UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ELECTRONIC FRONTIER FOUNDATION Plaintiff, v. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE and UNITED STATES DEPARTMENT OF JUSTICE Defendants.	)	Civil Action Nos. 08-1023 08-2997

DECLARATION OF J. MICHAEL McCONNELL,
DIRECTOR OF NATIONAL INTELLIGENCE

I, J. MICHAEL McCONNELL, hereby declare and state:

1. I am the Director of National Intelligence (DNI) of the United States. I have held this position since February 2007. Previously, I have served as the Senior Intelligence Officer for U.S. Seventh Fleet, the Assistant Chief of Staff for Intelligence for the U.S. Pacific Fleet, the Director of Intelligence for the Joint Chiefs of Staff during Operation Desert Storm, and the Director of the National Security Agency.

I. Purpose of Declaration

2. I am aware that the plaintiff in this case has made Freedom of Information Act (FOIA) requests for, among other things, records concerning communications from the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ) to any member of the Senate or House of Representatives or their staffs concerning amendments to the Foreign Intelligence Surveillance Act of 1978 (FISA). I am also aware that the plaintiff has challenged the government's decision to withhold

certain records responsive to this request. I am providing this declaration to support the government's decision to withhold two categories of records: 1) e-mails relating to the FISA reform legislation that Executive Branch staff, including White House staff, exchanged with each other and with congressional staff; and 2) records reflecting communications between the ODNI and/or the DOJ and representatives of telecommunication companies.

3. I have reviewed the declarations of Daniel Meyer, Assistant to the President for Legislative Affairs; Kathleen Turner, Director of Legislative Affairs for the ODNI; and Kenneth Wainstein, formerly the Assistant Attorney General for DOJ's National Security Division and currently the Assistant to the President for Homeland Security Affairs.

4. Based on these declarations, my personal knowledge, and information made available to me in the performance of my official duties I hereby attest that the communications reflected in these documents were instrumental to the enactment of the Protect America Act of 2007 ("Protect America Act"), Pub. L. No. 110-55, and the FISA Amendments Act of 2008 ("FISA Amendments Act"), Pub. L. No. 110-261, both of which effected necessary overhauls (the former on a temporary basis) of the legislative scheme governing aspects of foreign intelligence surveillance. I also attest that the development of a legislative product capable of garnering the President's signature would have been considerably more difficult, if not impossible, had the Executive and Legislative Branch participants in these discussions known that their communications would be subject to public disclosure under FOIA.

5. Other declarations being submitted to the Court also describe the documents that ODNI and DOJ have withheld that could reveal the identities of particular telecommunications companies that may have assisted, or may in the future assist, the government with intelligence activities. I believe that disclosing this material could reveal intelligence sources and methods that I am required by statute to protect.

II. Office of the Director of National Intelligence

6. Congress created the position of the Director of National Intelligence in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the United States Intelligence Community and as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. 50 U.S.C. § 403(b)(1), (2).

7. The United States Intelligence Community includes the Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the military services, the Federal Bureau of Investigation, the Office of Intelligence and Analysis of the Department of Treasury, the Office of Intelligence and Counterintelligence of the Department of Energy, the Drug Enforcement Administration, and the Coast Guard; the Bureau of Intelligence and Research of the

Department of State; the elements of the Department of Homeland Security concerned with the analysis of intelligence information; and such other elements of any other department or agency as may be designated by the President, or jointly designated by the DNI and the head of the department or agency concerned, as an element of the Intelligence Community. 50 U.S.C. § 401(a)(4).

8. The responsibilities and authorities of the DNI are set forth in the National Security Act of 1947, as amended, and Executive Order 12333, as amended. These responsibilities include ensuring that national intelligence is provided to the President, heads of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 403-1(a)(1). The DNI is charged with establishing the objectives of; determining the requirements and priorities for; and managing and directing the tasking, collection, analysis, production, and dissemination of national intelligence by elements of the Intelligence Community. 50 U.S.C. § 403-1(f)(1)(A)(i) and (ii).

9. In addition, the National Security Act of 1947, as amended, states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 403-1(i)(1). Consistent with this responsibility, the DNI establishes and implements guidelines for the Intelligence Community for the classification of information under applicable law, Executive Orders, or other Presidential directives and for access to and dissemination of intelligence. 50 U.S.C. § 403-1(i)(2)(A), (B).

10. By virtue of my position as DNI, and unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. 50 U.S.C. § 403-1(b).

III. The Foreign Intelligence Surveillance Act

11. Leading up to the enactment of the Protect America Act and the FISA Amendments Act, I testified before Congress a number of times both in public and closed sessions regarding the need to update the FISA. As I said in my open testimony, certain information regarding the need for FISA reform cannot be discussed publicly because it is classified. However, I provided as much information in open sessions as was possible. FISA reform was one of my highest priorities because shortly after becoming the Director of National Intelligence it became clear to me that changes in technology since the enactment of FISA had begun to degrade our foreign intelligence collection capabilities.

12. FISA is the nation's statute governing the conduct of electronic surveillance and physical searches for foreign intelligence purposes. FISA also has provisions governing pen register/trap-and-trace surveillance and access to certain business records. It is a complex statute that was intended to balance two fundamental national imperatives: the collection of foreign intelligence information and the protection of the civil liberties and privacy rights of United States persons. Generally, FISA provides for the establishment of a special court -- the Foreign Intelligence Surveillance Court -- to review applications seeking approval of electronic surveillance and physical search authority against foreign powers and agents of foreign powers within the United States.

13. Shortly after I began as DNI, I was informed of challenges the Intelligence Community faced in collecting foreign intelligence under FISA, and determined, along with the President and others in the Intelligence Community, that FISA reform was necessary in order to maintain the speed and agility expected and required of the nation's surveillance capabilities. The attacks of September 11, 2001 made the need for FISA reform even more apparent. There were two primary concerns. Our first concern was that significant post-1978 advances in the sophistication of communications technology had rendered certain elements of the FISA, which were premised on 1978 technology, out of date. Our second concern was that a number of private sector entities had been sued for allegedly assisting the government with surveillance activities. This increasing risk of legal liability was threatening to choke off the willingness of the private sector to cooperate with government in the acquisition of critical foreign intelligence information.

14. Accordingly, the Administration proposed, on the President's behalf, a FISA reform agenda that sought to modernize the regime established by FISA in a manner that honored and preserved FISA's legacy of protecting both the privacy and security of Americans. Two primary changes were at the heart of the FISA reforms that the Administration sought. First, as I explained in testimony before the House Permanent Select Committee on Intelligence and the House Judiciary Committee in September 2007, although Congress had intended in 1978 to exclude surveillance aimed at the communications of certain foreign intelligence targets outside the United States from FISA's requirement of prior judicial approval, changing technologies and the migration of communications from satellite and radio to fiber optic cables located in the United States were increasingly bringing those overseas communications within FISA's purview.

See Statement of J. Michael McConnell, Hearing on the Protect America Act of 2007, H. Permanent Select Comm. on Intelligence, (110th Cong.), pp. 3-6 (Sept. 20, 2007). Reversal of FISA's unintended expansion was necessary to return to the balance struck by Congress in 1978 and to halt the increasing diversion of scarce and specialized intelligence personnel and resources to the judicial approval process for targets outside the United States. In short, as a result of technological changes, the FISA regime was unnecessarily hampering the Intelligence Community's ability to more effectively and efficiently collect foreign intelligence information. Second, it was essential to extend both prospective and retroactive liability protection to those private sector entities that had provided or would in the future provide authorized assistance to the government in collecting foreign intelligence information. *See id.* at 17. The issue of retroactive immunity was particularly urgent because private plaintiffs had filed a number of lawsuits against certain telecommunications providers alleged to have improperly aided the government in connection with communications intelligence activities following the terrorist attacks of September 11, 2001. Quoting from a Senate Intelligence Committee report on proposed legislation (S.2248), the Attorney General and I expressed the view in a February 22, 2008 letter to the Hon. Silvestre Reyes that, in the absence of retroactive liability immunity, "the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation." Letter for Hon. Silvestre Reyes, Chairman, House Permanent Select Committee on Intelligence, House of Representatives, from Michael B. Mukasey, Attorney General, and J. Michael McConnell, Director of National Intelligence, at 5 (Feb. 22, 2008), *reprinted in* 154 Cong. Rec. H1797, 1799-1801 (Mar. 31, 2008) (statement of

Rep. Dent) (hereinafter "Reyes letter"). We also believed that it was unfair to punish providers who may have tendered assistance to the Intelligence Community in good faith reliance on government assertions of legality, particularly in light of the exigent circumstances following the attacks of September 11. *See id.* at 4-5.

15. In April of 2007, the Administration submitted proposed legislation to Congress that would have made the fixes that the Intelligence Community believed necessary to the FISA regime. In August of 2007, Congress passed and the President signed the Protect America Act, a temporary measure that helped close critical intelligence gaps even though it did not incorporate all of the Administration's proposals. Among other things, the Protect America Act: (i) removed the surveillance of targets located outside of the United States from the definition of electronic surveillance; (ii) provided for judicial review of the procedures by which the Intelligence Community determines that surveillance targets persons located outside of the United States; (iii) established a mechanism to compel communications providers to cooperate with government surveillance; and (iv) afforded liability protection to private parties that assisted the Intelligence Community pursuant to a lawful directive issued under the PAA. Congress also provided, however, that the authorities conferred by the PAA would expire in February of 2008. Congress thus gave the Intelligence Community the ability to collect foreign intelligence information from overseas targets more efficiently and effectively, but only on a temporary basis.

16. After the passage of the Protect America Act, a flurry of legislative activity ensued to work toward a long-term solution, with the House and Senate passing separate bills—H.R. 3773 on November 15, 2007, and S. 2248 on February 12, 2008,

respectively—that substantially differed in certain important respects. Debate and discussions involving Congress and the Executive Branch continued into 2008, and the authorities provided for in the Protect America Act expired on February 16, 2008, without a long-term agreement having been reached. As the Senate and the House considered differing versions of alternative FISA reform legislation, the Intelligence Community was able to continue with on-going surveillance activities pursuant to the authorizations under the Protect America Act. But once the Protect America Act expired, the Intelligence Community was unable to initiate any new measures under its authority. In late June of 2008 congressional leaders reached agreement on a compromise bill -- H.R. 6304 -- that majorities in both the House and Senate were willing to accept and that the President was prepared to sign, as he did on July 10. The FISA Amendments Act provided for the ability to conduct surveillance of targets located outside of the United States for foreign intelligence purposes, and a procedure for the dismissal of lawsuits brought against companies that were alleged to have assisted the government with communications intelligence activities after September 11. The legislation contained additional provisions, including the establishment of a new judicial framework for reviewing certain required documentation and significant additional Executive Branch and Congressional oversight provisions. The FISA Amendments Act was the quintessential product of legislative compromise, and without question, the American people have benefited from the enactment of this important piece of legislation. The FISA Amendments Act has made the nation safer by ensuring that the Intelligence Community can react with the speed and agility necessary to help safeguard against future terrorist attacks and other foreign threats.

17. The ultimate passage of the FISA Amendments Act -- by votes of 69-28 in the Senate and by 293-129 in the House -- demonstrates that large majorities in both Houses of Congress ultimately came to agree in large part with the core of the Administration's positions. However, because of the initial disagreements, the legislative process that resulted in the development of the final, successful compromise legislation was long and extremely delicate. Congress and the President reached agreement only after more than two years of intense and complex discussions and deliberation. Patient, focused, and sustained engagement between the Legislative and Executive Branches over a number of iterations of legislative proposals and counter-proposals was absolutely critical to the Government's ability to come together on a compromise package of reforms.

IV. Communications with Congress

18. In formal communications to Congress, the Administration expressed the view that a number of the objections to our reform proposal expressed by certain Members were misplaced and that the legislative proposals offered as alternatives were inadequate and unwise. *See, e.g.*, Letter to Hon. Harry Reid, Majority Leader, U.S. Senate, from Michael B. Mukasey, Attorney General, and J. Michael McConnell, Director of National Intelligence (July 7, 2008), *reprinted in* 154 Cong. Rec. S6400 (daily ed. July 8, 2008) (presenting the Administration's views); Reyes Letter, *supra*, at 2-4; Letter to Hon. Harry Reid, Majority Leader, U.S. Senate, from Michael B. Mukasey, Attorney General, and J. Michael McConnell, Director of National Intelligence (Feb. 5, 2008) (presenting the Administration's views), *reprinted in* 154 Cong. Rec. S651 (daily ed. Feb. 5, 2008). These formal communications, although an important part of the

legislative process, were naturally limited in their ability to move the parties toward resolution of their differences. The opportunity for the Branches to participate in confidential informal dialogue and deliberations greatly enhanced the prospect that they would understand each other's concerns and reach a compromise legislative position. The communications relating to the FISA reform legislation that are at issue in this case, which consist primarily of e-mails that Executive Branch staff, including White House staff, exchanged with each other as well as with congressional staff, contributed in many important ways to ensuring the passage of a final legislative package that could garner the President's approval.

19. These informal inter-Branch communications facilitated the transfer of important, relevant information to decision-makers in both the Executive and Legislative Branches. For example, in preparation for a meeting to discuss a legislative proposal, Legislative Branch staff at times provided detailed comments on specific proposed language so that their counterparts in the Executive Branch would be prepared to discuss the language at the meeting. In addition, Legislative Branch staff sent a number of e-mails to Executive Branch staff to inform them about important developments in the legislative process, such as the suggestion of alternative legislative language proposed by Members of Congress and the status of various alternative reform proposals. These communications were vital to the Executive Branch's ability to respond adequately and appropriately to such proposals and developments.

20. Informal inter-Branch communications also enabled staff within Congress and the Executive Branch to assist and advise each other with respect to FISA reform proposals, and to suggest possible approaches to and modifications of these proposals.

For example, Executive Branch staff were able to assist Congressional staff in determining the best approaches to particular policy or legal problems and in crafting technical legislative language that accomplished the intended effect. This assistance was of great importance given that the intelligence and national security professionals in the Justice Department and ODNI are among the most knowledgeable in the country about the surveillance capabilities necessary to thwart future attacks and the complexities of the intelligence laws. As the communications at issue in this case reflect, congressional staff often actively sought out the assistance of staff in the Executive Branch in crafting legislative provisions. Executive Branch staff also used informal communications to persuade congressional staff of the need for particular legislative approaches. By sharing their knowledge with congressional staff at an informal level, Executive Branch staff were able to make a sustained, forceful, and substantive case for the necessary reforms, which could then be passed on to other congressional staff and, ultimately, legislators. The sharing of legislative drafts was an integral part of the two-way exchange of information between the Executive Branch and Congress because it provided an opportunity to review actual legislative language, and thus to evaluate how alternative approaches would function in practice. The existence of informal communications enabled staff in each Branch to express their respective concerns to the other Branch, and it also facilitated fruitful discussions over the contours of the emerging legislation.

21. Although the parties had taken positions that appeared far apart initially, consensus became possible as continuous inter-Branch dialogue allowed movement towards a compromise solution. Free and candid inter-Branch communications through

confidential, informal channels facilitated the crucial compromise that broke the legislative impasse in July of 2008.

22. The discussion surrounding FISA modernization and liability protection for telecommunications providers became extremely controversial in the public arena. The ability of the Executive and Legislative Branches to have informal reasoned and thoughtful discussions regarding the concerns that were raised and the various legislative options was absolutely crucial to Congress's ultimate passage of the FISA Amendments Act. I believe that the possibility of public dissemination of the necessarily confidential and sensitive communications exchanged between Executive Branch and congressional staff with respect to these subjects would have severely compromised the candor, objectivity, and effectiveness of their conversations. As a general matter, it is my experience that the possibility of public dissemination of sensitive communications tends to cause individuals in government to be inhibited in what they say. It is my firm belief that the resulting legislative compromise would not have been achieved, or at least would have been delayed even longer than it was, had those engaged in the informal, non-public inter-Branch communications at issue in this case believed that their communications would be disclosed pursuant to the FOIA.

V. Communications with Representatives of Telecommunication Companies

23. During the legislative process described above, the ODNI and DOJ at times communicated with representatives of telecommunications companies. These communications are described and explained in more detail in various other declarations being submitted in this case. I am aware that the Government has withheld information

that could reveal which private parties were communicating with the ODNI and DOJ relating to FISA.

24. Whether any particular private party assists the government with intelligence activities is highly sensitive and must not be publicly disclosed. First, private entities typically agree to assist the Intelligence Community only after receiving assurances that their assistance to the government will not be publicly disclosed. Those that cooperate do so at great financial and personal risk. The potential of public disclosure that a particular company or CEO is assisting the government could lead private entities to refuse to assist the government in the future, which would be extremely damaging as it would impede the government's ability to gather intelligence information that is vital to the protection of our nation. In certain instances, the Intelligence Community simply cannot gather needed information without the assistance of the private sector. It is, therefore, vital that the Intelligence Community do everything it can to protect the identities of private entities that cooperate with the Intelligence Community, and it is no less imperative to do so in this instance.

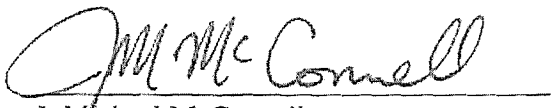
25. Furthermore, to disclose publicly which entities may or may not be assisting the government with intelligence activities provides our adversaries with extremely valuable information about our sources, methods and capabilities. Foreign adversaries could avoid certain communication methods or could target their resources against particular private sector entities and attempt to impede them from assisting the government in this way. The impact of disclosure of which entities are now, or may in the future, assist the government would be highly damaging to our intelligence operations and to our national security. We simply cannot take that risk and must, therefore, refuse

to confirm or deny whether or not any particular company is assisting the government with intelligence activities.

26. I am aware that the records in this case consist of faxes, letters and e-mail messages between the ODNI and/or DOJ and representatives of telecommunication companies about potential FISA amendments. I believe that disclosure of this type of material would allow the public and our adversaries to draw inferences about which companies are assisting us and which are not. Although it is true that companies that are not assisting the government may have contacted us to discuss liability protection due to the fact that they had been sued for alleged activities, I believe that taken as a whole, the type of information being withheld from plaintiffs could be viewed as confirming which private parties are or are not assisting the government, and that this information must be protected. Moreover, whether or not these inferences are correct is irrelevant. If the public or our adversaries believe that they know who is assisting us, significant damage to those entities could result.

27. I am required by the National Security Act of 1947, as amended, "to protect intelligence sources and methods from unauthorized disclosure." See 50 U.S.C. § 403-1(i)(1). I hereby assert my authority under the National Security Act to protect any information which could reveal whether any particular telecommunications company is assisting the U.S. Government with intelligence activities.

Executed this 5TH day of December, 2008



J. Michael McConnell