA was amended in 1996, to replace the broad “legitimate business need” exception with a more restrictive one.<sup>11</sup> Under the amended law, credit reports can be disclosed only to a person that the consumer reporting agency has reason to believe “has a legitimate business need for the information: (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an account to determine whether the consumer continues to meet the terms of the account.”<sup>12</sup>

The “experience information” exception, however, was expanded. The FCRA now excepts from the definition of “consumer report” not only “any report containing information solely as to transactions or experiences between the consumer and the person making the report,” but also “communication of that information among persons related by common ownership or affiliated by corporate control.”<sup>13</sup> Thus, even if a bank qualifies

---

<sup>11</sup> Pub. L. No. 104-208, Div. A, tit. II, §§ 2403-05, 2420, 110 Stat. 3009, 3009-430 to -434, 3009-454 (1996).

<sup>12</sup> 15 U.S.C. § 1681b(a)(3)(F).

<sup>13</sup> 15 U.S.C. § 1681a(d)(2)(A)(i) & (ii). We note that courts have not interpreted this exception.

as a “consumer reporting agency,” it may disclose information about its customers to an affiliate.

The same analysis applies to securities firms. Broker-dealers may disclose information about their customers to an affiliate because they collect private information through “transactions or experiences” (e.g., customers who open margin trading accounts). Moreover, broker-dealers are generally not in the business of providing such information in the form of consumer reports to third parties. Thus, NASD Notice to Members 97-12 explained that under the amended provisions “an entity may share without limitation ‘experience information’ (*i.e.*, information derived from transactions or experiences with the consumer) with both affiliates and non-affiliates without becoming subject to the FCRA.”<sup>14</sup>

#### Other Federal Statutes

Financial institutions also may be affected by other federal statutes, including the Fair Credit Billing Act<sup>15</sup> (restricting reporting of amounts a consumer disputes as delinquent to a third party), and the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991 (“Act”)<sup>16</sup> (authorizing the Federal Trade Commission (“FTC”) to regulate the conditions under which telemarketers may contact consumers).<sup>17</sup> Generally

---

<sup>14</sup> NASD Regulation Request for Comment, 97-12 (Mar. 1997).

<sup>15</sup> 15 U.S.C. §1666-1666j.

<sup>16</sup> 15 U.S.C. §§ 6101-6108.

<sup>17</sup> Although persons involved in the securities industry, such as brokers and investment advisers, are exempt from any such FTC rule, the Act required that the SEC adopt, for the securities industry, rules similar to those set by the FTC. At the request of the SEC, major self-regulatory organizations (“SROs”) have

speaking, the FTC, pursuant to the Federal Trade Commission Act, and the States play an important role in regulating activity that may abuse consumer privacy.

## II. State Privacy Statutes

Many states appear to have some statute governing the financial privacy of individuals. The content of these statutes varies. Like the RFPA, many states' statutes govern only disclosure to government authorities -- that is, state and local government authorities.<sup>18</sup> Other states -- including Connecticut, Illinois, Maine and Maryland -- appear to have financial privacy statutes that cover disclosures to private as well as governmental entities.<sup>19</sup> These statutes restrict disclosure of confidential financial information except to the customer or the customer's agent.

The types of financial privacy statutes in effect in other states vary widely. Some states have laws resembling the federal EFTA and RFPA laws. Some states, notably California, have privacy guarantees in their state constitutions. In addition, common law doctrines, such as invasion of privacy, defamation, and implied contract, may recognize certain privacy protection for financial records.

## III. European Union Data Protection Directive

Privacy concerns also have emerged recently in the international context. The EU's 1995 enactment of a Directive on Data Protection ("DPD"), when fully

---

changed their rules to correspond to those of the FTC. See Exchange Act Release No. 39010, at 4-5.

<sup>18</sup> L. Richard Fischer, *The Law of Financial Privacy* 5-37 (2d ed. 1991).

<sup>19</sup> Id.

implemented, will apply to U.S. securities firms doing business in the EU.<sup>20</sup> Article 1 sets forth a comprehensive system by which EU member states are obligated to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Article 2(a) of the DPD defines "personal data" as any information concerning a person who can be identified by reference specific to his economic identity, among other factors.<sup>21</sup> Each EU member country is required to enact laws that implement the DPD.

Significantly, part of the system to protect the privacy of EU citizens is a prohibition on the transfer by EU entities of personal data to third countries whose privacy protections are deemed inadequate.<sup>22</sup> The DPD applies to any company that receives or transfers personal data from the EU, including internationally active U.S. broker-dealers, investment advisers, investment companies, and banks. If EU member countries determine that privacy protections in the U.S. do not meet their standards for adequacy, the flow to the U.S. of personal data about EU citizens, including personal financial information, could be restricted. Such restrictions could impair the ability of U.S. financial services entities to function fully in the global market.

---

<sup>20</sup> Council Directive 95/46/EC of 24 October 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter "DPD"].

<sup>21</sup> DPD, art. 2(a).

<sup>22</sup> DPD, art. 25.

The DPD contains a number of exemptions<sup>23</sup> and derogations<sup>24</sup> from the transfer restriction, including exceptions for: data flow necessary for the performance of a contract, data flow pursuant to the consent of the data subject, data flow necessary or legally required on important public interest grounds or for legal action, data flow that protects the vital interests of the data subject, and data that is already a part of the public record.

The Department of Commerce has the lead role in negotiating with the EU on behalf of the U.S. Government with respect to the effects of the DPD on U.S. entities. The DPD became effective in October 1998. The U.S. and EU have agreed, however, that data flows to the U.S. would not be interrupted during negotiations.

To date, the EU-US negotiations have focused on a self-regulatory model that would address EU concerns. On November 4, 1998, the Department of Commerce introduced to the U.S. industry a set of draft privacy principles that were meant to serve as a safe harbor from the DPD.<sup>25</sup> Commerce issued those draft International Safe Harbor Privacy Principles under its statutory authority to foster international commerce. The intended goal of the safe harbor is that a U.S. entity that voluntarily complies with the principles will be presumed by the EU to have adequate privacy protections for personal

---

<sup>23</sup> DPD, art. 13.

<sup>24</sup> DPD, art. 26(1).

<sup>25</sup> Draft International Safe Harbor Privacy Principles (Apr. 19, 1999) <<http://www.ita.doc.gov/ecom/shprin.html>>. The principles were revised as of April 9, 1999.

data.<sup>26</sup> Provision of personal data to such an entity would not be arrested as long as the it self-certifies to compliance. We understand that these principles would apply to the financial services industry.

The draft International Safe Harbor Privacy Principles<sup>27</sup> are:

- Notice. When individuals first provide personal information to an organization, the organization must provide them with clear and conspicuous notice about the type of personal information that the organization collects, how the information is collected, the purpose for the data collection, to whom the information will be disclosed and the methods by which the organization allows individuals to limit the use and disclosure of the information.
  - Choice. Individuals must have the opportunity to choose to opt out of the organization's use of their personal information for a matter unrelated to the original use for which the information was initially disclosed.
- Organizations must, with respect to the use of sensitive information, such

---

<sup>26</sup> Organizations may also qualify for the safe harbor if they are subject to, and their activities are governed by, a "US statutory, regulatory, administrative or other body of law (or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that also effectively protects personal data privacy." Draft International Safe Harbor Privacy Principles (Apr. 19, 1999) <<http://www.ita.doc.gov/ecom/shprin.html>>.

<sup>27</sup> Draft International Safe Harbor Privacy Principles (Apr. 19, 1999) <<http://www.ita.doc.gov/ecom/shprin.html>>.

as medical information, allow individuals an opportunity to affirmatively opt in.

- **Onward Transfer.** Organizations must give individuals notice and the right to choose whether and how the organization transfers their personal information to a third party. When an individual is not provided with a choice because the transfer is related to the original use of the information, the third party must provide the same privacy protections as the individual received from the original recipient organization.
- **Security.** Organizations must take reasonable precautions to protect the information they collect concerning an individual from loss, misuse, disclosure, or other breaches of security.
- **Data Integrity.** Organizations must take reasonable measures to keep data accurate, complete and up-to-date, and may process data only for the intended use.
- **Access.** Individuals must have the right to reasonable access to personal data that an organization collects about them.
- **Enforcement.** Privacy protection must include methods to verify organizations' claims about their privacy policies, recourse methods to resolve individuals' complaints and disputes, and methods of remediating problems and consequences for non-compliance with the principles.



We understand that the Department of Commerce and the EU Directorate General XV, while having identified substantial common ground, continue to negotiate on the parameters of the safe harbor and its application.<sup>28</sup>

---

<sup>28</sup> The EU, however, has rejected the notion that the financial services industry should be deemed to meet the requirements of the safe harbor just because they are “heavily regulated.” David L. Aaron, Under Secretary of Commerce for International Trade, “Enabling Privacy in a Virtual World,” Address at the Smart Card Forum Symposium (May 20, 1999).

Testimony of the  
National Association of Insurance Commissioners

before the  
Committee on Banking and Financial Services  
Subcommittee on Financial Institutions  
and Consumer Credit  
United States House of Representatives

regarding  
Financial Privacy

July 21, 1999

George M. Reider, Jr.  
Insurance Commissioner  
Connecticut

## **Testimony of George M. Reider, Jr. National Association of Insurance Commissioners**

### **Introduction**

Good morning, Madam Chairwoman and members of the Subcommittee. My name is George Reider, and I serve as Insurance Commissioner in Connecticut. I also serve as President of the National Association of Insurance Commissioners (NAIC). I am testifying today on behalf of the NAIC, which is the national organization of the chief insurance regulators of the 50 States, the District of Columbia and four U.S. territories.

I am pleased to be here to testify on financial privacy issues, a matter of increasing importance as the integration of financial services industries becomes a reality, and as technology makes the sharing of information ever easier.

At a time when it seems that anyone can retrieve your financial information at the click of a button, it is important for consumers to know that protections are in place so their personal financial information is not unfairly used. At the same time, regulation should not unreasonably stifle the flow of information necessary to the operations of the insurance companies, banks and securities firms that provide our financial services.

It is this balancing act that is difficult. The challenge for Congress and the States is to determine how much disclosure is acceptable so that companies can do business, regulators can enforce the laws, and consumers' personal financial information is protected.

### **Privacy Means Keeping Personal Information Confidential and Protecting the Integrity of the Regulatory System**

- **Keeping Personal Information Confidential**

Protecting privacy means keeping personal information confidential. It means taking into consideration consumers' needs and wishes before sharing or disclosing their personal information.

People legitimately expect that companies holding personal information will not use it to take unfair advantage of them. At the same time, consumers are realistic. They understand that disclosure of some of their information is necessary for typical business needs like billing and record keeping. And they know that

sometimes disclosure of information can result in real advantages for them, in the form of cost savings and convenience, for example.

- **Protecting the Integrity of the Regulatory System**

Protecting privacy also entails protecting the integrity of the regulatory system. People must have confidence that information is being used correctly to protect them. They have a right to know that the government will not use their personal information unfairly, that their personal information is secure, and that it will not get into the wrong hands

Financial integration heightens the need for the protection of regulatory information. As insurers, securities firms and banks converge, State and Federal regulators will increasingly need to share information to do their jobs successfully. Protections need to be in place to ensure that such cooperation does not compromise the integrity of the regulatory system.

### **There are Two Sides to Maintaining Privacy – Commercial and Governmental**

Like banks and securities firms, insurers collect and have access to personal financial information about their customers. Similarly, State insurance regulators possess a significant amount of personal financial information about the insurance consumers in their States. Both face the need to share information in order to do business the right way, but both must also protect consumers.

Why is personal information shared? Companies believe that sharing information with affiliates or third parties will enable them to provide the services that their customers need in an efficient, cost effective manner. Regulators need to share information to more effectively supervise the industries they regulate in order to protect the public – collectively and individually – from fraud and abuse.

### **Here is what the NAIC and the States are doing to Assure that Insurance Companies and Agents will Protect Personal Financial Information.**

The States have long recognized the need to protect consumers from the unfair use of personal information. In my home State of Connecticut, for example, we have enacted a comprehensive insurance information privacy law based upon the NAIC's Insurance Information and Privacy Protection Model Act. We also have laws designed to protect personal information in connection with bank insurance sales activities and health information records. We are constantly working with our fellow States through the NAIC to monitor insurance privacy issues and assess the need for further action.

- **The Insurance Information and Privacy Protection Model Act**

In its Insurance Information and Privacy Protection Model Act, the NAIC has established standards for the collection, use, and disclosure of information gathered in connection with insurance transactions. The model law has been enacted in whole or part by 19 States.

The act is broad in scope. It applies to life, health, disability, and property and casualty insurers, as well as to agents and third party insurance support organizations. It covers all types of insurance information, including personal financial information. The act seeks to maintain a balance between the need by insurance companies and agents for information and the need of consumers for fairness in insurance information practices.

The principal provisions of the act:

- (i) require insurers to disclose their privacy policies to customers;
- (ii) give consumers the right to prohibit the disclosure of information, except under certain specified circumstances;
- (iii) outlaw pretext interviews, which is the soliciting or obtaining of personal information by false pretenses, unless fraud is suspected; and
- (iv) give consumers access to their personal information and the right to correct inaccuracies in such information.

- **Connecticut's Insurance Sales Privacy Law**

In addition to its comprehensive privacy law, Connecticut has specifically addressed the sharing of financial and other insurance information by banks that sell insurance and annuities. Like the privacy law, the insurance sales law requires the prior written consent of the customer before the bank may share personal information. It further requires a consumer's prior written consent before a bank may provide personal information to a third party in connection with the third party's solicitation or sale of insurance to such consumer.

- **Health Information Privacy in Connecticut**

In Connecticut, we have also recently strengthened our laws protecting medical-record information. Disclosure of medical-record information is prohibited for marketing purposes without the prior written consent of the individual.

- **Health Information Privacy Model Act**

In September 1998, the NAIC adopted the Health Information Privacy Model Act, which addresses health issues more specifically than the more general Insurance Information and Privacy Protection Model Act. The health privacy model act gives health insurance consumers the right to access and amend their protected health information, and requires consumer consent prior to the disclosure of such information.

**Here is what the NAIC and the States are doing to Assure that Regulators Protect Confidential Information**

The States possess a great deal of personal information about their citizens. Many States have enacted generally applicable laws – such as privacy or freedom of information laws – that address this issue. The State of New York, for example, has enacted the Personal Privacy Protection Law. The New York law limits the ability of State agencies to disclose personal information. It also gives individuals the right to see personal information held by State agencies, and correct inaccuracies in such information.

The States and the NAIC are addressing this issue on two other fronts:

- (i) We are revising confidentiality provisions in NAIC model laws; and
- (ii) We are addressing confidentiality issues in regulatory information exchanges with other regulators.

- **The NAIC's Regulatory Confidentiality Initiative**

The NAIC is in the midst of a Regulatory Confidentiality Initiative that was instituted at the beginning of this year. The purpose of the Initiative is to amend all applicable NAIC model laws to strengthen the ability of State insurance regulators to keep sensitive regulatory information confidential. This will help preserve the privacy of individuals and entities, in addition to providing a strong platform for States to use in entering into confidentiality agreements with State, Federal and international regulators.

The Confidentiality Initiative is scheduled to be completed by the end of this year, at which time the revised model laws will be ready for consideration and adoption by the States.

- **Information Sharing Among Regulators**

State insurance regulators are also working closely with our fellow regulators, including some of the Federal agencies represented by the distinguished members of this panel. Our goal is to ensure that financial services consumers continue to receive the same level of protection in the new world of financial integration that they have relied upon for years. State insurance regulators and Federal banking regulators have held joint training and education sessions, and are developing formal written agreements for cooperating and exchanging information on regulatory matters.

The NAIC recently approved a model consumer complaint information sharing agreement jointly developed with the Office of the Comptroller of the Currency (OCC). The purpose of this model agreement is to ensure that consumer complaints about bank sales of insurance are routed to the appropriate regulator. Ten States have already implemented agreements based on the model, and several other States are scheduled to sign such agreements in the coming weeks.

The NAIC is also working with the Office of Thrift Supervision (OTS) and the Conference of State Bank Supervisors (CSBS) to develop regulatory cooperation agreements. These agreements cover information sharing and cooperation on a broader range of consumer complaint, examination and enforcement matters. We expect them to be completed soon. Like the consumer complaint agreement with the OCC, they will serve as models for individual States to use as a basis for establishing ongoing working relationships with OTS and State bank regulators.

The OCC agreement and the agreements under development with the OTS and State bank regulators have strong confidentiality provisions making it clear that confidential information is to be protected to the fullest extent possible. This language not only protects consumers, but also protects companies, agents and other entities engaged in the business of insurance who may be the subject of shared regulatory information.

### **Congress Should Consider Improvements to Facilitate the Protection of Confidential Regulatory Information**

Congress should consider adopting the following proposals, which would strengthen the ability of State insurance regulators to protect the privacy of personal and financial information in their possession.

- 1. Protect the confidentiality of regulatory communications among NAIC, State regulators, and Federal agencies.**

Federal law should clearly state that confidential information can be exchanged between State insurance regulators and Federal agencies. Such protections may also extend to communications with international regulators.

**2. Provide State insurance regulators and NAIC with access to the national criminal history database (NCIC) for regulatory purposes and for checking criminal histories as required by the Federal Insurance Fraud Prevention Act.**

Protecting the integrity of private information in the insurance system means guarding against fraud and abuse.

State licensing, fraud, and enforcement staff have long sought access to the criminal history databases maintained by the FBI (usually referred to as NCIC access). The Department of Justice supplies criminal history information to the American Bankers Association so banks can run checks on employees, and also supplies the information to the securities and commodities trading industries. However, the Justice Department has not been willing to extend such authority to State insurance regulators, despite years of discussions.

Only a few States are currently able to access NCIC. In the remainder, enforcement personnel have no practical way to check the possible criminal background of an individual, even when they suspect a serious violation of law. Statistics from the few States which are able to run criminal history checks show that between 10 and 15 percent of agent applicants conceal criminal convictions on their applications.

Under the Federal Insurance Fraud Prevention Act (18 USC 1033), a person with a felony conviction involving dishonesty or breach of trust is barred from the business of insurance unless they have a specific exemption from a State insurance regulator. Insurance companies also have a duty not to employ convicted felons, but there is no reasonable means for them to check the criminal records of job applicants and employees.

Giving authority to the NAIC to obtain criminal records checks would provide a single mechanism for regulators and insurance companies to comply with their legal obligations, and would not overburden the FBI with multiple points of contact. The industry generally, as well as the Insurance Regulatory Information Network (IRIN) Board, support this goal.

**3. Grant Federal immunity from liability for NAIC and IRIN database activities.**

Protecting the integrity of the regulatory system means States, and entities acting on their behalf, must be able to maintain the privacy of confidential information without the threat of frivolous lawsuits.



Major financial and enforcement regulatory databases for insurance are all maintained by the NAIC. Key licensing data is supplied by the States to the producer database, which is part of IRIN.

Although NAIC and IRIN act on behalf of State governmental entities, they have no direct tort immunity from suit. This exposes IRIN and NAIC to potential legal actions. A number of States grant immunity to the NAIC, but this does not cover all potential suits; a plaintiff could simply file in a different State. Federal immunity would permit NAIC and IRIN funds to be spent for their intended purposes, not on lawsuits. Immunity would extend to the NAIC as an entity, as well as its members, officers, and employees.

**4. Grant exemptions from the Fair Credit Reporting Act for IRIN, the NAIC, and State insurance departments regarding regulatory licensing activities and related databases.**

State regulators' ability to protect privacy can be hampered by expansive interpretations of Federal regulations.

Recent amendments to the Fair Credit Act extended its provisions to databases not typically a part of the credit rating process. These amendments apply to databases used for both credit rating and employment purposes. Expansive interpretations by the Fair Trade Commission have extended the Act even to situations involving administrative licensing. The Act, if it were determined to apply to IRIN, would impose extensive notice and appeal requirements, just as if IRIN were a credit bureau. The solution to these problems is simple – State insurance regulatory activities should be specifically exempted from the Act.

**5. Authorize the use of social security numbers for licensing purposes, for the NAIC producer database, and for use by the Insurance Regulatory Information Network (IRIN).**

Accurate identification of individuals is a key part of maintaining privacy.

The use of social security numbers (SSN's) is restricted under the Federal Privacy Act of 1974. Most States have found ways to supply social security numbers for the producer data base, but a few States still have significant problems. Use of SSN's is the minimum element needed for properly identifying agents. A specific clarification in federal law would resolve any problems relating to use of SSN's for insurance regulatory purposes.

**6. Facilitate the use of regulatory databases, including digital signatures, acceptance of credit cards, and electronic funds transfers.**

Advances in technology provide opportunities to improve privacy protections.

Implementation of efficient electronic processing faces many hurdles, including various State requirements on how payments can be made, and what form of signatures will be accepted. Many of these requirements are in State laws or regulations outside the control of the insurance departments.

In some States, for example, no payments via credit cards can be made. Some require payment with each transaction, even if there are multiple transactions per day with one entity. Other States will bill periodically. Technology exists to use both electronic funds transfers and digital signatures, which would make many transactions more feasible and cost-effective.

**WRITTEN STATEMENT  
OF  
L. RICHARD FISCHER  
ON BEHALF OF  
AMERICAN BANKERS ASSOCIATION  
CONSUMER BANKERS ASSOCIATION  
THE FINANCIAL SERVICES ROUNDTABLE  
VISA U.S.A.  
BEFORE THE  
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
SUBCOMMITTEE  
OF THE  
COMMITTEE ON BANKING AND FINANCIAL SERVICES  
U.S. HOUSE OF REPRESENTATIVES**

**JULY 21, 1999**

Chairwoman Roukema and Members of the Subcommittee, my name is L. Richard Fischer. I am a partner of Morrison & Foerster and practice in the firm's Washington, D.C., office. I am appearing today on behalf of the American Bankers Association ("ABA"),<sup>1</sup> the Consumer Bankers Association ("CBA"),<sup>2</sup> The Financial Services Roundtable (the "Roundtable"),<sup>3</sup> and Visa U.S.A. ("Visa").<sup>4</sup> For nearly three decades, I have advised a variety of banks and other financial service providers across the United States and internationally on regulatory and retail banking matters, including those related to privacy. In addition, I am the author of the leading treatise in this field, entitled *The Law of Financial Privacy*, which is now in its third edition. We commend you for holding today's hearing, and appreciate the opportunity to appear before the Financial Institutions and Consumer Credit Subcommittee ("Subcommittee") of the Committee on Banking and Financial Services, of the U.S. House of Representatives, to discuss the ongoing efforts of financial institutions to protect consumer privacy.

Today, we are living through an information revolution and, as a result, are witnessing the development of new data management technologies that permit the assembly, storage, analysis and sharing of vast amounts of information. Although this information revolution is by no means limited to banks, within the financial services world, the resulting efficiency permits banks to offer consumers unparalleled choice of financial products and services, while simultaneously diminishing the number of unwanted offers. Understandable concerns about the collection and use of personal information by commercial firms have launched an open and dynamic discussion about the appropriate balance between the adequate protection of individual privacy and the fair use of personal information. Banks, for their part, are devoting significant resources to achieving this balance.

---

<sup>1</sup> The American Bankers Association is the largest bank trade association in the country. Its membership includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks.

<sup>2</sup> The Consumer Bankers Association is the recognized voice on retail banking issues in the nation's capital, representing the largest U.S. financial institutions.

<sup>3</sup> The Financial Services Roundtable represents the nation's largest bank-based, diversified financial services firms.

<sup>4</sup> Visa is a joint venture comprised of more than 21,000 financial institution members from around the world that have issued over 800 million Visa payment cards, which are accepted at more than 14 million merchant locations and over 480,000 automated teller machines worldwide.

In the course of addressing the Subcommittee's specific questions, my testimony today will focus on four key themes. First, I will describe the fundamental principle of customer confidentiality upon which banks have relied historically, and continue to rely, for their very success. Second, I will discuss the importance of information sharing to the modern American economy in general and to the banking industry in particular. In so doing, I will provide specific examples of the need for, and the benefits to consumers from, information sharing by financial institutions. I also will describe the significant adverse consequences both for consumers and banks which could arise from significant new information sharing restrictions. Third, I will underscore a critical point that is repeatedly overlooked in many of today's privacy debates: the fact that existing law already regulates information sharing and provides consumers with numerous privacy protections. Finally, I will discuss on-going banking industry efforts to protect consumer privacy, which are vibrant and effective.

As a result, I will express my belief, and that of ABA, CBA, the Roundtable and Visa, that the existing legal framework which governs the sharing of information by the banking industry provides effective consumer privacy protection, while permitting the flow of information that is vital to the banking industry and to the U.S. economy as a whole. Given this framework, consumers today have unprecedented access to, and information about, a universe of products and services which could only have been imagined just a few years ago, while retaining the ability to express and enforce their reasonable expectations of privacy.

Maintaining the Confidentiality of Customer Information  
is a Banking Industry Cornerstone

Financial institutions have a long history of successfully balancing the need to maintain personal information to serve the financial needs of and identify opportunities for their customers, with the privacy concerns of those customers. Banks historically have recognized that personal information about bank customers should be protected, and consequently have developed strong, internally-initiated safeguards to ensure the confidentiality and proper use of customer information. Given the special relationship they share with their customers, banks are particularly well suited to protect consumer privacy in the electronic commerce age. Although the form and quantity of information may have changed, it is a change in degree, not in kind.

The fundamental operating premise of banks -- that to be commercially viable, they must protect their customers' privacy -- extends to new financial services holding companies which, under H.R. 10, will be able to offer an expanded range of products and services to consumers. These financial

institutions understand that although their products may be highly innovative, their operating principles must remain traditional -- that is, the protection of consumer privacy is, and will remain, the cornerstone of successful banking.

The fact is, the marketplace works. Market-driven dynamics and an ever-increasing public focus on privacy compel each individual bank to respect the privacy wishes of its customers. Stated another way, protecting privacy is not only the right thing to do, but is critical to the commercial success of every financial institution. The banking industry is subject not only to continuous government oversight, but also to close scrutiny by the media and the public. Particularly given the intensely competitive nature of these industries, no bank can thrive, or perhaps even survive, for long should it gain a reputation for indifference about the confidentiality of customer information. Consequently, although the increased availability of consumer information in the modern era enables banks to provide consumers with increasingly diverse product and service opportunities, the use of such information is necessarily balanced with the fundamental commitment of banks to maintain the privacy of personal customer information. In fact, the protection of privacy is increasingly becoming a separate product characteristic, on which consumers shop for products and services, and banks compete for customers.

Today and into the foreseeable future, consumers have and will continue to have the ability to choose among a tremendously diverse group of financial institutions -- including community banks, institutions offering only traditional deposit and loan services, and diversified institutions offering a growing array of financial services. Moreover, recent experience demonstrates that the marketplace is vigorous, and that even the suggestion of a market failure with respect to privacy is rapidly addressed. The American public is both sensitive to and vocal on privacy issues, and the marketplace has responded with alacrity to public privacy concerns. This fact was powerfully demonstrated by recent widely-publicized events in which financial institutions quickly reexamined and promptly curtailed the communication of personal information to third parties for certain marketing purposes in direct response to expressions of concern by the public, the press, and federal and state regulators.

Furthermore, the banking industry generally -- and ABA, CBA, the Roundtable and Visa in particular -- has been supportive of addressing market failures through legislative action, when appropriate. For instance, the banking industry has actively supported Congressional efforts to address privacy issues relating to identity theft, illegal information brokers and pretext calling.

It also is important to note that many of the existing consumer privacy protections have arisen not out of government intervention, but out of market-

driven business principles that compel banks to value and protect consumer privacy. Of course, the confidentiality of bank customer information receives additional protection through a variety of federal laws and regulations (some of which I discuss in more detail later in this testimony), as well as through the internal policies and procedures of individual banks. Nevertheless, these laws and regulations are primarily procedural in nature, and are designed principally to facilitate the smooth functioning of the market.

Information Sharing is Critical to the U.S. Economy  
and to the Banking Industry

The importance of information sharing to the modern American economy cannot be overstated. Many experts attribute the unparalleled strength of the U.S. economy in large measure to the efficient availability of information and the extraordinary investment of U.S. industry in burgeoning information technologies. For instance, in a recent speech, Federal Reserve Board Chairman Alan Greenspan observed that

information technologies have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago. . . . Prior to the advent of what has become a veritable avalanche of IT innovations, most of twentieth century business decisionmaking had been hampered by limited information. . . . Large remnants of information void, of course, still persist and forecasts of future events on which all business decisions ultimately depend are still inevitably uncertain. But the recent years' remarkable surge in the availability of real-time information has enabled business management to remove large swaths of inventory safety stocks and worker redundancies, and has armed workers with detailed data to fine tune product specifications to most individual customer needs.<sup>5</sup>

With respect to the importance of consumer data to the American economy, Chairman Greenspan writes, "the plethora of information on the characteristics of consumers" has been a "critical component of our ever more finely hewn competitive market system."<sup>6</sup> Greenspan further explains that "[s]uch information has enabled producers and marketers to fine tune production schedules to the ever greater demands of our consuming public for diversity and individuality of

---

<sup>5</sup> Remarks by Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System, at the Conference on Bank Structure and Competition of the Federal Reserve Bank of Chicago, Chicago, Illinois (May 6, 1999).

<sup>6</sup> Letter from Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System, to the Honorable Edward J. Markey (July 28, 1998).

products and services. . . . It has enabled financial institutions to offer a wide variety of customized insurance and other products. Detailed data obtained from consumers as they seek credit or make product choices help engender the whole set of sensitive price signals that are so essential to the functioning of an advanced information based economy such as ours."<sup>7</sup>

As Chairman Greenspan's statement shows, information sharing is particularly important to the financial institution sector of the American economy. Information sharing is essential to the ability of financial institutions to meet the ever-increasing consumer demand for the efficient provision of innovative, individually-tailored financial products and services. For instance, information sharing permits financial institutions to outsource many basic business operations -- such as customer account servicing, records administration, auditing, check-printing, and compliance functions -- to third parties, who perform these operations on behalf of financial institutions. These third-party specialists typically perform such services more efficiently, and at a lower cost, than the institution itself might, serving consumers in the most cost-effective and efficient way possible. Moreover, particularly with respect to smaller institutions, such as community banks and credit unions, outsourcing such functions enables institutions to offer products and services to consumers that the institution otherwise simply would not have the capacity or expertise to offer. In this way, the ability to share information and outsource banking operations heightens efficiency and promotes competition in the financial services sector, to the ultimate benefit of consumers.

In addition, information sharing is critical to a financial institution's ability to control risk and combat fraud. When, for instance, a bank discovers that it has been defrauded by one of its customers, information sharing allows the bank to promptly inform its mortgage or credit card affiliates of the fraud, which dramatically reduces the chances of the fraudulent operator perpetrating the same scheme on those affiliates. Similarly, when a bank customer reports that a wallet or purse has been stolen, information sharing permits the bank to inform the affiliates and other parties so that they may prevent fraudulent or unauthorized account activity. Thus, any restrictions on the ability of financial institutions to share information for fraud and risk control purposes could threaten the very safety and soundness of insured financial institutions.

In this regard, it is worth noting that federal authorities have long understood the potential benefits of information sharing with regard to fraud and other law enforcement activities, and the banking industry has worked with the

---

<sup>7</sup> *Id.*



government to achieve an information-privacy balance. The banking industry is subject to a number of reporting requirements relating to the prevention of fraud and related activities, including the requirement that financial institutions share certain information -- including currency transaction and suspicious activity reports -- with law enforcement and other government authorities to combat criminal activities such as money laundering. While the banking industry has generally supported government efforts directed at fraud prevention, we also have frequently raised concerns about the various mandates crafted to address that worthy goal. These requirements create a constant dilemma for the banking industry: how to balance our obligations to identify and report illegal activities, while also protecting the privacy of customer financial records.

In addition, information sharing allows banks to improve services in countless ways that benefit consumers. For instance, information sharing permits financial institutions to offer consumers the convenience of "one-stop shopping," so that a bank customer can, through a single monthly statement or in a single telephone call, obtain information and make decisions about his or her checking account, mortgage loan, credit card account or other financial relationships of the customer with the bank and its affiliates. Otherwise, consumers would be forced to receive multiple statements, or to make multiple telephone calls, to deal separately with each type of account -- a costly and inefficient result for consumers and financial institutions alike.

Information sharing also permits consumers to receive lower rates on a variety of products and services offered by financial institutions. For instance, information sharing permits operation of the secondary market in home mortgage and other loans, which provides consumers with significantly lower interest rates that may save the consumer thousands of dollars over the life of the loan. The ability to share information also allows a financial institution to offer reduced rates and fees to a customer of the institution's affiliate, permitting consumers and institutions to benefit from the inherent efficiencies of so-called "relationship banking." For example, the savings provided to consumers by the lower interest rates which result from the secondary mortgage market may be even greater for consumers who choose to link their mortgage loan with a checking or savings account at the lender's affiliate.

Information sharing also enables financial institutions to offer consumers popular products such as "affinity" or "co-brand" credit card accounts. Such programs provide frequent flyer miles, grocery or gasoline rebates and other benefits to credit cardholders. Other such programs permit universities and other not-for-profit organizations to benefit from cardholder use of their accounts. These programs simply could not operate without the sharing of information

between the credit card issuer and the unaffiliated "affinity" or "co-brand" partner, with whom the consumer also has an existing relationship which is separate from, but related to, the consumer's relationship with the financial institution. Moreover, as Federal Reserve Board Chairman Greenspan has noted, information sharing permits financial institutions to offer products and services that are more closely tailored to consumer needs and desires, dramatically increasing efficiency both for banks and consumers. Finally, the ability to share information has enabled financial institutions to develop and offer consumers an astonishing array of financial products and services, which provide consumers today with unparalleled choice, convenience and opportunity.

Consequently, additional restrictions on the flow of information to and among U.S. companies -- particularly financial institutions -- could have severe unintended consequences for the U.S. economy, consumers and the banking industry. New information-sharing restrictions would harm consumers by restricting, or denying altogether, the availability of the various products and services discussed above, as well as of countless other offerings. Moreover, the enactment of new information-sharing restrictions would inevitably have adverse consequences for the development of increasingly innovative offerings. In particular, the establishment of new restrictions could stifle, or even halt, the burgeoning development of new products and services, thereby harming consumers and banks alike. As Federal Reserve Board Chairman Greenspan has said, "Given the high degree of uncertainty inherent in the development of new products and processes, policymakers should be cautious when attempting to anticipate the future path of innovation, or the effects new regulations may have on innovation. . . . Incentive compatible regulation, flexibly constructed and applied, is the logical alternative to an increasingly complex system of rigid rules and regulations that inevitably have unintended consequences, including possible deleterious effects on the innovation process."<sup>8</sup>

With this statement in mind, I want to touch on the privacy provisions that are contained in Subtitle A of Title V of H.R. 10 as passed by the House of Representatives, about which the Subcommittee has requested comment. The privacy provisions of H.R. 10 contain a number of unprecedented and sweeping information-sharing restrictions. For instance, H.R. 10 would establish a comprehensive notice and opt-out requirement for the sharing of customer information with unaffiliated third parties, institute a flat prohibition on disclosure to unaffiliated third parties of customer account numbers for specified marketing

---

<sup>8</sup> Remarks by Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System, at the Conference on Bank Structure and Competition of the Federal Reserve Bank of Chicago, Chicago, Illinois (May 1, 1997).

purposes, and mandate the provision of extremely detailed privacy disclosures at the beginning of a customer relationship and, thereafter, annually. ABA, CBA, the Roundtable and Visa are fervently committed to addressing privacy concerns that may arise from the reforms of H.R. 10. We believe, however, that a number of technical clarifications and corrections to the H.R. 10 privacy provisions are necessary in order to avoid significant adverse unintended consequences which would result from these provisions as approved by the House. Moreover, if Congress determines to enact the privacy provisions contained in H.R. 10, ABA, CBA, the Roundtable and Visa believe it is absolutely essential that they be enacted as the uniform law of the land, so that the same requirements will apply to all financial institutions, and the same protections will be afforded to all consumers, throughout the country.

Existing Law Already Regulates Information Sharing  
and Provides Consumers with Extensive Privacy Protections

I now want to underscore a critical point that is often overlooked in many of today's fervid privacy debates. The fact is, existing federal law already regulates information sharing and provides consumers with a plethora of privacy protections. Given time constraints, I will discuss briefly just a handful of the federal laws that play principal roles in regulating information sharing by financial institutions and others: the Fair Credit Reporting Act<sup>9</sup> ("FCRA"), the Electronic Fund Transfer Act<sup>10</sup> ("EFTA"), the Right to Financial Privacy Act of 1978<sup>11</sup> ("Financial Privacy Act"), and the Telephone Consumer Protection Act of 1991<sup>12</sup> ("TCPA").

*The Fair Credit Reporting Act*

The FCRA mandates that, before non-experience consumer information is shared among affiliated companies, consumers must be clearly and conspicuously informed of the possibility of that sharing and be provided an opportunity to opt out of the sharing arrangement altogether.<sup>13</sup> In other words, under the *existing* FCRA, if a consumer does not want his or her application information or other personal information obtained from third parties, such as credit bureaus, shared among affiliated companies, the consumer is empowered simply to prohibit the sharing of that information. Moreover, it is important to note that the FCRA allows only *affiliated* companies to share such application or credit bureau information, after provision to the consumer of notice and an opportunity to opt

<sup>9</sup> 15 U.S.C. § 1681 *et seq.*

<sup>10</sup> 15 U.S.C. § 1693 *et seq.*

<sup>11</sup> 12 U.S.C. §§ 3401 *et seq.*

<sup>12</sup> 47 U.S.C. § 227.

<sup>13</sup> 15 U.S.C. § 1681a(d)(2)(A)(iii).

out. If a bank were to share such information with unaffiliated third parties, the bank could become a consumer reporting agency subject to burdensome, complex and onerous requirements of the *existing* FCRA.

Moreover, the FCRA mandates that other notices be provided to consumers in connection with the use of shared consumer information. For example, the FCRA *already* requires that banks notify consumers when adverse action is taken in connection with credit, insurance, or employment based on information obtained from an affiliate. This affiliate-sharing adverse action notice must inform the consumer that he or she also may obtain the nature of the information that led to the adverse action simply by requesting that information in writing. Once such a request has been made, the bank affiliate then has 30 days to respond by disclosing the nature of the affiliate information used.

In addition, the FCRA *currently* empowers consumers by providing them with choice about how consumer reporting agencies may use their information for so-called "prescreening" purposes. Prescreening is the process in which a consumer reporting agency prepares a list of consumers who, based on the agency's review of its files, meet certain criteria specified by a creditor who has requested the prescreening. In addition to providing the consumer with a firm offer of credit, the FCRA also mandates that banks include prescreening disclosures with *every* written solicitation to consumers explaining that the offer results from a credit bureau prescreen and that the consumer has the right to opt out of future prescreening by notifying the credit bureau that created the prescreened list. Under the FCRA, a credit bureau that operates on a nationwide basis also is required to operate a joint system with other nationwide credit bureaus that allows consumers to opt out of future prescreening by *all* such bureaus.

#### *The Electronic Fund Transfer Act*

The FCRA, however, is not the only existing federal law currently mandating that disclosures be made to consumers in connection with information sharing activities. For instance, the EFTA and its implementing Regulation E<sup>14</sup> currently require that consumers be informed about a financial institution's information-sharing practices with regard to all accounts that may incur electronic fund transfers ("EFTs"), which today includes virtually all checking, savings and other deposit accounts. Specifically, Regulation E requires that a financial institution provide consumers with extensive disclosures at the beginning of the consumer's EFT relationship with the institution.<sup>15</sup> As part of these initial

---

<sup>14</sup> 12 C.F.R. § 205.

<sup>15</sup> 15 U.S.C. § 1693c(a); *see also* 12 C.F.R. § 205.7(a).

disclosures, each financial institution *already* must state the circumstances under which the financial institution in the ordinary course of business will disclose information concerning a consumer's deposit account to third parties.<sup>16</sup> For purposes of this requirement, the term "third parties" includes other subsidiaries of a financial institution's parent holding company.<sup>17</sup> In making the required disclosure, an institution must describe the circumstances under which information relating to that account generally, not just information concerning EFTs, will be made available to third parties.<sup>18</sup>

### *The Right to Financial Privacy Act*

The purpose of the Financial Privacy Act is to protect consumer records maintained by financial institutions from improper disclosure to federal government officials or agencies. Specifically, the Financial Privacy Act *currently* prohibits disclosure to the federal government of records held by certain financial institutions without providing notification to the consumer whose records are sought<sup>19</sup> and the expiration of a "waiting period," during which the consumer may challenge and prevent disclosure through legal action.<sup>20</sup> The Financial Privacy Act requires the government to give the financial institution a certificate of compliance with the statute before the financial institution releases customer records.<sup>21</sup> In order to avoid civil liability for that disclosure, the financial institution must receive and rely on this certificate in good faith in disclosing the records sought.<sup>22</sup> Historically, the most significant privacy concern of consumers relates to government access to their financial records; a concern that far exceeds privacy questions regarding use of information by bank affiliates or third parties.<sup>23</sup>

### *The Telephone Consumer Protection Act*

The TCPA and its implementing regulation<sup>24</sup> ("TCPA Regulation"), issued by the Federal Communications Commission, provide consumers with important protections by placing significant limitations on live telephone solicitations, among other things. Under the TCPA Regulation, companies can make telemarketing

---

<sup>16</sup> 12 C.F.R. § 205.7(a)(9).

<sup>17</sup> 12 C.F.R. § 205 Supp. II, Ques. 7-17 (1995).

<sup>18</sup> 12 C.F.R. § 205 Supp. II, Ques. 7-16 (1995).

<sup>19</sup> 12 U.S.C. §§ 3402, 3403(a), 3404-3408.

<sup>20</sup> *See, e.g.*, 12 U.S.C. § 3405.

<sup>21</sup> 12 U.S.C. § 3403(b).

<sup>22</sup> 12 U.S.C. § 3417(c).

<sup>23</sup> This deep concern was dramatically demonstrated by the unprecedented and overwhelming public opposition to the "Know Your Customer" proposals of the federal bank regulatory agencies, which were withdrawn in response to this public concern.

<sup>24</sup> 47 C.F.R. § 64.1200 *et seq.*

calls to residential telephones only if: (i) the call occurs between 8 a.m. and 9 p.m. (local time at the called party's location); (ii) the caller provides certain identifying information to the consumer; and (iii) the company maintains a company-specific do-not-call list of persons who do not wish to receive telephone solicitations made by or on behalf of the company.<sup>25</sup> Thus, if a consumer wishes to opt out of future telemarketing calls from a particular company, the consumer only need indicate that he or she does not wish to be called again. The company then must add the consumer's name to the company's do-not-call list. In other words, the TCPA Regulation *already* gives consumers the right under federal law to opt out of telemarketing calls from a particular company. In addition, the TCPA protects consumers by, among other things, restricting the use of automatic telephone dialing devices and prerecorded or artificial telephone messages.<sup>26</sup>

### Banking Industry Self-Regulation is Vibrant and Effective

The Subcommittee also has asked me to discuss banking industry self-regulatory efforts to protect consumer privacy, particularly with respect to electronic commerce. I am pleased to report today that banking industry self-regulation is vibrant and effective. The banking industry is far more than just a collection of individual institutions: each bank has a direct interest in maintaining consumer confidence in the privacy practices of the industry as a whole. Not only do market forces compel each individual bank to protect customer privacy, but market forces also give each bank a direct interest in the adequacy of other institutions' privacy practices, so that consumer confidence in the banking industry as a whole remains strong and unwavering. As a result, industry self-regulatory efforts are extensive and increasing.

This determination is underscored by the Federal Trade Commission's ("FTC") recent report to Congress, entitled *Self-Regulation and Privacy Online*, which was released on July 13, 1999.<sup>27</sup> In that report, the FTC concludes that industry has made significant progress over the past year in its efforts to self-regulate online privacy and, as a result, that the enactment of legislation to address online privacy is not appropriate at this time.<sup>28</sup> As FTC Chairman Robert Pitofsky said in his prepared testimony before a Subcommittee of the House Commerce Committee, while significant challenges remain, industry self-regulatory efforts "reflect industry leaders' substantial effort and commitment to fair information

---

<sup>25</sup> 47 C.F.R. § 64.1200(e).

<sup>26</sup> 47 U.S.C. § 227(b).

<sup>27</sup> Federal Trade Commission, *Self Regulation and Privacy Online: A Report to Congress* (July 1999).

<sup>28</sup> *Id.* at 12.

practices. They should be commended for these efforts."<sup>29</sup> Chairman Pitofsky discussed the rationale for the FTC's recommendation against new online privacy legislation: "[t]he Commission believes that self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology."<sup>30</sup>

While Chairman Pitofsky's statement was made in the context of online privacy, and did not focus solely on financial institution privacy-related efforts, the progress to which he refers, and the efforts that led to that progress, apply equally to the banking industry. The fact is that, consistent with its long-standing tradition of protecting consumer privacy, the banking industry has been at the forefront of U.S. industry efforts to protect consumer privacy in the modern era. One of the best examples of the banking industry's leadership in efforts to protect consumer privacy, in electronic commerce and elsewhere, is the early adoption of industry-wide privacy principles. For instance, in 1995, Visa adopted and published the Visa Issuer Privacy Principles. In 1996, the ABA and CBA each adopted best practices guidelines to serve as a blueprint for financial institutions to use in developing their own policies. Then, in 1997, all the major bank trade associations jointly adopted uniform Banking Industry Privacy Principles which have served as the basis for the development of individual privacy policies and guidelines by financial institutions throughout the country. These financial institutions, as a result, are obligated, consistent with unfair and deceptive practices and other standards, to comply with their individual privacy policy statements. Copies of the Visa Issuer Privacy Principles and the Banking Industry Privacy Principles are attached to this statement.

The banking industry also has demonstrated its leadership in consumer privacy protection through the industry's long-standing, substantial educational efforts. For instance, ABA, CBA, the Roundtable and Visa have used their respective Privacy Principles as the basis for privacy training efforts with thousands of their members around the country. Similarly, among countless other efforts, ABA provides its members, free of charge, a video training tool developed by The Chase Manhattan Bank, which is intended to increase both bank employee and public awareness of privacy issues, such as those relating to prevention of identity theft and pretext calling; CBA sponsors a number of efforts to increase awareness of privacy issues among its members, including weekly programs at which its members discuss key issues with privacy experts; the Roundtable

---

<sup>29</sup> *Electronic Commerce: Current Status of Privacy Protections for Online Consumers: Hearing before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Comm. on Commerce, 106th Cong. (July 13, 1999)* (statement of Robert Pitofsky, Chairman, Federal Trade Commission).

<sup>30</sup> *Id.*

provides numerous alerts to its members and suggestions in addressing privacy, and the Roundtable's Banking Industry Technology Secretariat ("BITS") has provided open forums for bankers to attend, be briefed and discuss privacy issues; and Visa and its member financial institutions have distributed consumer education programs and materials on a wide range of personal financial topics extending far beyond privacy to millions of Americans nationwide, including materials that help consumers learn to live within their means (such as the *Choices and Decisions* multi-media teaching curriculum, which assists consumers in planning their financial futures), help consumers to recognize the warning signs of potential financial problems, and assist those who are having trouble get out of debt (like *Managing Your Debts: How to Regain Financial Health*, which is distributed by Visa, the Consumer Federation of America and the National Foundation for Consumer Credit).

\* \* \* \* \*

The ABA, CBA, the Roundtable and Visa believe that the existing legal framework governing the sharing of information by financial institutions -- which effectively employs the interplay of consumer demands, federal laws and regulations, and the teeming marketplace itself -- provides effective consumer privacy protection, while permitting the flow of information that is vital to the banking industry and to the U.S. economy. The result? Ready consumer access to, and information about, a universe of products and services that were only dreamed of just a few years ago.

Once again, I want to thank you for the opportunity to appear before you today on behalf of ABA, CBA, the Roundtable and Visa. Please let us know if we can be of additional assistance to the Subcommittee or its staff.





## Visa Issuer Privacy Principles

In the course of opening accounts and providing services for individual Visa cardholders, Visa Issuers are entrusted with information related to cardholders' accounts. This information is vital to each Issuer's ability to provide cardholders with quality services, products and opportunities that are tailored to their individual interests and qualifications. Visa recognizes, however, the reasonable expectation of privacy that cardholders may have concerning aspects of this information, and recognizes the importance of respecting and protecting the privacy of Visa cardholders.

Accordingly, Visa has adopted these privacy principles with the expectation that they will serve as a foundation upon which Issuers will build their own privacy policies, tailored to their particular needs and circumstances. By adopting these principles, Visa and Visa Issuers will continue their leadership in the financial services industry and will continue to respect and protect the trust and confidence of Visa cardholders.

### **Principle One: Recognize Cardholder Privacy Expectations**

**Issuers should recognize and respect the privacy expectations of Visa cardholders.**

Consumer privacy is an important public concern. Lou Harris surveys have found that American consumers express a general concern about the use of their information, and how technology is used to collect and distribute information about them. Visa recognizes the importance of this issue to cardholders and the important role it plays in their trust and confidence in Visa and Visa Issuers. Accordingly, the Visa Issuer Privacy Principles are based on the premise that Issuers should recognize and respect the privacy expectations of Visa cardholders.

### **Principle Two: Collect and Use Cardholder Information Only to the Extent Needed**

**Issuers should collect and use information about individual cardholders only to the extent it is needed for their organizations' activities and to provide services and other opportunities to their cardholders.**

Surveys show that one of the principal consumer privacy concerns is the use of information corporations collect. Visa recognizes the importance of this concern. Thus, Issuers should limit the amount of information they collect and use about individual cardholders to what is needed to administer their business activities and to provide services and other opportunities of interest to cardholders.

**Principle Three: Maintain Accurate Information**

Issuers should have procedures to ensure that cardholder account data -- information directly related to the cardholder's account -- are as accurate, up to date and complete as possible.

The accuracy of cardholder account data is of particular importance in protecting and maintaining cardholder trust and confidence. The accuracy of cardholder information can also play an important role in the financial and service opportunities available to cardholders. Consequently, Issuers should have procedures to ensure that cardholder account data -- information directly related to the cardholder's account -- are collected and maintained in an accurate, up to date and complete fashion as is possible.

**Principle Four: Maintain Information Security**

Issuers should maintain appropriate security standards and procedures regarding the unauthorized disclosure of and access to cardholder information.

A fundamental element of maintaining adequate cardholder privacy procedures is providing reasonable protection against unauthorized disclosure of or access to cardholder information. To properly safeguard cardholder information, Issuers should maintain appropriate security standards and procedures in their business practices and incorporate them into their own privacy policies.

**Principle Five: Limit Employee Access to Information**

Issuers should implement policies and procedures to limit employee access to cardholder information to a need to know basis.

Traditionally, business access to cardholder information has been guided by a need-to-know standard: access to such information should be provided only to those employees who have a business need to know the contents. Visa endorses this time-honored standard. Therefore, to help maintain adequate consumer privacy protection, Issuers should implement policies and procedures to limit access to cardholder information to those employees who need to see it in order to carry out the Issuer's business and service functions.

**Principle Six: Restrict Disclosure of Account Information**

Issuers should not reveal specific information about cardholder accounts to non-affiliated third parties, unless (1) the information is provided to help complete the transaction, (2) the cardholder requests it, (3) the disclosure is provided or required by law, or (4) the cardholder has been informed in advance through a cardholder agreement or communication about such disclosure activities.

In addition to the general consumer concern about unwanted uses of their personal information, there is a particular concern among consumers about release of specific information regarding individual financial transactions (such as location and time of purchase and the transaction amount). Visa recognizes the importance of this concern. Consequently, Issuers should restrict disclosure of specific information about individual cardholder accounts to situations where such information is provided to help complete the transaction, when the cardholder requests it, the disclosure is provided or required by law, or where the cardholder has been informed in advance through a cardholder agreement or communication about such disclosure activities. Thus, cardholders might be informed that information about them may be provided to others in connection with various business activities related to their accounts, such as collection efforts, fraud prevention and credit reporting.

**Principle Seven: Honor Cardholder Requests to be Excluded from Marketing Lists**

If an Issuer provides cardholder information to a non-affiliated third parties for marketing purposes, the Issuer shall honor its cardholders' requests to exclude their names from such marketing lists.

According to Lou Harris surveys, most people believe that they do not have control over how information about them is circulated by corporations. Visa recognizes this consumer concern and believes that cardholders should be given an opportunity to request that their information not be made available to non-affiliated third parties for marketing purposes. Therefore, in the event that an Issuer provides cardholder information to non-affiliated third parties for marketing purposes, the Issuer shall honor cardholders' requests to remove their names from these marketing lists.

**Principle Eight: Maintain Cardholder Privacy in Relationships with Third Parties**

Where an Issuer provides cardholder information to a third party, the Issuer should require the third party to adhere to equivalent privacy standards with respect to that information.

The significant commitment of Visa Issuers to provide adequate cardholder privacy measures could be compromised if third parties with whom Issuers maintain business relationships do not provide equivalent privacy protections for cardholder information. Consequently, Issuers should require these third parties, when dealing with cardholder information, to adhere to privacy standards that are equivalent to the Issuer's privacy policy.

**Principle Nine: Conduct Employee Education and Monitoring Compliance**

Each Issuer should educate its employees about its privacy standards and employees' responsibilities to protect cardholder privacy. Issuers should monitor employee compliance.

Employees of Visa Issuers have a responsibility to help maintain trust and confidence of Visa cardholders and to help to protect the privacy of cardholder information. Accordingly, Issuers should undertake appropriate employee education efforts to help ensure that employees understand the meaning and requirements of their privacy policies. In addition, Issuers should monitor employee compliance with their established privacy policies.

**Principle Ten: Make the Issuer's Privacy Guidelines Available to Cardholders**

Issuers should make their privacy guidelines available to cardholders.

An important part of the Visa Issuers' commitment to providing meaningful consumer privacy protection is ensuring that cardholders understand their Issuer's privacy guidelines. Therefore, an Issuer should make its privacy guidelines available to its cardholders to help maintain their trust and confidence.

## BANKING INDUSTRY PRIVACY PRINCIPLES

**1. Recognition of a Customer's Expectation of Privacy.**

Financial institutions should recognize and respect the privacy expectations of their customers and explain principles of financial privacy to their customers in an appropriate fashion. This could be accomplished, for example, by making available privacy guidelines and/or providing a series of questions and answers about financial privacy to those customers.

**2. Use, Collection and Retention of Customer Information.**

Financial institutions should collect, retain, and use information about individual customers only where the institution reasonably believes it would be useful (and allowed by law) to administer that organization's business and to provide products, services, and other opportunities to its customers.

**3. Maintenance of Accurate Information.**

Financial institutions should establish procedures so that a customer's financial information is accurate, current and complete in accordance with reasonable commercial standards. Financial institutions should also respond to requests to correct inaccurate information in a timely manner.

**4. Limiting Employee Access to Information.**

Financial institutions should limit employee access to personally identifiable information to those with a business reason for knowing such information. Financial institutions should educate their employees so that they will understand the importance of confidentiality and customer privacy. Financial institutions should also take appropriate disciplinary measures to enforce employee privacy responsibilities.

**5. Protection of Information via Established Security Procedures.**

Financial institutions should maintain appropriate security standards and procedures regarding unauthorized access to customer information.

**6. Restrictions on the Disclosure of Account Information.**

Financial institutions should not reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence, unless 1) the information is provided to help complete a customer-initiated transaction; 2) the customer requests it; 3) the disclosure is required or allowed by law (e.g., subpoena, investigation of fraudulent activity, etc.); or 4) the customer has been informed about the possibility of disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (i.e., "opt out").

**7. Maintaining Customer Privacy in Business Relationships with Third Parties.**

If personally identifiable customer information is provided to a third party, the financial institutions should insist that the third party adhere to similar privacy principles that provide for keeping such information confidential.

**8. Disclosure of Privacy Principles to Customers.**

Financial institutions should devise methods of providing a customer with an understanding of their privacy policies. Customers that are concerned about financial privacy will want to know about an institution's treatment of this important issue. Each financial institution should create a method for making available its privacy policies.

**WRITTEN STATEMENT OF  
BRANDON BECKER**

**ON BEHALF OF THE  
SECURITIES INDUSTRY ASSOCIATION ("SIA")**

**BEFORE THE  
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT OF  
THE COMMITTEE ON BANKING AND FINANCIAL SERVICES OF THE  
UNITED STATES HOUSE OF REPRESENTATIVES**

**HEARINGS ON  
THE FINANCIAL SERVICES ACT OF 1999 (H.R. 10)**

**JULY 21, 1999**

Madam Chairwoman and Members of the Subcommittee, my name is Brandon Becker. I am a partner at the law firm of Wilmer, Cutler & Pickering and practice here in Washington. I was formerly Director of the Division of Market Regulation at the Securities and Exchange Commission and was responsible for the SEC's program to oversee securities professionals and markets.

Today I am appearing on behalf of the Securities Industry Association ("SIA")<sup>1/</sup> to present its views on customer privacy in the financial services industry. SIA appreciates this opportunity because SIA and its member-firms have long considered customer financial privacy to be an issue of utmost importance. Madam Chairwoman, we commend you and the other

---

<sup>1/</sup> The Securities Industry Association brings together the shared interest of more than 740 securities firms to accomplish common goals. SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. The U.S. securities industry manages the accounts of more than 50 million investors directly and tens of millions of investors indirectly through corporate, thrift, and pension plans. The industry generates approximately \$270 billion in revenues yearly in the U.S. economy and employs more than 380,000 individuals.

Members of the Subcommittee for holding these hearings, which fill an important gap in the record concerning financial modernization. As you know, when the SIA wrote to Speaker Hastert this past June, to support the House's financial modernization legislation, we called for hearings such as these. Therefore, we very much appreciate your prompt consideration of these issues.

As I will explain in more detail, SIA believes that H.R. 10's privacy provisions, within the context of the bill's overall financial modernization provisions, represent a workable, market-based approach for bolstering privacy protection. As SIA Senior Vice President Steve Judge stated on enactment of H.R. 10, "The privacy provisions attached to H.R. 10 build upon the industry's long-standing policy of respecting and protecting its customers' privacy." Indeed, we believe that the carefully crafted privacy requirements in H.R. 10 should preempt possible state legislation in this field. SIA looks forward to working with Congress as it moves to enact H.R. 10, which will bring about the financial modernization that SIA believes is needed for the benefit of consumers and the U.S. economy as a whole.

***THE BEST PROTECTION AGAINST THE MISUSE OF CUSTOMER INFORMATION IS  
THE COMPETITIVE MARKET.***

The first and most important point to underscore today is that, long before H.R. 10 and its privacy provisions were even proposed, securities firms were deeply concerned with meeting their customers' expectations about how their personal, financial information will be handled. Indeed, it would be impossible for a securities firm to prosper for long in today's competitive marketplace if it were to gain a reputation for misusing its customer's information or

allowing others to do so. A firm that uses customer information in ways customers find objectionable quickly will lose investor confidence — and market share as well.

Furthermore, securities firms have a strong proprietary interest in protecting their customer data. Securities firms invest substantial resources to develop relationships with their customers, and firms therefore treat the data they gather as a valuable asset. Consequently, firms protect information zealously and do not carelessly let other firms gain access to this valuable information.

Thus, the best and most dependable constraint on the misuse of customer information by financial services firms is the operation of the competitive marketplace. And because securities firms face these strong market incentives to protect the privacy of their customers' data, they are continually examining ways to ensure that their treatment of personal information meets the expectations of their customers. Especially today, as the financial industry is undergoing rapid structural changes and addressing emerging technological advances such as the World Wide Web and online trading, securities firms are reviewing and strengthening their privacy practices to ensure that they remain current both with emerging technology and consumer expectations. Charles Schwab and many other securities firms, for example, educate investors about their privacy policies through privacy practices statements that are accessible from their homepages on the World Wide Web. Indeed, the Federal Trade Commission recently concluded that, based on its survey of online privacy practices, the American business community as a whole is responding to market pressures by adopting privacy policies, and that no further Internet legislation is needed at this time.



Furthermore, SIA is itself pursuing several initiatives to promote privacy in the securities industry. For example, SIA recently established a board-level committee that will be devoted specifically to addressing privacy issues. The committee will educate SIA's member firms about privacy issues and will work with firms to develop the most effective means for meeting their customers' privacy expectations.

***H.R. 10 WOULD REINFORCE THESE MARKET INCENTIVES BY PROVIDING CONSUMERS MORE INFORMATION ABOUT PRIVACY PRACTICES SO THEY CAN MAKE INFORMED DECISIONS ABOUT FINANCIAL SERVICES COMPANIES.***

The second major point is that SIA supports the privacy provisions of H.R. 10 in the context of financial modernization legislation because the privacy provisions take a market-based approach for protecting consumer privacy. Instead of imposing a set of new, "one-size-fits-all" regulatory burdens, the privacy provisions of H.R. 10 promote privacy by enhancing consumer choice and thereby bolstering the operation of competitive market forces.

Let me be more specific. By requiring financial institutions to disclose their privacy policies to consumers, the bill promotes market incentives. Consumers will be armed with specific information that will enable them to select those firms whose privacy policies comport with their wishes. The choices that customers make in response to this flow of information resulting from the disclosure provisions will reward those securities firms that honor consumer preferences and punish those that do not. This provision thus gives consumers the ultimate ability to "opt-out" of information-sharing practices that they do not like: The bill empowers consumers to vote with their feet and take their business to financial services firms that meet their privacy expectations.

In addition, H.R. 10 affords consumers an additional "opt-out" opportunity by permitting them to prevent information-sharing with non-affiliated third parties. This provision protects customers' expectations and reassures them that they have control over the use of their personal information without unduly hindering responsible business practices. Some customers might not expect or desire that their personal, financial information will be shared with non-affiliated third parties. The opt-out provision provides the customer the opportunity to make an educated decision about whether he or she wishes the firm to provide his or her information to non-affiliates. At the same time, the requirement does not unduly restrict firms' ability to share information provided by customers who wish to receive benefits that arise from such sharing.

***ADDITIONAL PRIVACY OBLIGATIONS BEYOND THOSE CONTAINED IN H.R. 10 ARE UNNECESSARY AND ULTIMATELY WOULD HARM CONSUMERS.***

SIA does not believe that any additional regulation of personal, financial information is needed beyond the privacy provisions of H.R. 10. Indeed, the privacy requirements and exceptions contained in the bill were carefully crafted to reflect two important principles that militate against additional privacy regulations. First, customers' privacy interests are already protected by a broad array of regulatory requirements, common law principles, and market pressures. Second, any additional regulatory obligations could harm consumers by restricting firms' legitimate uses of customer financial information in ways that benefit customers.

On the first point, it is important to emphasize that, wholly apart from the privacy provisions of H.R. 10, consumers already enjoy legal protection against the misuse of their personal, financial information. A broad set of common law principles, statutory provisions, and

administrative regulations impose on securities firms duties to protect private information that customers entrust with them. For example, securities firms owe their customers a common law duty of loyalty, which among other things requires firms to put the interests of the investor ahead of their own. Thus, a firm that intentionally discloses, or otherwise makes use of, a customer's confidential information to benefit itself at the expense of the customer may violate its agency duties to the client and face liability for any resulting damages.

Similarly, securities firms are heavily regulated by industry self-regulatory organizations ("SROs") such as NASD Regulation, and these organizations have enforceable regulations in place that would cover the misuse of confidential information by their members or affiliated persons. Most generally, NASD-R Conduct Rule 2110 provides, "[a] member, in the conduct of his business shall observe high standards of commercial honor and just and equitable principles of trade." This general provision would reach unauthorized disclosure, or other misuses, of confidential information benefiting a securities firm at the expense of an investor. Other SROs maintain similar rules that would reach abuses of confidential information by their members.

Thus, it is important to recognize that Congress need not address in H.R. 10 all potential types of misuse of customer information in the financial services industry. Other safeguards do exist. SIA supports H.R. 10 as a workable supplement to those safeguards.

The second reason that Congress should not add to the regulatory obligations in H.R. 10 is that such modifications would harm consumers. Indeed, as I will explain, securities

firms gather and share personal information about their customers for many legitimate purposes that benefit consumers both directly and indirectly. In enacting privacy legislation, Congress should be careful not to hamper inadvertently these legitimate uses of customer information.

A few examples will illustrate the point. Securities firms are required to gather information about their clients in order to meet SRO "suitability" rules. Those rules require that firms recommending securities to retail customers must have a reasonable basis for recommending the securities, based on information disclosed by the customer. Thus, firms routinely gather financial information about their customers to satisfy that obligation, including information about the customer's financial and tax status, investment holdings, and investment objectives. Restricting the ability of securities firms to gather and use this information would hamper the effectiveness of these suitability rules, which, after all, were designed to protect consumers.

Furthermore, information sharing is essential for one of the principal consumer benefits associated with the recent trend towards diversified financial firms that H.R. 10 seeks to promote: the ability of a single firm to offer a package of products tailored to meet a customer's individual needs. Customers who come to a diversified financial firm expect to gain access to and receive offers for a variety of products and services under a single brand name. Indeed, many investors come to diversified firms precisely because such firms give the investor opportunities to benefit from the diversified offerings of an integrated firm.

Information sharing among affiliates also promotes customer convenience and lower costs. For example, an asset management firm may introduce customers to an affiliated broker-dealer for the execution of a securities trade. Before it can execute the trade, however, the broker-dealer necessarily needs to obtain information about the customer. By obtaining the information directly from its affiliated asset management firm, the broker-dealer is able to avoid the administrative costs and needless delays associated with contacting the client directly. The savings may then be passed on to investors in the form of lower fees and commissions. In short, diversified financial firms must, to meet customer expectations and offer greater financial opportunities to customers, share customer information with affiliated entities in the same corporate family.

Restricting the sharing of information among affiliates would impede these beneficial uses of personal information and impose needless costs on consumers. Indeed, restricting the flow of information from one affiliate to another reflects the sort of outdated thinking that this financial modernization bill is designed to eliminate. An opt-out requirement for interaffiliate sharing of information, for example, would confuse consumers and effectively defeat efforts by firms to promote a "one firm" identity and bring convenient, one-stop shopping to their customers through corporate branding and advertising. An opt-out restriction would require a financial institution to send customers an ambiguous, confusing message with respect to product offerings from affiliates sharing a common name. At the same time that customers are presented with a "one firm" brand image, they will be asked whether they wish to opt-out of receiving information on products and services that have been designed to meet their financial goals.

Furthermore, restrictions on information sharing among affiliates would impose significant administrative costs on diversified financial services firms. Those firms build and operate their back office computer systems to achieve efficiencies in processing, storing, and retrieving information. Different arms of a diversified firm typically will share these systems. An opt-out right that applies to the internal sharing of information among affiliates would effectively prohibit the use of shared computer systems and require firms to incur substantial development costs to develop and maintain stand-alone back office systems for each of their affiliates, leading to duplicative costs and inefficiencies.

Finally, restricting the sharing of information among affiliates could make it more difficult for securities firms to meet regulatory requirements. For example, Congress has recognized that broker-dealers face risks from the activities of affiliated companies, and that broker-dealers therefore must carefully monitor the activities of their affiliates. In the Market Reform Act of 1990, Congress granted the SEC authority to obtain from a broker-dealer information about affiliated companies. The temporary risk assessment rules that the SEC adopted under this authority contemplate that broker-dealers will use information from all available sources — obviously including the affiliate companies themselves — to assess their financial exposure. Congress must be careful not to let privacy regulation interfere with other important market safety measures that call for the sharing of information.

***BECAUSE H.R. 10 ALREADY IMPOSES COMPREHENSIVE DISCLOSURE OBLIGATIONS, CONGRESS SHOULD AMEND THE BILL TO PREEMPT STATE LAWS THAT ATTEMPT TO REGULATE THE USE OF PERSONAL FINANCIAL INFORMATION IN THE FINANCIAL SERVICES INDUSTRY.***

Because additional privacy regulation is unnecessary and could be harmful to consumers, Congress should amend H.R. 10 to preempt state laws that attempt to regulate the use of personal financial information by firms in the financial services industry. By enacting H.R. 10 with its current privacy provisions that promote the dissemination to consumers of information they need to select firms with appropriate privacy policies, Congress will ensure that consumers are equipped to make informed and effective choices about the handling of their personal, financial information. The comprehensive disclosure obligations of H.R. 10, in other words, make further federal or state intervention superfluous, because the market incentives reinforced by the legislation will ensure that firms implement effective and efficient privacy policies.

There is a very real danger, however, that states will enact additional, more burdensome regulations that would undermine the market-based approach that Congress has taken in H.R. 10. Indeed, several states are considering such proposals today. In today's national market for financial services, however, firms cannot reasonably comply with 50 different, and sometimes conflicting, standards for privacy protection. It would be impractical, for example, for a financial services firm to establish specialized computer programs and information-handling practices tailored to individual privacy requirements in each of the 50 states. Thus, the state that adopts the most restrictive privacy regulations will, in effect, set the policy for the nation, because national financial services firms will have to conform their nationwide operations to that state's regulations. Congress should not let individual states

override its judgment that, with H.R. 10's comprehensive information disclosure provisions in place, further privacy regulations are unnecessary. Congress therefore should amend H.R. 10 to preempt state laws that attempt to regulate the use of personal financial information in the financial services industry.

***TWO PROVISIONS OF H.R. 10 SHOULD BE MODIFIED TO AVOID CREATING UNINTENDED AND UNNECESSARY REGULATORY BURDENS.***

Although the SIA supports the privacy provisions in H.R. 10 as part of Congress's financial modernization initiative, two of its specific provisions need modification. It is also crucial that Congress not alter the exceptions in the legislation that are carefully tailored to ensure that the disclosure and opt-out provisions do not impede standard and appropriate industry practices.

The first provision requiring modification is the language in section 501 describing the congressional purpose behind the privacy provisions. We believe this language has the potential to be misconstrued as providing a basis for a private cause of action under state common or statutory law. The language could be read, however inappropriately, to create liability for any practice that might be deemed inconsistent with a standard of conduct that Congress might be perceived to have established through this language. Furthermore, the language might be construed to grant regulators broad power to engage in the very type of micromanagement of privacy practices that the bill itself successfully avoids. Congress should modify this provision to preclude such unintended legal consequences.



Second, language in section 503 requiring annual notification about privacy policies is unduly burdensome and unnecessary. This confusingly drafted provision would appear to require a firm to make annual privacy disclosures even to customers that are inactive and that do not otherwise receive any regular notices from the firm. Indeed, a firm would be required to send these additional and costly notices to customers every year even if the firm's privacy policy has not changed since the customers last received such notice. Congress should modify or eliminate this annual disclosure requirement. Once customers have received notice of a company's privacy policies, they are able to make an informed choice about whether to do business with the company, and that should be the end of the company's notice obligations. Little purpose is served by inundating customers with subsequent, identical notifications from companies with whom the customers are already doing business.

\* \* \* \*

In conclusion, I would again like to thank the Subcommittee, on behalf of SIA, for providing this important opportunity to share our views on the privacy provisions of H.R. 10. SIA believes that prompt enactment of financial services modernization is essential for the nation's growth and the enhancement of consumer services. Within that overall context of reform, SIA believes that, notwithstanding the existing protections for consumer privacy interests, the H.R. 10 privacy provisions are an acceptable way forward to address both business concerns and consumer expectations. If enacted, however, we believe these provisions should be the exclusive national standard for privacy protection in the financial services industry. We thank you again for this opportunity. I look forward to addressing any questions you may have.



**American Council of Life Insurance®**

Testimony of the

**AMERICAN COUNCIL OF LIFE INSURANCE**

Before the

**HOUSE COMMITTEE ON BANKING AND FINANCIAL  
SERVICES  
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND  
CONSUMER CREDIT**

On

**Emerging Privacy Issues**

Presented By  
Roberta Meyer  
Senior Counsel  
June 21, 1999

2128 Rayburn House Office Building

## INTRODUCTION

Chairwoman Roukema and members of the subcommittee, I am Roberta Meyer, Senior Counsel at the American Council of Life Insurance (ACLI). The ACLI is a national trade association with 493 member life insurance companies representing approximately 77 percent of the life, 81 percent of the disability income, and 88 percent of the long term care insurance in force in the United States. The ACLI very much appreciates being given the opportunity to present its views on emerging privacy issues related to the sharing of personal medical and financial information by life, disability income, and long term care insurers. These issues are critically important to ACLI member companies as well as to their customers.

The very nature of the life, disability income and long term care insurance businesses involves personal and confidential relationships. The ACLI is here today because these insurers must be able to obtain, use, and share their customers' personal health and financial information to perform **legitimate insurance business functions**. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers. ACLI member companies also believe that the sharing of information with affiliates and unaffiliated third parties generally increases efficiency, reduces costs, and makes it possible to offer economies and innovative products and services to consumers that otherwise would not be available.

## ACLI POLICY POSITION

Life, disability income, and long term care insurers are well aware of the unique position of responsibility they have regarding an individual's personal medical and financial information. ACLI member companies are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information. Last year, the ACLI Board of Directors adopted a series of "Confidentiality of Medical Information Principles of Support" based on this concept. (They are attached for your review.) As an industry, life, disability income, and long term care insurers have a long history of dealing with highly sensitive personal information, both medical and financial, in a professionally appropriate manner. We are proud of our record as custodians of this information.

The ACLI policy position regarding the protection of personally identifiable information is reflected in our long-standing support of the National Association of Insurance Commissioners (NAIC) Insurance Information and Privacy Protection Model Act (NAIC Model Act), enacted in 19 states. The ACLI believes this model strikes a proper balance between the legitimate expectations of consumers concerning the treatment of information that insurers obtain about them and the obligation of insurers to use personal information responsibly. Among other things, it requires that insurers provide a notice of information practices, outlines the content of disclosure authorization forms, imposes limitations and conditions on the disclosure of information and provides a process by which individuals can access, correct, and amend

information about them. Many, if not most, ACLI member companies doing business in at least one state which has enacted the NAIC Model Act adhere to its requirements in all states in which they do business.

## **LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURANCE POLICIES**

The fundamental purpose of life, disability income and long term care insurance is to provide financial security for individuals and families:

- **Life insurance** provides financial protection to beneficiaries in the event of the insured's death. Proceeds from a life insurance policy may help a surviving spouse pay a mortgage or send children to daycare or college.
- **Disability income insurance** replaces lost income when a person is unable to work due to injury or illness.
- **Long term care insurance** helps protect individuals and families from the financial hardships associated with the costs of services required for continuing care, for example, when someone suffers a catastrophic or disabling illness.

Every year America's life, disability income and long term care insurers enter into millions of insurance contracts. Those contracts represent the promises we keep to our policyholders.

## **USE OF PERSONAL HEALTH AND FINANCIAL INFORMATION BY LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURERS**

### **UNDERWRITING THE POLICY**

When a consumer begins the search for a life, disability income, or long term care insurance product, he or she usually begins by meeting with an insurer's sales representative. Generally, the sales representative will discuss with the individual his or her family's financial security and estate planning goals. If the consumer decides to apply for individually underwritten insurance, the sales representative will complete an application.

Many of the application questions concern nonmedical information, such as age, occupation, income, net worth, other insurance and beneficiary designations. Other questions focus on the proposed insured's health, including current medical condition and past illnesses, injuries and medical treatments. The sales representative also will ask the applicant to provide the name of each physician or practitioner consulted in connection with any ailment within a specified period of time (typically five years).

Up to this point in the process, the information the insurance company receives about the applicant has come directly from the applicant. Depending on his age and medical history and

the amount of insurance applied for, the insurance company may require medical record information or additional financial information. When the sales representative takes the consumer's application for insurance, he or she also will ask him to sign a consent form authorizing the insurance company to verify and supplement the information about him, and to obtain additional information if it is needed to evaluate the application.

The medical information that insurance companies typically request of applicants includes routine measurements, such as height and weight, blood pressure, and cholesterol level. The insurer may also seek an evaluation of blood, urine or oral fluid specimens, including tests for tobacco or drug use or HIV infection. **Medical tests are done only with the applicant's consent.** Since life, disability income, and long term care insurance policies are long range financial products purchased to provide financial security, it is often necessary for the insurer to also assess and use personal financial information, such as occupation, income, net worth, assets, and estate planning goals.

The price of life, disability income, or long term care insurance is generally based on the proposed insured's gender, age, present and past state of health, possibly his or her job or hobby, and the type and amount of coverage sought. Life, disability income, and long term care insurers gather this information during the underwriting process. Based on this information, the insurer groups insureds into pools in order to share the financial risks presented by dying prematurely, becoming disabled or needing long term care.

This system of classifying proposed insureds by level of risk is called risk classification. It enables insurers to group together people with similar characteristics and to calculate a premium based on that group's level of risk. Those with similar risks pay the same premiums. The process of risk classification provides the fundamental framework for the current private insurance system in the United States. It is essential to insurers' ability to determine premiums which are adequate to pay future claims and fair relative to the risk posed by the proposed insured.

**Some individuals are concerned that their medical record information will be "used against them" to deny or cancel coverage, or to increase premiums.** In fact, underwriting and the process of risk classification, based in large part on medical record information, have made life, disability income and long term care insurance widely available and affordable: **95 percent of individuals who apply for life insurance are issued policies and 91 percent obtain it at standard or better rates.**

**Once a life, disability income, or long term care insurance policy is issued, it cannot be canceled for any reason except for nonpayment of premiums. Premiums for these types of coverage cannot be raised** because an individual files a claim, or because an individual becomes ill after purchasing the policy. However, if an individual suffers from a serious medical problem at the time a life insurance policy is issued, the premium may be reduced in some cases when the insured's health improves. Also, although premiums for some disability income or

long term care insurance policies may be increased based on macro-economic factors, they may never be increased on an individual basis. Disability income and long term care insurance premiums may only be increased for a whole block of policies, usually only to ensure that premiums are adequate to pay claims.

## **THE BUSINESS OF LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURANCE**

Once a life, disability income, or long term care insurer has an individual's personal health and financial information, the insurer limits who sees it. However, the insurer must use and share that information to perform **legitimate, essential insurance business functions** – to underwrite the applications of prospective customers, as described above, to administer and service existing contracts with consumers, and to perform related product or service functions. Life, disability income, and long term care insurers must disclose personal information in order to comply with various regulatory/legal mandates and in furtherance of certain public policy goals (such as the detection and deterrence of fraud). Activities in connection with ordinary proposed and consummated business transactions, such as reinsurance treaties and mergers and acquisitions, also necessitate insurers' sharing of personal information.

## **PERFORMANCE OF ESSENTIAL INSURANCE BUSINESS FUNCTIONS**

Many insurers use affiliates or unaffiliated third parties to perform all or part of the essential, core functions associated with an insurance contract. It is quite common for these insurers to use affiliates or third parties to perform basic functions such as underwriting, claims evaluation, and policy administration. In addition, insurers also use third parties to perform important business functions, not necessarily directly related to a particular insurance contract, but essential to the administration or servicing of insurance policies generally, such as, for example, development and maintenance of computer systems.

Third parties, such as actuaries, employee benefits or other consultants, physicians, attorneys, auditors, investigators, translators, records administrators, third party administrators, and others are often used to perform business functions necessary to effect, administer, or enforce insurance policies or the related product or service business of which these policies are a part. **Often these arrangements with affiliates or unaffiliated third parties provide the most efficient and economical way for an insurer to serve prospective and existing customers. The economies and efficiencies devolving from these relationships inure to the benefit of the insurer's customers.**

If an individual were to be permitted to withhold consent or to "opt out" of a life, disability income, or long term care insurer's right to share his or her personal information with an affiliate or a third party performing a core insurance business function for the insurer, it would be extremely difficult, if not impossible, for the insurer to provide that consumer with the coverage, service, benefits, or economies that otherwise would be available. For example, suppose an

individual seeks life insurance coverage from an insurer which uses an affiliate or a third party to do its underwriting. If the individual subsequently withholds consent or “opts out” of the insurer’s right to divulge his personal health information, the insurer either cannot underwrite the policy because it does not have the internal capacity to do so or it must create a special system to accommodate this one individual.

Suppose an insured under an existing life insurance policy withholds consent or “opts out” of the insurer’s right to use or divulge his personal health and financial information, and the life insurer uses an affiliate or a third party to process policy loans or claims. The life insurer will either not be able to process a loan request or claim submitted by that individual or, again, will have to create a special system to accommodate that individual. If the life insurer has a third party computer company work on its computer system, it will not be able to give the computer company access to that individual’s file which needs to be part of the system. If the individual wants to assign his policy as collateral for a loan, the insurer will not be able to share the individual’s file with the prospective creditor, significantly jeopardizing the individual’s ability to get the loan. **In sum, insurers’ ability to conduct core insurance business operations may not be subject to an “opt-out” provision without significantly impairing, if not totally undermining, their ability to do business with individuals who choose to “opt-out”.**

#### **DISCLOSURES PURSUANT TO REGULATORY/LEGAL MANDATES OR TO ACHIEVE CERTAIN PUBLIC POLICY GOALS**

Life, disability income, and long term care insurers must regularly disclose personal health and financial information to: (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers; (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers’ conduct in the marketplace; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information. **Any limitation on these disclosures would seem likely to operate counter to the underlying public policy reasons for which they were originally mandated – to protect consumers.**

Life, disability income, and long term care insurers need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies, state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators, which work for the insurer. **Any limitation on insurers’ right to make these disclosures would seem likely to undermine the public policy goal of reducing fraud, the costs of which are ultimately borne by consumers.**

The continued right to make disclosures to the MIB is essential to insurers' efforts to combat fraud, yet it often comes under attack. The purpose of the MIB is to **reduce the cost of insurance** by helping insurers detect (and deter) attempts by insurance applicants to conceal or misrepresent facts. As part of the application process, **consumers receive a written notice** which describes the MIB and its functions. No information can go to the MIB unless an individual: (1) is applying for an individually underwritten insurance policy; and (2) has received a notice that information MIGHT be sent to the MIB. **Only a company that underwrites life, health, long term care insurance or disability income insurance may be a member of the MIB.**

Out of every 100 applications, information is only sent to the MIB in maybe 15 to 20 cases. It is sent in an encrypted fashion. Also, individuals can access and amend information MIB has about them. Corrections to information are usually completed within 30 days. MIB records are purged after 7 years. Insurance company members of MIB **will only request information regarding an individual applicant from MIB after the applicant has signed an authorization.** Again, member insurers may have access to MIB information only after receiving the individual's authorization.

A provision permitting individuals to withhold consent or to "opt-out" of an insurer's right to make disclosures to the MIB would require the insurance industry to abandon this effort at combating fraud and abuse. It would be like asking a bank not to do a credit check before it issues a mortgage. The result would be higher costs for all consumers.

#### ORDINARY BUSINESS TRANSACTIONS

In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer be able to disclose company files. Naturally, these files can contain personal information. Such disclosures are often necessary to the due diligence process which takes place prior to consummation of the deal and are clearly necessary once the deal is completed when the newly created entity often must use policyholder files in order to conduct business.

Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the amount and volume of coverage they can provide. These arrangements often necessitate the disclosure of personal information by the primary insurer to the reinsurer. Depending on the particular reinsurance treaty, this might happen because the reinsurer: (1) wishes to examine the ceding insurer's underwriting practices; (2) actually assumes responsibility for underwriting all or part of the risk; or (3) administers claims.

**If an individual insured were to be permitted to withhold consent or to "opt-out" of an insurer's right to disclose personal information in situations where the sharing of that individual's file is necessary to a merger, acquisition, or reinsurance arrangement, that**



**individual could hold hostage or prevent a transaction likely to benefit hundreds, or possibly thousands, of other policyholders. This would deprive other policyholders of the economies and product opportunities for which the transaction was originally sought.**

#### **MEDICAL PRIVACY PROVISIONS IN H.R. 10**

The medical privacy provisions of H.R. 10, as passed by the House of Representatives, while arguably not perfect, appropriately balance individuals' legitimate interest in the proper collection and handling of their personal health information with insurers' essential need to use and disclose that information necessary to perform legitimate, core insurance business functions, to fulfill legal mandates, and to achieve certain laudable public policy goals. These provisions do not represent all the medical privacy protections that some might consider appropriate. However, they are not intended to be comprehensive or to be the "final" answer to medical records privacy.

In fact, the language specifically states that these provisions will sunset when an omnibus medical records statute is enacted which satisfies the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These provisions **do not take away** the Secretary's authority to promulgate regulations on health information privacy, granted in HIPAA. Furthermore, the Secretary's authority goes beyond the entities covered in this bill ---- for example, to doctors and hospitals.

The ACLI is supportive of a **totally preemptive**, omnibus federal approach to medical records confidentiality that would permit insurers to perform legitimate insurance functions essential to their ability to serve and meet their contractual obligations to consumers. A federal statute that outlines a broadly preemptive set of specific standards to protect personal health information, and remedies for breach of those standards, will respond to the American public's concern about the confidentiality of their health information. Setting a **national, uniform standard for health information** is fundamental to the debate relating to medical privacy. Consumers would know that they were protected by the same, strong health information privacy law, regardless of their address. Also, life insurance, disability income, and long term care insurers engaged in business across the country would have a single standard to facilitate the industry's ability to provide financial security to individuals and their families in the most efficient, economical and innovative way possible. **Although the H.R.10 medical privacy provisions do not provide a comprehensive approach to this issue, the ACLI believes that they represent a good "first step" and provide privacy protection that does not currently exist under federal law.**

It is important to recognize that these provisions restrict disclosures of customer "health and medical and genetic information" which the insurance company has generally obtained either directly from the individual or pursuant to the individual's authorization. The provisions require the individual's consent (or an "opt-in") in order for an insurer to disclose this information **unless** the disclosure is being made for **limited, legitimate insurance business purposes.**

## EXPLANATION OF EXCEPTIONS TO THE CONSENT REQUIREMENT

The exceptions to the consent (or “opt-in”) requirement provide for disclosures of medical information which are made in connection with the performance of ordinary, legitimate insurance business functions. They appropriately reflect insurers’ need to share medical information with affiliates and third parties in order for them to fulfill functions necessary for the insurer to best serve and fulfill its contractual obligations to its customers. **If these exceptions, with respect to ordinary business practices, were not provided for, insurers’ ability to continue to perform essential business functions for their millions of existing customers, as well as prospective customers, would be jeopardized.**

Specifically, the exceptions take into account disclosures for the following legitimate, core insurance business functions:

### “Underwriting Purposes”

As noted above, life, disability income, and long term care insurers must use and often must disclose health information to affiliates or third parties in order to medically underwrite and to classify risks. The process of risk classification is **fundamental** to the current private, voluntary life, disability income, and long term care insurance business. Insurers commonly use affiliates or unaffiliated third parties (such as outside physicians, laboratories, or third party administrators) to perform part or all of this function and, consequently, must share personal health information about their customers with them so that they may do their jobs for insurers. **If a consumer were to be permitted to withhold consent for these disclosures of medical information, it would be very difficult, if not impossible, for the insurer to underwrite or issue the policy for which the consumer came to the insurer in the first place.**

### “Reinsuring Purposes”

As noted above, life, disability income, and long term care insurers commonly enter into reinsurance arrangements under which the reinsurer either audits the primary insurer’s underwriting practices, actually performs the underwriting, or pays claims. All of these activities necessitate the sharing of personal medical information by the primary insurer with the reinsurer. **If an individual were to withhold consent for the sharing of personal health information under these circumstances, it could jeopardize the consummation of a reinsurance transaction likely to benefit possibly hundreds or thousands of other policyholders or it could make it impossible for the insurer to underwrite that particular individual’s application for coverage or pay his claim for benefits.**

### “Account Administration”, “Processing Premium Payments”, “Processing Insurance Claims”:

Again, insurers often use affiliates or retain unaffiliated third parties to administer or

service insurance policies which activities include account administration, the processing of premium payments and the payment of claims. These are basic business functions which, in the case of claims benefits, certainly go to the core of the insurer's relationship with the customer. **If an individual were to withhold consent for the insurer to share medical information to an entity performing this type of function for the insurer, it would either not be able to fulfill its contractual and service obligations to the individual or would have to set up a special system just for that individual.**

**"Reporting, Investigating or Preventing Fraud or Material Misrepresentation"**

Unfortunately, there are times when individuals have incentive not to disclose all of their health information to an insurer to which they are applying for life, disability income, or long term care insurance coverage. In these instances, it is possible that the insurer will issue coverage that it would not have issued or will issue coverage at a significantly lower price than it would have had it had complete information about the proposed insured's health. Also, fraudulent claims are sometimes submitted to insurers. The costs of fraud and material misrepresentations ultimately are borne by other policyholders. **Individuals cannot be permitted to withhold consent for disclosures of medical information relating to the reporting of fraud or material misrepresentation without jeopardizing the public policy goal of detecting and deterring fraud.**

**"Providing Information to the Customer's Physician or Other Health Care Provider"**

Insurers must be permitted to release information to an individual's physician in the event medical testing performed in connection with underwriting indicates that there may be a medical condition previously undiagnosed.

**"Participating in Research Projects"**

Insurers do research for many purposes, most significantly, in connection with mortality studies. This information is essential to insurers in medical underwriting. **Disclosures necessary for these studies cannot be limited without jeopardizing insurers' ability to appropriately classify risk.**

**"Enabling the Purchase, Transfer, Merger or Sale of Any Insurance Related Business"**

When an insurer enters into an insurance contract with a new policyholder, it is unlikely to know if it will engage in a merger or acquisition or will be sold during the next 10, 20, or 30 years. **It would be impractical, if not impossible, for the insurer to be required to obtain thousands of authorization forms from all of its policyholders before such a transaction. Moreover, were individuals to be permitted to withhold consent for such a transaction, a single individual could prevent the whole transaction from being consummated, depriving other policyholders of opportunities and benefits which might otherwise have been available.**

**“As Otherwise Required or Specifically Permitted by Federal or State Law”**

As noted above, some states require or specifically permit the disclosure of medical information by insurance companies under certain circumstances. For example, a company may be required to disclose health information to a state insurance commissioner which is investigating an alleged unfair trade practice or to a self regulatory organization which is monitoring market practices. **These disclosures are mandated or permitted because they designed to protect consumers in the marketplace. Any limitation on these disclosures would seem to work counter to this public policy goal.**

**H.R. 10 FINANCIAL PRIVACY PROVISIONS**

The ultimate effect of the H.R.10 financial privacy provisions will be determined by the regulations promulgated to carry out the purposes of this new law. However, the provisions themselves are reflective of a conscious effort to balance consumers’ legitimate financial privacy concerns with consumer demands for convenience and prompt service. These also would permit insurers to pass on to their customers the economies and opportunities made possible by affiliation under H.R. 10 and to perform legitimate insurance business functions. These provisions appropriately permit the sharing of nonpublic personal information with affiliates and with certain unaffiliated third parties, where the third party is acting on behalf of the financial institution or pursuant to a joint agreement between two or more financial institutions. **This sharing of nonpublic personal information is essential to insurers’ ability to make available to their customers the efficiencies and product innovations which are the underlying purposes for enacting H.R. 10 in the first place.**

Because the privacy provisions in H.R. 10 were not the subject of hearings and are not based on a comprehensive record, there was a conscious effort not to impose broad restrictions on information sharing that might have unintended consequences or otherwise undermine the fundamental purposes of the bill. We believe that the exceptions to the general opt-out requirement for information sharing with third parties are wholly appropriate for reasons discussed below.

**EXPLANATION OF THE EXCEPTIONS TO THE NOTICE AND “OPT-OUT” REQUIREMENTS**

The financial privacy provisions also appropriately exempt from the “notice and opt-out” requirement disclosures which are made in connection with the following legitimate business functions:

**“As necessary to effect, administer, or enforce a transaction” or “in connection with servicing or processing a financial product or service”**

**This exception is one of the most important to life, disability income, and long term care insurers. As noted above, many insurers use affiliates or third parties to perform all or part**

of the core functions associated with a life, disability income, or long term care insurance contract, such as underwriting, claims evaluation, or policy administration. In addition, it is common for insurers to use unaffiliated third parties to perform other important business functions, not directly related to a particular insurance contract, but necessary to the general business of insurance, such as for maintenance of computer systems, for auditing or for other similar functions. **Unless insurers are permitted to disclose nonpublic personal information to affiliates or third parties, performing functions that are necessary to “effect, administer, or enforce” the transaction or “the product or service business of which the transaction is a part”, these insurers will be significantly hampered, if not totally prevented, from fulfilling their contractual and service obligations to prospective and existing customers.**

This exemption appropriately refers to disclosures that are necessary to “...administer, or enforce a transaction” or made “in connection with servicing or processing a financial product or service” as well as to disclosures necessary “to effect...a transaction”. Administration and service are inherent parts of an insurer’s relationship with its customer. **In the absence of such an exception, individuals would be permitted to “opt-out” of the insurer’s right to disclose nonpublic personal information to an affiliate or unaffiliated third party which must have access to that information in order to perform essential administrative or service functions, such as to process the individual’s application for coverage (for a disability income policy, for example), or his request for a collateral assignment of a life insurance policy for a loan.**

By virtue of the definition of “necessary to effect, administer, or enforce”, this exemption also appropriately applies not only to disclosures made in connection with a “transaction”, but also to disclosures made in connection with the “product or service business of which the transaction is a part”. This is important because life, disability income, and long term care insurance policies involve many “transactions”, after the origination of the contract, such as policy loans or claims payments, which may be part of the contract itself or part of the administration or servicing of the contract. The definition of “necessary to effect, administer, or enforce” also appropriately brings within the scope of the exemption disclosures which are “usual, appropriate, or acceptable” for underwriting, reinsurance purposes, account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits, participating in research projects, or as otherwise required or specifically permitted by Federal or State law. The importance of and need for these disclosures to affiliates and third parties has been discussed above as have the reasons why their limitation would work against the best interests of consumers.

**“With the consent or at the direction of the consumer”**

If an individual has given his consent to the sharing of his nonpublic personal information, there would seem to be no reason to prevent it or to keep him from enjoying the opportunities and benefits likely to result.

**To “protect against or prevent actual or potential fraud”**

As has been discussed above, insurers need and, in some cases, have a legal requirement to make certain disclosures in order to protect against or to prevent actual or potential fraud. These disclosures ultimately benefit consumers by lowering the societal cost of insurance fraud.

**To “persons holding a beneficial interest relating to the consumer”**

Sometimes a policyholder of a life insurance policy wishes to assign the policy (or the cash value of the policy) as collateral for a loan. If such a policyholder were to be permitted to “opt-out” of the insurer’s right to inform the potential lender of the value of the policy, this would make it difficult, if not impossible, for the policyholder to get the loan.

**“To the institution’s attorneys, accountants, and auditors”**

Like any other financial institution, life, disability income, and long term care insurers must also be able to disclose information, which might include nonpublic personal information, to outside advisors, including auditors, attorneys, and consultants who perform key business functions relating to individual policies or to the product or service business of which a policy is a part. Again, if an individual were to be permitted to opt-out of such disclosures, it might jeopardize the insurer’s ability to do business with that particular individual or possibly jeopardize its ability to do business generally.

**To “a State insurance authority” or “self-regulatory organizations”; to “comply with federal, state or local laws”, or “ in connection with a proposed or actual sale, merger, transfer, or exchange of all of a portion of a business”**

Again, the importance of and need for disclosures in these instances has been addressed above as have the reasons that it would be ill-advised for an individual to have the right to “opt-out” of these disclosures.

The ACLI appreciates having been given the opportunity to present these comments on these important issues relating to medical and financial privacy and would be delighted to answer any questions. Thank you.

## Confidentiality of Medical Information Principles of Support

Life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. The life insurance industry is proud of its record of protecting the confidentiality of this information. The industry is committed to the principles that individuals have a legitimate interest in the proper collection and use of individually identifiable medical information about them and that insurers must continue to handle such information in a confidential manner.

1. Medical information to be collected from third parties for underwriting life, disability income and long-term care insurance coverages should be collected only with the authorization of the individual.
2. In general, any redisclosure of medical information to third parties should only be made with the authorization of the individual.
3. Any redisclosure of medical information made without the individual's authorization should only be made in limited circumstances, such as when required by law in legal proceedings.
4. Upon request, individuals should be entitled to learn of any redisclosures of medical information pertaining to them which may have been made to third parties.
5. All permissible redisclosures should contain only such medical information as was authorized by the individual to be disclosed or which was otherwise permitted or required by law to be disclosed. Similarly, the recipient of the medical information should generally be prohibited from making further redisclosures without the authorization of the individual.
6. Upon request, individuals should be entitled to have access and correction rights regarding medical information collected about them from third parties in connection with any application they make for life, disability income or long-term care insurance coverage.
7. Individuals should be entitled to receive, upon request, a notice which describes the insurer's medical information confidentiality practices.
8. Insurance companies providing life, disability income and long-term care coverages should document their medical information confidentiality policies and adopt internal operating procedures to restrict access to

medical information to only those who are aware of these internal policies and who have a legitimate business reason to have access to such information.

9. If an insurer improperly discloses medical information about an individual, it could be subject to a civil action for actual damages in a court of law.
10. Any federal legislation to implement the foregoing principles should preempt all other state requirements.



ORAL STATEMENT OF MATTHEW P. FINK

PRESIDENT,  
INVESTMENT COMPANY INSTITUTE

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT  
IN THE HOUSE OF REPRESENTATIVES

ON  
EMERGING FINANCIAL PRIVACY ISSUES

JULY 21, 1999

Good morning Madam Chairwoman, Ranking Member Vento and members of the Subcommittee. I am Matthew P. Fink, President of the Investment Company Institute, which is the national association of the American mutual fund industry. I appreciate the opportunity to testify before you today on the important subject of financial privacy.

The mutual fund industry has enjoyed steady success in recent years. The foundation of that success is the trust and confidence of millions of individual investors. For this reason, the fund industry takes issues concerning the use and protection of our shareholders' personal information very seriously. In fact, over one year ago, the Institute urged the National Association of Securities Dealers to adopt a rule governing the sharing of customer confidential information by NASD members.

Mutual funds have a unique and rather complex business structure. It is vitally important to understand this structure when considering the information sharing issues at the heart of privacy discussions.

A mutual fund is a pool of assets without its own employees. The fund's operations typically are conducted by a number of affiliated and unaffiliated service providers. These service providers include the fund's investment adviser, principal underwriter, transfer agent, and custodian. My written statement explains the critical roles played by these service providers, and includes a diagram depicting a typical mutual fund organization.

To allow a mutual fund to operate, it is essential that shareholder information flow unimpeded among the fund and its various service providers. Information sharing must occur in order to maintain a shareholder's account, for example, by providing the shareholder and the IRS with required tax reporting information. Information also needs to be shared to properly service a shareholder's relationship with the entire fund organization, for example, to prepare consolidated account statements containing information as to the shareholder's investments in related products. These types of information sharing are unlikely to give rise to concerns over financial privacy because as a practical matter, fund shareholders generally view themselves as customers of the entire mutual fund organization. Few, if any, shareholders would be concerned with the fact that, as a technical matter, each of the entities within the complex is organized separately. In contrast to these types of information sharing, I am not aware of any mutual fund organization that sells its shareholders' personal information to unaffiliated companies or views that information as a source of additional revenue.

We cannot emphasize too strongly the importance of ensuring that any legislation addressing financial privacy take the unique structural characteristics of mutual funds into account. Legislation also must strike an appropriate balance between two important shareholder interests: giving shareholders control over uses of their personal information that reasonably might be considered objectionable and ensuring that shareholders efficiently receive financial products and services. The privacy protections included in H.R. 10, as recently passed by the House of Representatives, effectively strike such a balance. They would require all financial institutions – including mutual fund organizations – to disclose their policies on sharing personal information. They also would permit customers to opt out of any arrangements that involve sharing of information with unaffiliated entities for reasons not related to servicing customers. We support inclusion of these provisions in a final bill.

Proposals that would impose additional restrictions on the sharing of information could diminish the range and quality of services provided by mutual fund organizations to the detriment of their shareholders. For example, if mutual fund organizations were required to allow their shareholders to "opt out" of information sharing between the fund and its service providers, they might be unable to service the accounts of those shareholders who chose to opt out. Because mutual fund operations are invariably carried out by these service providers, this problem is especially acute for mutual funds. At the very least, fund organizations would be forced to develop and maintain systems that differentiate between shareholders who opted out and other shareholders and that could track this information on an ongoing basis. In addition, fund organizations would have to institute procedures and train personnel to ensure continuing compliance. The costs of these measures likely would be substantial, and would be difficult to justify given the small number of people likely to opt out. In fact, such restrictions could discourage some fund organizations from offering innovative products and services. Requiring that shareholders "opt in" to information sharing arrangements would be even more problematic, because of the extreme difficulty of obtaining affirmative consents.

Although the Institute supports the balanced approach taken by H.R. 10, we believe the Subcommittee needs to be aware that inconsistent state law requirements could upset this balance. Such requirements would be very burdensome for companies, such as mutual fund organizations, that do business in national markets. We believe that federal legislation to protect financial privacy should override inconsistent requirements under state law, and urge that such a provision be added to H.R. 10.

Thank you for the opportunity to present our views. We would be pleased to provide any additional information that the Subcommittee might request.

**American Medical Association**

Physicians dedicated to the health of America



1101 Vermont Avenue, NW  
Washington, DC 20005

# Statement

to the

Subcommittee on Financial Institutions  
and Consumer Credit  
Committee on Banking and Financial Services  
U.S. House of Representatives

## **Re: Medical Privacy Issues in HR 10**

Presented by Donald J. Palmisano, MD, JD

July 21, 1999

Division of Legislative Counsel  
202 789-7426

Statement  
of the  
American Medical Association  
to the  
Subcommittee on Financial Institutions and Consumer Credit  
Committee on Banking and Financial Services  
U.S. House of Representatives  
RE: Medical Privacy Issues in HR 10  
Presented by Donald J. Palmisano, MD, JD  
July 21, 1999

The American Medical Association (AMA) is pleased to provide testimony to the Financial Institutions and Consumer Credit Subcommittee of the House Banking and Financial Services Committee regarding the privacy of medical information in the context of financial services modernization legislation.

The AMA's Position on Medical Privacy

The patient-physician relationship is based first on trust. Confidentiality of communications within this relationship is a cornerstone of good medical care. In order for physicians to provide the best and most appropriate care, patients must feel that they can disclose to their physicians personal facts and information that they would not want others to know. Without such assurances, patients may not provide the information necessary for proper diagnosis

and treatment. Nor might they avail themselves of genetic tests that may be available to assist in the detection and possible amelioration or prevention of various disorders.

The AMA believes that patients have the basic right of privacy of their medical information and records and that this right should be honored unless waived in a meaningful way. This requires informed consent for disclosures of personally identifiable health information for any purpose. Recognizing that there are situations in which obtaining specific informed consent is not always practicable or possible, however, the AMA believes that, in such instances, either (a) the information should have identifying information stripped from it, or (b) an objective, publicly accountable entity must determine that patient consent is not required after weighing the risks and benefits of the proposed use.

#### The AMA's Position on HR 10

The stated purpose of HR 10, the "Financial Services Act of 1999," is to remove current barriers preventing affiliation among banks, securities firms, insurance companies, and other financial service providers, with the goal of enhancing competition in the financial services industry and fostering innovation and efficiency.

The AMA went on record, in coalition letters to Members of the House of Representatives preceding the full House's debate and vote on HR 10, expressing deep concerns about the medical information component of the bill. Since health insurers are considered "financial services institutions" under the bill, new opportunities are created for personally-identifiable health information collected by insurers to move laterally through a company and its

affiliates without patient consent or knowledge. We appreciate Representative Greg Ganske, MD, Representative Edward J. Markey and other Members bringing the issue of medical information privacy to the attention of their colleagues during the HR 10 debate. While the laudable intention of medical privacy language added to the bill was to limit the sharing of personal medical information among financial industries and their affiliates, in fact, the bill ended up doing exactly the opposite – facilitating the broad sharing of just such information. Our testimony today expands on the concerns raised in our letters to the House.

Financial entities other than health insurers that are included in HR 10's scope would become *de facto* secondary users of personal medical information. Generally speaking, secondary users are those whose use of medical records does not go directly to the treatment, payment or quality assessment of medical and health care provided to an individual. They can include life insurers; auto, property and casualty insurers; employers; licensing agencies public health agencies; medical researchers; educational institutions and even the media. "The flow of information to these parties in some cases affects people's lives in very direct ways, determining whether they are hired or fired, whether they can secure business licenses and life insurances, whether they are permitted to drive cars, whether they are placed under police surveillance or labeled as security risks." (*Protecting Privacy in Computerized Medical Information*, Office of Technology Assessment report, 1993, p. 48.) It is essential that individuals be notified of such information sharing and that their affirmative consent be required for disclosure of their individually-identifiable health information.



### The Dual Role of Insurers

The matrix of the financial services affiliations covered by HR 10 is complex. Health insurers, as a function of paying claims for medical care, are privileged to have access to personal medical information and records. When insurers function as financial service institutions, the medical record becomes an item of commerce and a market indicator. Insurers claim, in the context of the congressional debate on a comprehensive confidentiality bill, that they are “providers” seeking to improve the quality of care for populations. Yet in their role here as “financial services institutions,” they also seek to benefit from affiliating with banks, mortgage companies, holding companies, brokers and dealers and other insurers, to name a few possibilities envisioned by HR 10, creating financial services conglomerates. We find this troubling and believe that specific constraints are required to preclude inappropriate and unconsented-to disclosures of personally identifiable medical information in this context.

The medical record is created primarily as a clinical tool to assist in the diagnosis and treatment of individuals in trust relationship with their physicians. We believe that, as a general rule, patients must be provided the opportunity to consent to disclosures on their personal medical information, with narrowly tailored exceptions for certain defined public benefits. When the record migrates from its primary purpose as a clinical tool, that consent becomes even more important in that its secondary uses are not generally anticipated by the individual in facilitating his or her personal care and payment for that care.

### The Medical Privacy Provisions in HR 10

The medical privacy provisions in HR 10, as set out in Section 351, while well-intentioned, are inadequate to protect patients' sensitive medical information in the non-clinical setting. Despite the fact that patient consent is offered as a first alternative for insurers releasing personal medical information, a series of broad ranging exceptions swallow the rule. One exception, for example, would allow financial institutions to share an individual's personal medical information for "research projects." This term is not defined and could easily be construed to include a vast array of marketing evaluations or consumer profiling ventures. Further, it does not relate in any way with "research" and related protections as defined by the Common Rule (45 CFR 46).

Another set of exceptions would allow disclosure of individually-identifiable health information "in connection with" an array of largely transaction-related activities. While some of these are legitimate functions of insurers, it is nevertheless imperative that they be carefully defined and, more important, that consumer consent be required for disclosures for any of these functions. "In connection with" is vague language that, read with each of the exceptions, creates gaping holes in any systematic effort to protect patient privacy.

Even more troubling than what appears in Section 351 is what *doesn't* appear in Section 351. Granted, the "Financial Services Act of 1999" should not become the vehicle for comprehensive medical privacy legislation; nevertheless, if provisions are included at all, they should contemplate the full range of protections for such information in at least the financial services context. The bill does not preclude redisclosures or circumscribe

subsequent uses by affiliates and others. The bill does not create limits on government's and law enforcement's access to medical information. The bill does not provide any remedies for privacy breaches, except for those available at the state level, thus reducing the incentive for institutions to comply. The bill does not include any incentives whatsoever to de-identify personal medical information prior to sharing it with affiliates or unaffiliated third parties.

#### Title V Privacy Provisions

The "opt-out" provision offered in Section 502 of the bill – Title V, Subtitle A – does not apply at all to medical information. Section 507, also in Title V, Subtitle A, states that "[t]his subtitle shall not apply to any information to which subtitle D of title III applies, namely, section 351, "Confidentiality of Health and Medical Information." The only protections afforded by Title V to a consumer's health records would flow from Subtitle B, regarding "Fraudulent Access to Financial Information."

#### Curing the Medical Privacy Provisions of HR 10

The AMA believes that it may be possible to improve the privacy language of HR 10, such that it provides adequate protections until comprehensive privacy legislation is passed by the Congress. However, it is a difficult task to define the proper boundaries and decide how comprehensive the provisions should be. We are prepared to join with other interested parties in assisting the House with this task.

HR 10 should prohibit the transfer of medical information, even among affiliates, without the explicit consent of the individual. “Opt-out,” even if it would apply to medical information disclosures under the bill – which it does not – is insufficient. Individuals should have the affirmative right to direct who has access to their information, particularly outside of the therapeutic and payment context. One approach we believe could work would be to include an explicit “opt-in” provision for individually identifiable health information. Financial institutions, their affiliates and any unaffiliated third parties would be required to affirmatively acquire an individual’s consent to disclose their personally-identifiable medical and health information.

We understand the arguments from the floor of the House regarding the expectation of consumers for efficient and integrated financial operations regarding their related accounts in a financial institution. However, health insurers play a dual role that does not fit so easily into this construct. Insurers want to be characterized as “financial service institutions” for the purposes of affiliating with other financial and securities based corporate entities. Yet when it comes to the health care delivery system, insurers want to be regarded as health “providers.” They cannot have it both ways, and their inclusion in HR 10 explicitly demonstrates the dangers inherent in such an approach.

The most prudent option would be to adopt stringent privacy protections, which the Congress may then have the opportunity to modify in comprehensive privacy legislation. It would be reckless to provide so-called “protections” that would allow personal health information to flow freely without individual consent among affiliated and unaffiliated third

parties when the consequences are so enormous. Deleting the medical privacy provisions completely, leaving the status quo of state law in place for the time being, would be preferable to passing a version of HR 10 that allows such sweeping access to private medical information.

The Congress should take the most measured approach possible in HR 10 to information sharing – the gate cannot be closed once it is opened. Information cannot be “un-shared.” Once a financial institution has our medical information, it will become a permanent part of our consumer profile, regardless of future protections that might be imposed. Thus, we would urge the utmost caution so that, if Congress errs at all, it is on the side of protecting patients and their information rather than financial conglomerates’ desire to exploit that information.

#### Relationship to State Laws

If the Congress decides to retain and strengthen these medical privacy provisions, rather than deleting them entirely, we think it is essential to allow more protective state laws to remain in force. It is our understanding that the sponsor intended a “federal floor,” however, and we suggest the language be modified to permit more protective state provisions to prevail. This would be consistent with the intent in Title V, Section 524, which provides that subtitle B, regarding “Fraudulent Access to Financial Information,” should not be construed as superceding State law, and that greater State protections should prevail.

#### Conclusion

HR 10 provides an opportunity for significant enhancement of financial services industry operations. It also presents the potential for ethically perilous conglomerations of information and power as regards individually-identifiable health records. When insurers function as financial service institutions, the medical record becomes an item of commerce and a market indicator. Health insurers' dual role as "providers" and as "financial services institutions" highlights the concern of physicians and patients that information will be shared without consent or knowledge of the individual, for purposes unanticipated by the individual. The AMA finds this to be a troubling possibility and urges the Congress to seek more protective language in HR 10 to specifically prohibit inappropriate and unconsented-to disclosures of personally identifiable medical information in the financial services context.

Issues as to how medical information is disclosed and used are not a footnote to HR 10; rather they go to the heart of individuals' rights within evolving commercial and market systems. The AMA thanks the Subcommittee for focusing its specific attention on these important matters.

## American Psychiatric Association

1400 K Street, N.W.  
 Washington, D.C. 20005  
 Telephone 202.682.6000  
 Fax 202.682.6850  
 E-mail [apa@psych.org](mailto:apa@psych.org)  
 Internet [www.psych.org](http://www.psych.org)

### Board of Trustees

#### 1999-2000

Allan Tasman, M.D.  
*President*  
 Daniel B. Borenstein, M.D.  
*President-Elect*  
 Richard K. Harding, M.D.  
*Vice President*  
 Paul S. Appelbaum, M.D.  
*Vice President*  
 Michelle Riba, M.D.  
*Secretary*  
 Maria T. Lymbens, M.D.  
*Treasurer*

Rodrigo A. Muñoz, M.D.  
 Herbert S. Sacks, M.D.  
 Harold I. Ecox, M.D.  
*Past Presidents*

Kathleen M. Mogul, M.D.  
 Herbert S. Pevsler, M.D.  
 Edward C. Leonard, Jr., M.D.  
 Norman A. Ciemens, M.D.  
 Jack Bonner, III, M.D.  
 Maurice Rappaport, M.D., Ph.D.  
 Michael F. Myers, M.D.  
 Marcia K. Gonn, M.D., Ph.D.  
 Richard S. Epstein, M.D.  
 Ann Maloney, M.D.  
 Julie K. Schulman, M.D.  
 Sandra DeJong, M.D.

### Assembly

#### 1999-2000

Alfred Herzog, M.D.  
*Speaker*  
 R. Michael Pearce, M.D.  
*Speaker-Elect*  
 Nada L. Stotland, M.D.  
*Recorder*

Nancy C. Andreasen, M.D., Ph.D.  
*Editor, American Journal of  
 Psychiatry*  
 John A. Talbott, M.D.  
*Editor, Psychiatric Services*  
 James P. Kravitz, M.D.  
*Editor, Psychiatric News*  
 Steven M. Minn, M.D.  
*Medical Director*

John Blanghin  
*Director, Public Affairs*  
 Jay B. Cutler, J.D.  
*Special Counsel & Director,  
 Government Relations*  
 Kathleen Dempsey  
*Chief Financial Officer*  
 Charles Kilian  
*Chief Information Officer*  
 Ronald A. McMillen  
*Director, Publishing Operations*

Ivin L. Muszynski, J.D.  
*Director, Healthcare Systems & Financing*  
 Harold Alan Pincus, M.D.  
*Deputy Medical Director*  
 James W. Thompson, M.D.  
*Deputy Medical Director*  
 Jack W. White, D.B.A.  
*Deputy Director, Business  
 Administration*  
 Deborah Zann, M.D.  
*Deputy Medical Director*

## TESTIMONY OF RICHARD HARDING, M.D.

On behalf of

## THE AMERICAN PSYCHIATRIC ASSOCIATION

on

## MEDICAL RECORDS PRIVACY

before the

## SUBCOMMITTEE ON

## FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

## U.S. HOUSE OF REPRESENTATIVES

July 21, 1999



Madame Chair, I am Richard Harding, M.D., Vice-President of the American Psychiatric Association (APA), a medical specialty society representing more than 40,000 psychiatric physicians nationwide. I am Vice-Chairman, Clinical Affairs and Professor of Neuropsychiatry and Pediatrics at the University of South Carolina Medical School. I also serve on the National Committee on Vital and Health Statistics which was charged by the Congress to make recommendations to the Secretary of Health and Human Services on protecting the privacy of medical records. The views I am presenting before the Sub-committee today are my views and the views of the American Psychiatric Association.

First let me thank the Chair of the Subcommittee, Mrs. Roukema and Ranking Member Vento for holding these valuable hearings. And let me add my particular thanks to Representative Roukema for your outstanding and continuing support not only for non-discriminatory insurance coverage of mental illness, but your overall leadership on mental health and indeed health issues in general.

It is unfortunate that recent debates on medical records privacy have become divisive. Privacy is a natural issue for conservatives concerned about state rights, individual liberty, and freedom from intrusive government policies to work with liberals dedicated to personal privacy, and Fourth Amendment Constitutional due process protections. In fact, earlier this year the American Psychiatric Association and others worked closely with Senators Roth and Leahy and Representatives Stark, Markey, Paul and Whitfield to modify a HCFA regulation that would have seriously undermined patient privacy. I hope individuals on both ends of the political spectrum will be able to work together on this issue.

Turning to the medical records provisions of H.R. 10, APA is extremely concerned that these provisions will undermine patient privacy and the quality of health care. Because the provisions would overturn the principle of patient consent before disclosure of records and may overturn certain state privacy laws, H.R. 10 represents a significant step *backwards* for patient privacy. Moreover, since doctor-patient confidentiality is an essential element of effective medical treatment, these provisions will also have significant ramifications for the quality of health, and particularly mental health, care.

Without a very high level of patient privacy, many patients will be deterred from seeking needed health care or from making a full and frank disclosure of critical information needed for their treatment. For these and other reasons over 40 physician, provider, and patient groups, including the American Medical Association, the American Lung Association, the American Academy of Family Physicians and two major unions oppose these provisions.

As great as our concerns are about H.R. 10, the sponsor of these provisions has stated that his intention is not to preempt state privacy laws. He has also expressed his general support for the principle of patient consent before the disclosure of medical records. These are two critically important principles that we strongly support. When combined



with other changes I outline in my written testimony, these principles offer hope of a positive resolution of this issue.

However, we do urge members of the Subcommittee to err on the side of caution and indeed of protecting privacy when considering these provisions. Just as “the first rule of medicine is to do no harm” we hope the Subcommittee will adopt the same approach on medical records privacy issues. If the Congress permits extensive use and disclosures of patients’ medical records without the informed voluntary consent of patients in H.R. 10, it will be enormously difficult if not impossible to undo the damage later. At least if we do no harm, states’ efforts to address this issue can continue and positive and comprehensive medical records legislation can be enacted into law.

Finally, I know that most members of this Subcommittee are probably more familiar with financial privacy issues than with medical records privacy issues. It is critically important to recognize the difference between medical records privacy and financial privacy. If financial information is wrongfully disclosed it can be a nuisance, an embarrassment, and in some cases may even cause financial loss. But one can seek legal redress to recover any financial losses.

But the damages from breaches of medical records privacy are of a different nature. Medical records information can include information on heart disease, terminal illness, domestic violence, and other women’s health issues, psychiatric treatment, alcoholism and drug abuse, sexually transmitted diseases and even adultery. The U.S. Supreme Court noted in its 1996 *Jaffee v. Redmond* decision that disclosures of medical records information may cause personal “disgrace.” These disclosures can jeopardize our careers, our friendships, and even our marriages.

And if such disclosures occur, there are truly few meaningful remedies. Seeking redress will simply lead to further dissemination of the highly private information that the patient wished to keep secret. Nor can a financial settlement do much to compensate the individual for these highly personal losses. For all these reasons very strong medical privacy protections are needed.

Our particular concerns concerning Section 351 are as follows:

The medical records provisions of H.R. 10 would allow the use and disclosure of medical records information without the consent of the patient in extraordinarily broad circumstances. To give just two examples, law enforcement entities would enjoy virtually unfettered access to medical records and insurance companies could review individual medical records in performing marketing studies. The list of entities that could obtain medical records is also extensive. Why should life insurers, auto insurers, and even insurers providing travel cancellation insurance be able to routinely access patients’ entire medical records without patient consent or even knowledge?

To complicate matters further, Section 351 establishes no limitations on subsequent disclosures of medical records to non-affiliated entities. Once a disclosure has occurred, there is no limitation on the types of disclosures that the recipient of this information may make. Thus, if an insurer contracts out a certain authorized service to a bill collection

agency or an administrative support company, nothing in the legislation would prevent these organizations from disclosing the information for a host of inappropriate purposes far beyond any legitimate health use. These secondary recipients could even disclose the medical records information to malpractice attorneys seeking potential clients, tabloids seeking publicity, etc.

Section 351 lacks the basic protections included in all the major confidentiality bills before the Congress. The legislation lacks specific requirements for physical, technical, and administrative safeguards to prevent unintended disclosures of medical records. Nor does the legislation encourage the use of deidentified medical records or insure that patients will receive notice of the confidentiality, use, and disclosure practices of the insurance companies. These provisions are even more troublesome because they could preempt state privacy laws.

Let me also explain more fully the two key principles that should serve as the foundation of any privacy legislation.

Preemption. I believe the most important medical records privacy provision is to insure that stronger state medical records privacy laws are preserved and that states' ability to enact stronger medical records privacy laws is protected. States have adopted valuable protections for patients, including laws blocking insurers' access to verbatim psychiatric notes. States are also actively considering numerous additional proposals. In fact, the National Council of State Legislatures estimates that a total of 56 medical records confidentiality bills have passed through at least one chamber of a state legislature. We must not block states' efforts to protect citizens' medical privacy.

Consent. APA believes three principles should govern authorization and consent for disclosure of medical records. *First*, patients themselves should decide whether or not personal health information is disclosed. Consent before use and disclosure of medical records is critically important and this time-tested approach should be preserved and strengthened in order to remain meaningful in the changing world of health care delivery. In general, whatever problems may now exist with confidentiality of health information are derived from our failure to observe this principle. No one is in a better position than patients themselves to identify sensitive information and to determine to whom it ought not to be revealed. Those who would alter this traditional approach have failed to justify such a radical change.

*Second*, identifiable personal health information should be released only when deidentified data is inadequate for the purpose at hand. *Third*, even when consent has been obtained, disclosure should be limited to the least amount of personal health information necessary for the purpose at hand. This is consistent with our recognition of the importance of protecting medical privacy.

These principles have implications for some of the major policy questions regarding authorization of disclosure. For patients to retain meaningful control over personal health information, prospective consent for routine disclosures of identifiable information should be largely limited to information needed for treatment and payment purposes. Other health care operations can usually be accomplished with deidentified data. With

such a provision, a strong incentive will exist for the use and further enhancement of technology to perform a wide array of administrative functions.

Conclusion

As physicians, we take an oath first stated by Hippocrates that, "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick...I will keep silence thereon, counting such things to be as sacred secrets." In order to make sure that doctor-patient confidentiality continues to protect patients in the new millennium, I strongly urge the Subcommittee to address these important issues.

We thank you for this opportunity to testify, and we look forward to working with the Committee on medical records privacy issues.

**STATEMENT  
OF THE  
AMERICAN  
INSURANCE  
ASSOCIATION**

---

**Testimony Submitted by the  
American Insurance Association  
On  
Emerging Financial Privacy Issues**

**Before the  
Subcommittee on Financial Institutions and Consumer Credit  
Committee on Banking and Financial Services  
U.S. House of Representatives**

**July 21, 1999**

---



The American Insurance Association is a national trade organization of property and casualty insurers.

House of Representatives  
Subcommittee on Financial Institutions and Consumer Credit  
Privacy Hearings  
July 20-21, 1999

Statement of the American Insurance Association

The American Insurance Association ("AIA") is a trade association representing more than 300 insurance companies which write a large portion of the property/casualty insurance sold in the U.S. and in the global marketplace. We appreciate the opportunity to offer AIA's views on financial privacy, particularly as it relates to H.R. 10, as passed by the House of Representatives on July 1, 1999.

We would like to take this opportunity to commend Chairman Roukema for the constructive role she has played in co-sponsoring the Oxley/Pryce/Roukema amendment to H.R. 10, which was approved on the House floor by a 427-1 vote. We support this amendment but agree with her position that it is important to take the time to explore the many issues involved in protecting personal financial information in order to avoid unintended consequences for consumers and financial institutions alike. We believe today's hearing will lead to a constructive dialogue.

Banks, securities firms, and insurance companies already are covered by an array of federal and state privacy requirements, and many have instituted voluntary privacy protection policies that go beyond the specific requirements of federal or state law. Yet despite these regulatory and private sector protections, many Americans are concerned about how personal information about them is circulated and used by their financial institutions. In light of these concerns, H.R. 10 has served as a vehicle for debating the adequacy of current financial privacy protections and the need for additional measures.

Initially, AIA believed that it would be better to debate the privacy issue on a free-standing basis, in that H.R. 10 already was a complex measure that has been subject to more than two years of extensive debate. However, when it became clear that the House of Representatives wanted to include new privacy protections in H.R. 10, we worked proactively with Chairman Roukema, as well as other Members of Congress and our colleagues in the financial community, to construct a privacy amendment that would provide new consumer protections without undermining the core principles of H.R. 10—expanded consumer choice, greater market efficiency, a level playing field for all competitors, and functional regulation. We recognize that this amendment will impose new regulatory requirements on our members and affect certain data transfers that are in their business interests. Nonetheless, we believe it strikes a fair balance between all affected parties.

By contrast, the more draconian restrictions contained in the Markey amendment, a key element of Congressman Markey's failed effort to recommit H.R. 10, would cost

consumers choice, quality, and value in their use of financial services. Moreover, it would undermine the core principles of H.R. 10 and cause many financial institutions to reverse their support for critically needed financial modernization legislation.

As you move forward, any financial privacy protections approved by Congress must take into account the legitimate information sharing needs of property/casualty insurance companies and other financial institutions, regardless of their size and corporate structure. Moreover, whether such protections are enacted as part of H.R. 10 or on a stand-alone basis, it is important to avoid unintended consequences for all participants in the evolving financial services marketplace.

### Current Landscape for Insurer Privacy Protections

A wide range of federal and state privacy laws now govern the privacy practices of p/c insurance companies. At the federal level, this includes the Fair Credit Reporting Act, the Fair Credit Billing Act, the Electronic Communications Privacy Act, the Fair Debt Collection Practices Act, and the Right to Financial Privacy Act. At the state level, the NAIC Model Privacy Act has been adopted in some 20 states, and virtually every insurance department incorporates privacy protections into their market conduct examinations of their state's insurance companies. Indeed, the National Association of Insurance Commissioners' market conduct handbook specifically instructs examiners to "recognize the privacy accorded to individual policyholders and claimants by applicable privacy laws."

Beyond these specific legislative and regulatory mandates, protecting individuals' privacy is good business for property/casualty insurers that deal with sensitive information arising from automobile crashes, home fires, liability claims, and other covered losses. Indeed, a number of p/c insurers have developed privacy protection policies that go well beyond the requirements of current law. While we are aware of recent legal actions brought against the privacy practices of some financial institutions, we know of no similar concerns involving p/c insurance or p/c insurers.

### Overview of H.R. 10's Privacy Provisions

Despite the presence of the many federal, state, and private sector privacy protections, a near unanimous House of Representatives voted to include additional privacy provisions in H.R. 10. The amendment approved by the House will, for the first time, require financial institution regulators to establish standards for the safeguarding of customer information from unauthorized access. Also for the first time, it requires banks, insurance companies, securities firms, and other financial institutions to have in place and disclose a privacy policy that meets federal standards. It prohibits the sharing of credit card and deposit account information with unaffiliated third parties for the purpose of third party telemarketing or other marketing. It includes an "opt out" requirement that allows consumers to opt out of having their financial institution share nonpublic personal

information about them with unaffiliated third parties, while allowing the processing of transactions that are central to the customer's relationship with their financial institution. It prohibits the repackaging of nonpublic personal information by unaffiliated third parties who receive it in ways that would undermine the privacy protections applied to the originating financial institution. Recognizing the difficult issues raised by information sharing among affiliated entities, the Treasury Department is required to study this issue and report its findings and conclusions to Congress in a prompt manner. Taken together, these provisions represent a significant expansion of existing federal and state privacy mandates that are applicable to financial institutions.

From AIA's perspective, it is critical that these or other privacy protections considered by the Congress preserve critical data sharing needs of the p/c insurance industry, and be complementary to the core principles of H.R. 10.

#### The Data Sharing Needs of P/C Insurers Must Be Preserved

P/C insurers sell a unique and valuable product—the promise to pay claims associated with unexpected events in the future, such as automobile accidents, fires, storm damage, and liability lawsuits. For the insurance mechanism to function properly, p/c insurers must have access to a wide range of customer information what will allow them to underwrite and rate policies, secure reinsurance, pay claims, fight fraud, and protect their policyholders in lawsuits. The use and exchange of personal information is vital to insurance companies' ability to carry out their duties and obligations under their insurance contracts, as well as those imposed by statute and regulation. It therefore is critical that new federal privacy requirements preserve insurers' ability to execute the various elements of the insurance transaction.

The privacy subtitle of H.R. 10 as approved by the House of Representatives satisfies this requirement. The provision contains a number of exceptions that enable insurers to continue to serve their customers, without compromising legitimate privacy needs. For example, the bill excepts information transfers that are necessary to effect, administer, or enforce insurance transactions from otherwise applicable "opt out" requirements between unaffiliated third parties. This exception specifically covers disclosures that are needed for insurance underwriting, reinsurance, insurance account administration, insurance premium processing, insurance claims processing, insurer fraud prevention, insurance benefit administration, research activities, and other insurance functions specifically permitted by state or federal law. Absent such an exception, insurance companies would not be able to serve the most basic needs of their policyholders because they would have no basis upon which to underwrite risks or process claims or otherwise effect insurance transactions.

The bill permits information sharing between insurance companies and insurance guaranty funds, rate advisory organizations, and rating agencies. Here, too, the consumer is well-served. For example, guaranty funds are state-established mechanisms designed to step into the shoes of an insolvent insurance company in order to protect policyholders

and claimants. It is critical for an insolvent insurer to be able to share information with the guaranty fund so that its claims can be properly paid. Similarly, because state insurance codes require insurers to submit data to justify their rates, it is critical to allow data transfers between insurance companies and state-authorized rate advisory organizations. Private rating agencies, also covered by this provision, assess the financial strength and claims-paying ability of insurance companies, and make these ratings widely available to state regulators and the public at large.

Another provision permits information sharing that is necessary to protect against fraud, unauthorized claims, or other liability, as well as to facilitate risk management and resolve customer disputes. These, too, are critical insurance functions. Insurance companies work with law enforcement agencies and state-sanctioned fraud bureaus to detect and defer fraud and other criminal activity, such as arson and theft. This activity directly benefits policyholders and the public by preventing crime and reducing the costs of insurance. Property/casualty insurance companies also use accident data to improve safety standards for the home and highway.

#### Privacy Mandates Should Not Undermine The Core Principles of H.R. 10

Whether enacted as part of H.R. 10 or on a stand-alone basis, new privacy mandates should not undermine the core principles of financial modernization legislation, which include expanded consumer choice, greater market efficiency, a level playing field for all competitors, and functional regulation.

Enactment of H.R. 10 is much needed and long overdue, so that our nation's archaic financial services laws will comport with the realities of a converging financial services marketplace. Sharing of customer information has become an important business tool in this new market, and it has allowed financial services firms to offer customers specific, tailored products that will meet their needs. At the same time, legitimate concerns that have been expressed about privacy must be addressed. The privacy provisions of H.R. 10 as passed by the House of Representatives strike an appropriate balance between expanded consumer choice and protection of those consumers' personal financial information. Moreover, while they will increase regulatory compliance and marketing costs for many financial institutions, there was a conscious effort by the House to avoid restrictions that would have undermined the consumer benefits provided by H.R. 10.

Creating and maintaining a level playing field among all financial services institutions is another important principle of H.R. 10. A key component of the level playing field concept is that financial institutions offering similar products are treated as similarly as possible, regardless of their size or corporate structure.

The privacy provisions of the bill draw a significant distinction between information sharing among affiliated and unaffiliated financial institutions, specifically with respect to "opt out" requirements, which apply to disclosures of personal financial



information among unaffiliated third parties but not to disclosures of such information among affiliates in a holding company structure.

For some insurers, this distinction between affiliated and unaffiliated financial institutions is a major concern. However, we are pleased that the House attempted to address this issue by including two provisions that are important to the insurance industry. The first permits the transfer of personal financial information between insurance companies and independent agents who are operating on the company's behalf. This provision is critical to the on-going vitality of the independent agency system, which has served consumers extremely well since the birth of the American insurance system. Absent this important exception to otherwise applicable opt out requirements, insurance companies would be forced to form captive agency operations in order to assure the free flow of customer information that is necessary to market their products.

Another important provision allows unaffiliated financial institutions to share customer information—subject to limitations and protections not applicable to the sharing of information among affiliates—if this is done as part of a joint effort to offer, endorse, or sponsor financial products or services and the customer is fully informed about each institution's participation. Such joint agreements would be permitted only between financial institutions—not between an insurance company and a mail-order catalogue, for example. While this provision does not create a perfectly level playing field between affiliated and unaffiliated financial institutions, it should at least allow independent financial firms to continue to stay competitive, and not be forced into a holding company structure.

The final principle of H.R. 10 which we would like to bring to your attention is functional regulation, through which federal bank regulators oversee bank products, and state insurance regulators oversee insurance products. For the privacy provisions to operate effectively, insurance, banks, and securities regulators all must have appropriate jurisdiction over the privacy practices of the institutions under their jurisdiction. At the same time, it is important to avoid the application of contradictory regulations or standards to financial institutions that are sharing customer information with each other. This is further complicated by the fact that insured depository institutions and securities firms are regulated at the federal level, while insurance regulation is a state function.

The privacy provisions of H.R. 10 as passed by the House provide a sensible approach to functional regulation. In order to assure that uniform regulations are applied to all financial institutions, the federal banking agencies, the National Credit Union Administration, and the Securities and Exchange Commission, after consultation with the Federal Trade Commission and state insurance authorities, are directed to jointly prescribe regulations to carry out the privacy requirements of the Act. It is critical to involve insurance regulators in this process, given the unique attributes of insurance companies in this regard, and the approach taken in H.R. 10 does so in a way that is consistent with Congressional authority to direct state action. Moreover, given our concern about the Federal Trade Commission's authority to impose mandates on

companies which it does not functionally regulate, we think it is appropriate to grant the FTC consultative, as opposed to prescriptive, authority.

With respect to enforcement, the subtitle provides that the jointly prescribed regulations referenced above are to be enforced by the functional regulators for each industry, including, in the case of insurance, the state insurance authority in the state where the company in question is domiciled. We support this approach because it is consistent with the principles of functional regulation provided elsewhere in H.R. 10.

#### Conclusion

Despite the wide range of federal, state, and private sector privacy protections that are currently in place, many Americans are concerned about how personal information about them is circulated and used by their financial institutions. The Oxley/Pryce/Roukema amendment to H.R. 10 is a constructive response to these concerns. As Congress considers the financial privacy issue in more detail, any new legislative or regulatory privacy requirements must take into account the legitimate information sharing needs of insurers and other financial institutions. We look forward to working with you in this process.

William P. Binzel  
Vice President  
Government Relations

**MasterCard International**  
Global Communications  
1401 Eye Street, N.W.  
Suite 240  
Washington, DC 20005-2225  
202 789-5972  
Fax 202 789-5964  
Internet Home Page:  
<http://www.mastercard.com>

*MasterCard  
International*



July 21, 1999

The Honorable Marge Roukema  
Chair, Subcommittee on Financial Institutions and Consumer Credit  
Committee on Banking and Financial Services  
U.S. House of Representatives  
2129 Rayburn House Office Building  
Washington, DC 20515

Dear Madame Chair:

On behalf of the 23,000 member financial institutions, serving consumers in 220 countries and territories around the world, MasterCard International joins in the testimony and views expressed today by the financial services industry's witness, L. Richard Fischer.

MasterCard concurs in the position that existing laws governing the sharing of information by financial institutions provide a broad array of effective consumer privacy protections while permitting a flow of information that greatly enhances consumer choice and is vital to the American economy.

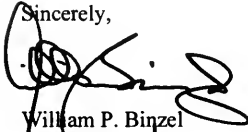
Specifically, MasterCard endorses and supports the following key points included in Mr. Fischer's testimony:

- Maintaining customer confidentiality is a cornerstone of the financial services industry. Market-driven dynamics and an ever-increasing public focus on privacy compel each financial institution to meet the privacy wishes of its customers.
- Information sharing benefits consumers, the economy, and the financial services industry. This practice provides consumers with innovations in products and services that today's marketplace demands while allowing the industry to control costs, risks, and fraud.

- Existing laws already regulate information sharing and provide consumers with extensive privacy protections.
- The banking industry's self-regulation is vibrant, effective, and increasing. Self-regulation is supported by industry tradition and spurred by competition and consumer demand. For example, the banking industry was one of the first to adopt industry-wide privacy principles and has demonstrated continued leadership in consumer privacy education programs.

I respectfully request that this statement be included in the Subcommittee's hearing record at the beginning of Mr. Fisher's testimony.

Sincerely,

A handwritten signature in black ink, appearing to read 'W. Binzel', with a large, stylized flourish extending to the right.

William P. Binzel  
Vice President, Public Affairs  
MasterCard International Incorporated

○

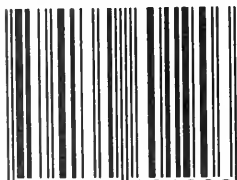


BOSTON PUBLIC LIBRARY



3 9999 05903 569 9

ISBN 0-16-060190-8



9 780160 601903



90000



