


Exhibit A

Expectations of Privacy: Balancing Liberty, Security, and Public Safety

- 
- James B. Comey
- Director
- Federal Bureau of Investigation
- Center for the Study of American Democracy Biennial Conference, Kenyon College
- Gambier, OH
- April 06, 2016

Remarks as delivered.

Thank you so much President Decatur. I wish I could explain to my parents as well as you just explained it why they were paying for an education in chemistry and religion. They thought it was about alchemy or something.

Thank you all for being here. I very much appreciate your taking the time on a rainy weeknight. There's only one of you who is required to be here and that is my son. The rest of you could have actually been enjoying a little free time before finals. As the weather has finally improved, I am very grateful that you've taken the time to stay and to listen to me and I hope to talk with me, because I want to share some thoughts and I'd like to have a conversation with you that focuses on the things you'd like to know about, and the things you'd like to test me on, and push me on. That you're here means you care about these issues which I do very much, and this is a great thing that Kenyon is sponsoring this conference.

Tonight I want to talk to you about privacy as the keynote speaker. I also want to talk to you about how we might have better conversations about privacy, how we deal with the issues of privacy, how we think about the costs associated with the tough decisions will affect your lives—I'm talking to the students now—most of all and longest. I think we need to find a way to make smart balanced decisions. Ones that will serve us well over the long run, and to make good decisions we have to find a way to have good conversations about things that matter, and that can often separate people of goodwill. Let me start with something you heard earlier, expectations of privacy.

What does privacy mean to you? What are your expectations, and what should they be? Right now I suspect your privacy revolves mostly around social media, and your personal lives. You don't want your mom to see the text you're exchanging with somebody in bio class. You don't want your next employer to know that you're a big fan of taking fish gape selfies with your friends. I understand the fish gape has replaced the duck face in selfie world. I am much cooler than I appear to be.

You want to keep your nosey relatives from reading your Facebook posts, your tweets, visiting your Instagram account, looking at your texts. You really don't like the idea of the government, law enforcement in particular, seeing any of it, not pictures, not texts, not tweets, who your friends are, where you've been online. I get that, I really do. I don't want anybody looking at my stuff either. I don't want anyone poking through my Instagram account, which has seven followers. They're all my children, my spouse, and I've let one son-in-law in so far.

As much as I get that, I also think there are other perspectives in play, other issues to consider. Imagine this, what if law enforcement had a phone owned by somebody who abducted your sister? A phone used by a suicide bomber who blew up the train station in your hometown? The phone of somebody who hurt a little kid in your neighborhood? Would that cause you to think about it differently? I think it should, or at least it should change the way that we have a conversation about it, and I'll tell you why.

In this great country, we often have a reasonable expectation of privacy in our houses, in our cars, in telephone booths, in our devices, that makes good sense. That has long meant that the government could not invade our privacy without good reason reviewable in court. It also meant that with good reason, law enforcement could enter private spaces. Since the founding of our country, if law enforcement had probable cause to believe that there was evidence of a crime in some space, whether that's a house, or a vehicle, or a device, some space that you controlled, law enforcement could go to a judge and get a warrant, go to that private space look through your stuff.

They could search wherever the judge said they could, in your car, in your closets, in your computer, in your phone. They could take whatever the judge said they could take. There are vital constraints on law enforcement, and we must never ever forget them, but the general principle is one we've always accepted in this country. There is no such thing as absolute privacy in America. There is no place outside the reach of judicial authority. That's a bargain that we made with ourselves 240 years ago to achieve two things we all treasure, liberty and security.

And that bargain—"No invasion of private spaces without good reason and appropriate oversight"—has made America a country rooted deeply in the rule of law. It has also meant that there are no absolutes in American life. All kinds of interactions that are incredibly important to everybody here, and to me, incredibly personal and private, none of them are absolutely so under the law.

Private conversations that matter most to us often at the most difficult moments in our lives, conversations with our doctors, with our attorneys, with our therapists, with our lawyers, with our spouses, with reporters, with all kinds of people that we have to have important conversations with, those are all protected by law, but none of them absolutely so.

All of those zones of privacy can be pierced if a court finds compelling reasons to do so, and have long been physical spaces in our lives that are intensely personal, and private to all of us, but none of them absolutely so. Safe-deposit boxes, storage units, car trunks, our diaries, even if we have one of those

little locks on them, all of those things, all of those things can be opened if the interests favoring opening them are compelling. As strange as it sounds even our memories are not absolutely private.

Anyone of us could be compelled by a judge to testify about what we saw, what we heard, what we remember. We can be compelled to say what's in the content of our minds even if it would hurt us, even if it was incriminating to us so long as we were protected from the government's use of that information by an immunity order. In America we've always balanced privacy and security. It can be messy, it can be painful, but we've always worked through the three branches of government to achieve that balance in a sensible way.

The country's effort to achieve that balance for over 200 years was not complicated by technology, because there was no widely available space in American life that couldn't be entered if there was a court order. No car, no trunk, no closet, no safe-deposit box, no safe that couldn't be opened if a judge said it should be open. Here's what changed, the advent of widely available strong encryption has changed the entire thing. It's really happened in a huge way just in the last three years.

I say it that way because encryption has always been around at least for decades, always available to the sophisticated user, both for data at rest sitting on a device, and data in motion being transmitted over a line. What's changed in the last few years is that it has now become the default covering wide swaths of our lives, and covering wide swaths of law enforcement's responsibilities. For mobile devices for instance, Apple and Google made the move to encrypt the devices only in late 2014.

It seems like a lifetime ago, WhatsApp announced that encryption moved on all of their services yesterday. A billion people now communicating in ways that can't be intercepted even with a judge's order. Today those of us in law enforcement are confronted with boxes that can't be opened. We face devices that we can't open, we face data that even if we're able to collect it with a court order, we can't read it. It's gobbledygook to us, so encryption brings us to a place or to quote a portion of the Fourth Amendment, all of our papers and effects can be entirely private to a place where nobody can listen to our conversations, read our texts, look at our documents, see our pictures, know what's in our e-mails, unless we give them permission, unless we say so.

There is a lot to love about this. I love strong encryption. It protects us in so many ways from bad people. It helps the FBI with our mission, which centers on protecting privacy and fighting hackers. In many ways I think all of us like the idea of a storage space in our lives that no one can get into, a safe box that's only mine, but it takes us to a place of absolute privacy that we have not been to before where the balance we have long struck is fundamentally challenged, and changed.

That's why we have to talk about it, that's why we have to have an adult conversation about the balance that means so much to all of us, because no matter how you feel about it, you have to acknowledge there are costs to this new world. You may decide the costs are outweighed by the benefits, or you may decide that there's nothing we can do about it technologically, but you simply have to as part of the

conversation stare at the cost in a fair way. The reason for that is we are not the only ones who love strong encryption.

Child predators love it, organized criminals love it, terrorists love it, and it's part of their tradecraft. Hackers love it in all of their work. All of those people understand the power of strong encryption. ISIL, the so-called Islamic State, uses mobile messaging apps that are encrypted end-to-end to reach its followers, motivate them, and then direct them. We work very, very hard in the FBI to track those who might be moving to violence on ISIL's behalf, but sometimes it's like searching for a needle in a haystack. When that needle moves to a mobile messaging app that's end-to-end encrypted, that needle disappears.

The great fear that dominates our lives is that that needle's going to reappear at a train station wearing a suicide vest. As I said before, we can get a court order, but what we collect is unreadable. Last spring to give one example, a group of terrorists tried to attack, and did attack a "Draw Mohammed" contest in Garland, Texas. Before that attack, one of those people in Texas exchanged 100 messages with an overseas terrorist. We today have no idea what they said to each other, because they used a mobile messaging app that was end-to-end encrypted.

We can look at that, it's gobbledygook to us. This isn't a problem just in national security cases. Last spring an eight-month pregnant woman opened her front door in Baton Rouge, Louisiana, to somebody she apparently knew, and that person killed her. The case is cold already, her mom says she kept a detailed diary on her phone. The phone was there with her body, and the phone is locked, and we can't open it. We don't know what was going on in her life that she confided to her diary, and that case remains unsolved.

These are powerful and painful examples, but I think everybody has to agree that whether you work in technology, or law enforcement, or you simply own a phone, which I think is all of us, the logic of strong encryption means that all of our lives, including law enforcement's life will soon be affected by strong encryption. We live our lives on these mobile devices, and when those are off-limits despite court orders, our world changes.

My first point is simply we have a problem.

Maybe there is nothing that can be done about it, maybe there is, but we should weigh things differently. I hope we will start with the common ground, that ubiquitous strong encryption is bringing significant change to the way we think about liberty and security. We should try to have a thoughtful conversation about what we do about it as a people. Let's turn to what I hope, what I dream that conversation can be like.

I have discovered that it is incredibly difficult to have a good conversation about the impact of encryption on law enforcement and national security.

There is for reasons I don't fully understand, an intensity of emotion around the issue on all sides that makes even really bright people struggle to find balance and empathy that they might otherwise bring readily to hard topics. A group of technology companies last year sent the letter to President Obama where they urged him to promise never to seek legislation to address the intersection of encryption and public safety. That's certainly an understandable position, and these were serious people from serious companies.

When I read the letter at the time, I said something that maybe one of those things that's in your head, you said, "Did I say that out loud?" I did say it out loud, and I meant it so I'm going to repeat it, I said, "I think the letter is depressing." The reason I said that is, the letter did a great job of talking about awesome things that encryption offers all of us, and I agree with all that. The letter made no mention of the impact on public safety, and to my mind that meant either that these folks writing the letter didn't understand the potential costs, or that they weren't being fair-minded about it.

Either way that was a depressing thing, because to me it said either we have to spend a ton more time trying to have people understand why we're talking about this, or a ton more time trying to get people to be open and fair with us in the conversation. I've got to tell you I found a whole lot of the rhetoric of that we have engaged in this country in connection with the recent litigation involving the government and Apple, I found a whole lot of it similarly disheartening.

First let me make sure though that we're all on the same page when it comes to that case. In December, two terrorists attacked an office gathering in San Bernardino, and they killed 14 people and wounded 22 others. They left behind three phones. Two were cheapo phones that they smashed, and we could not recover anything from them. The third was an iPhone 5C running IOS 9, and that matters. It was a phone owned by one of the killer's employers, the County of San Bernardino.

For the FBI to competently investigate a mass murder in the United States, we believe we had to use all lawful tools to find out whether there was evidence on that phone that either shed more light on what these two killers had done, or shed light on who else might be involved and still out there. We got a search warrant, and we got consent from the phone's owner—the county—and we tried to open the 5C. We checked with everybody inside the U.S. government, and we checked with a whole lot of people outside of the U.S. government to see if anybody had a solution that will allow us with the court order to open a 5C running IOS 9.

The danger is if we try to guess the passcode beyond the 10th guess, the phone may well auto encrypt permanently, essentially erase itself. Even if that feature goes away, guessing would take us decades, because the phone is designed to have each guess require a longer period of time as you wait to make the next guess, and to make the number of guesses you'd have to crack the code it would take us many, many years. We went to court, the court from which we'd gotten the search warrant, and the government's lawyers from the Department of Justice required a court order that would direct Apple to do a couple of things, two things:

Shut off that auto encrypt feature on the phone, and shut off the feature that delays successively longer periods after each unsuccessful guess. With those two features disabled, then the government would be able to try to guess the code, and our people are confident that they could guess it without those features, with electronic pulses in about 26 minutes. Under the judge's order, Apple would be required to write code for that phone to turn off those features. The phone could stay in Apple's possession, the software that they wrote would stay in Apple's possession.

Apple resisted the order, which is their right, and their main argument was that the court didn't have the authority to order them to take the step of creating software for that particular device, that it went beyond the court's authority to direct Americans to assist with the execution of court orders. That's a good-faith reasonable argument about a federal court's authority, and it's an interesting question. Obviously the government has a different view of the law there, because we believe that the court's authority does extend to such assistance, but it was Apple's right to make that argument.

If I were their lawyer, I would have made the same argument. I believe it was a reasonable argument even if I have a different view of the law, but beyond the reasonable arguments, the controversy over the Apple case, over the challenge of encryption more broadly, has been chock-full of slippery slope arguments, and absolutist arguments. If we do this for example, and you can supply your own "this," but if we open this phone, if we make this accommodation, then horrible things will inevitably happen.

It's the first step down a slippery slope, or a whole lot of folks have said things like, "We must protect privacy absolutely. Phones contain our lives, and they must be off-limits to the government." Now I know you've already learned this from your philosophy classes here at Kenyon, but every time you hear somebody making a slippery slope argument, an alarm should go off in your head. There is a reason your professors call this "slippery slope fallacy." It could be that if you take one step you'll inevitably fall down a slick slope, it could be.

It depends a lot on what kind of shoes you're wearing, whether the slope is a stairs slope, and whether there's a railing. It is a fallacy, because it is deceptively misleading. Sometimes one step leads inevitably to others, sometimes not; it depends upon a whole lot that a good conversation is needed to figure out. The notion that privacy should be absolute, or that the government should keep their hands off our phones, to me just makes no sense given our history and our values—something that President Obama said two weeks ago in Texas.

You may still end up disagreeing with the government, but starting from the position that privacy should be absolute is just not a fair-minded place to be in my estimation. What I find so frustrating about the emotion around encryption, is that very, very smart people who would otherwise be deeply skeptical of slippery slope, and absolute arguments in the context of other issues like guns, seemed less skeptical of those rhetorical techniques in this context for reasons that I honestly don't understand.

It is simply not the case that if Apple wrote software for the killer's phone it would inevitably be at

catastrophic risk, anymore than we are at catastrophic risk now that the government has purchased a tool that allows court-authorized access to the phone. As I mentioned, until late 2014, neither Apple nor Google made phones that law enforcement couldn't open, and with court orders they routinely opened those phones. Today, the iCloud is encrypted, Apple decrypts it in response to court orders, and produces the contents in law enforcement investigations.

In my view, privacy and security didn't end in 2014, and we are not ending it today. There are risks, there are benefits, there are steps that make us more secure, there are steps that make us less secure. It requires detailed facts, and balancing to assess how do those risks, how do those benefits change with each step? I believe the stakes are high enough that thoughtful people should work very hard to resist fallacies, and talk to each other in a fair-minded way. It's also not the case I believe that any infringement on privacy is to be feared.

The question we must all ask is this: So what's the nature of the infringement, and under what circumstances, and with what oversight, and what are the benefits of the costs associated with that incremental infringement? We have to find thoughtful, productive ways to talk about issues of privacy and security, and here's the thing, by thoughtful I don't mean that I'm right, and you're wrong. I could be wrong about the way I assess, the way I perceive, the way I balance, the way I reason, but I think all productive conversations start from a place of humility. I could be wrong.

I hope very much that you recognize that you could be too, and if we start there, that's the basis for a good conversation. On behalf of the grown-ups of the United States, I'd like to apologize that we have not done a good job in this country in recent years at modeling how to have good conversations about hard things. We tend to shout talking points at each other, or as we get cooler, even though we're old we launch tweets at each other without any real interest in questioning our own assumptions, our own perceptions, our own reasoning, and without an openness to be wrong, in whole or in part.

The litigation between the government and Apple over the San Bernardino phone has ended, because the government has purchased from a private party a way to get into that phone 5C running IOS 9. I think that's a very good thing for at least two reasons. First, that litigation really, really was about the government needing to get access to a terrorist's device. As I said at the time, we should be fired if we had a lawful means to get into terrorist's phone and we didn't try to. It was not—repeat not—about trying to send a message, or create a precedent.

We kept trying to find ways into that phone before we brought the litigation. We kept trying to find ways to get into that phone after the litigation, and one of the benefits, one of the maybe few benefits to all the controversy around it, is that a worldwide market of creative people was stimulated that hadn't existed before, where a whole lot of folks tried to see, "Could I break into a 5C running IOS 9?" Everybody and his Uncle Fred called us with ideas. We had people in Congress asking me about ideas during hearings, and I said, "I welcome all comers, this really is about trying to get into that phone."

We have a conversation we have to have about the broader issues. I don't want this to be part of it, I want to find out whether there's something we need to know in a terrorist's phone. Someone outside the government in response to that attention came up with a solution. One that I am confident will be closely protected, and used lawfully and appropriately. That's a very good thing for this terrorist investigation. Second, litigation is a terrible place to have any discussion about a complicated policy issue, especially one that touches on our values, on the things we care about most, on technology, on trade-offs, and balance.

It is a good thing that the litigation is over, but it will be a bad thing if the conversation ended, because we have to have it. It's unbelievably complicated, touching on every issue we care about, it has implications for safety, privacy, innovation, human rights, national security, international relations, and probably a few others that you can think of that I can't think of. It does not fit in a tweet. We must have the conversation because encryption's impact is great, wonderful in a lot of ways, and growing.

At some point it's going to figure in a major tragedy in this country. It is very hard for us as a people to have thoughtful conversations in an emergency, and in the wake of a major tragedy. We have to have this conversation now, and let me now show you what a dreamer I am.

I hope as we have this conversation that we will successfully resist some of the most challenging aspects of our very nature. One of the strongest forces I think in human experience is the confirmation bias.

That extraordinary aspect of our brains that makes us hungry for data, that is consistent with that which we already believe, and often keeps contrary data from reaching my consciousness. From never entering into my mind, because it got filed away before it got there. I don't know about you, but that is terrifying to me. I think it's part of the reason that humans can convince themselves of nearly anything, and then cling to it like a life raft in a storm. It's one of the things that should make all of us in government, out of government, skeptical of power.

John Adams once wrote to Thomas Jefferson, "Power always thinks it has a great soul." People, in my experience are at their most dangerous when they are certain their cause is just, and certain that their facts are right. Oh lordy, they are frequently certain of both. Today, even if you're tempted to doubt, you can be quickly reinforced by an echo chamber that's on your device 24 hours a day. It will buttress that which you already believe, so there's very little risk of you overcoming the confirmation bias that way.

To depress you further, I think humans also have a tendency to travel in packs, and surrender individual judgment to the will of a group, and allow the loudest voices to hijack that group, the lowest common denominator to hijack that group. That side of us is only reinforced today by the technology that's around us. By the world of reflexive likes and retweets. Human nature, and our respect for it, and fear of it, is the reason why all FBI agents in training, and all FBI intelligence analysts in training go to the Holocaust Museum in Washington, so they can see, and hear, and feel what we are capable of.

What people who are believing they are righteous, and lack constraint and oversight can do. When

people surrender their moral authority to the group. It's also the reason why every new analyst and agent at the FBI is required to take a course on this organization's interactions with Dr. Martin Luther King, Jr. It's intended to remind all of them of the dangers of becoming untethered to oversight and accountability without having checks on human nature.

As a further reminder about human nature, I think all of my employees now know this.

I have an old desk that has a glass tabletop. In the right-hand corner of it under the glass is a single piece of paper. It's from October 1963, and it's a memo from J. Edgar Hoover to Robert F. Kennedy, the Attorney General of the United States, asking for permission to bug Martin Luther King Jr. It's five sentences long, it's utterly devoid of factual content, of any consequence. There is no date limitation, there's no geographic limitation, it simply says we need to bug this guy essentially. Hoover signed it, Kennedy signed it, and they were off to the races.

This isn't about me trying to pick on Bobby Kennedy, or J. Edgar Hoover, but here's the thing. I have no doubt that they believed they were doing the right thing. I keep it there to remind me in that spot, because that's the spot where every morning I review the thick stack of applications that the FBI's going to send to federal judges to ask permission to wiretap or bug people in our national security investigations. Those things are thicker than my arm, it's a huge pain in the neck to get those orders, that's a great thing.

It sits there—that order—to remind me and everybody who hears about it, to be very, very careful about being certain that your cause is just and that your facts are right.

I'm hugely grateful to Kenyon for a bunch of reasons. You have afforded my son an incredible education. I'm grateful to all of you for fighting to find the space to have a quality conversation about privacy, and to talk about things that matter. My hope is that tonight when we start talking, and over the next two days you will engage, you will question assumptions, and biases, your own, and those of the people you're talking with.

You'll ask good questions, you'll listen with an open mind, and by that I mean a mind open to being convinced, even if you're not convinced at the end of the day. I also hope we will resist the temptation to demonize anybody in this discussion, whether that's the tech companies, or the government, or anybody else. I haven't seen any demons in this conversation. We are all people trying to do the right thing as we see the right. It is not for the FBI to decide how this country should govern itself.

It's not for the FBI to decide what the right approach is here. Our job is to investigate. Our job is to tell you, the people who pay for us, when the tools you count on us to use aren't working so much anymore, so you can figure out what to do about that. It's also not the job of the technology companies to tell us—to tell you—what to do about this. Their job is to innovate and come up with the next great thing, and they're spectacular at that, which is to be treasured. How we move forward needs to be resolved by the American people, and especially the young who know technology so well, and who care so deeply about

getting the hard things right.

Thank you for caring about it, thank you for getting involved, and I look forward to our conversation.
Thank you very much.