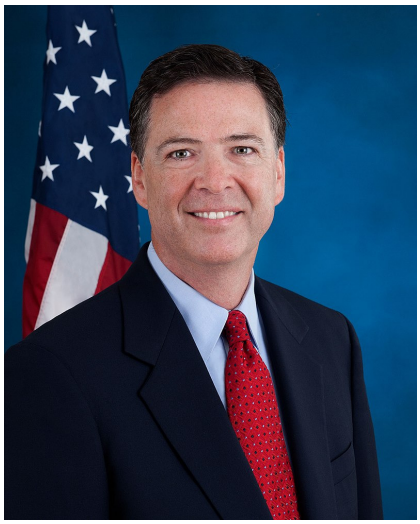
AmericanRhetoric.com

James Comey

Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?

delivered 16 October 2014, Brookings Institution, Washington, D.C.



AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio

Well, thank you, Ben, and good morning, everybody. It's great to be here at Brookings. I'm told also that I am going to be the subject of a recorded podcast for Lawfare, which is a blog I read every single day. So that's actually the real reason I'm here and so excited. What I'd like to do is share some thoughts with you, and then, for me, the most important part is going to be our conversation together. So I thank you in advance for asking *whatever* is on your mind.

I've been on this job [as FBI Director] now for one year and one month. Sometimes I joke and express my tenure in "months remaining," as if I'm incarcerated or something, but I don't mean that. I have what I believe is the best job in the entire world 'cause I get to come to work at the FBI everyday.

Over the last year, I've confirmed what I long believed -- that the FBI is a remarkable place, filled with amazing people doing amazing work all over the country and all over the world everyday. And I've also confirmed what I've long known -- that a commitment to the rule of law, and civil liberties, is at the core of the FBI. I believe it is the organization's spine.

But, as you know, we confront serious threats -- threats that are changing every single day -- and I want to make sure that I have every lawful tool available to make sure that I'm addressing those threats. And so I see this as an opportunity to begin a national conversation about something that is affecting, in a serious way, the investigative work we do.

I want to talk to you about the impact of emerging technology on law enforcement. And within that context, I think it's very important for me to talk about the work we do at the FBI, what we need to do the work that we've been entrusted to do. I believe there are a fair number of misconceptions in the public discussion about what we in government collect -- especially, we at the FBI -- and the capabilities we have for collecting information.

I think my job is, as best as I can, to try to explain, and to clarify where I can, the work of the FBI. But at the same time, I really want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need without your trust and your support. And we have no monopoly on wisdom. My goal today is not to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation as a country about where we are, where we want to be, especially with respect to law enforcement authorities.

So, let me start by talking about the challenge of what we call "Going Dark." Technology has forever changed the world we live in. All of you know this. Every single day we're online, in one way or another, all day long. Many of us are online during the night when we should be sleeping. Our phones and our computers have become reflections of our personalities. They reflect our interests and our identities. They hold much of what is important to us in life.

And with that comes a desire to protect privacy and our data. We want to be able to share our lives with the people we choose to share our lives with. I very much feel that way. But the FBI also has a sworn duty to try to keep every American safe from crime and from terrorism, and technology has become the tool of choice for some very dangerous people.

And unfortunately, the law has not kept pace with technology, and this disconnect has created a significant public safety problem we have long-described as "Going Dark." And what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism, even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to a court order, but we often lack the technical ability to do that.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, or e-mails, or live text or chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, or text messages, or photos, or videos -- what we call "data at rest." And both real-time communication (data in motion) and stored data (data at rest) are increasingly encrypted. So let me start by talking about court-ordered interception, and then talk about the challenges posed by the proliferation of different means of communication and encryption.

In the past, doing electronic surveillance was straightforward. We identified a target phone, used by a bad guy, with a single carrier. We got a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, countless networks, countless means of communicating. We have laptops. We have smartphones. We have tablets. We take them to work, to school. We take them from the soccer field to the Starbucks, over many different networks, using many different apps. And so do those conspiring to harm us. They use the same devices, the same networks, the same apps to make plans, to target victims, and to cover up what they're doing. And that makes it very tough for us to keep up.

If a suspected criminal is in the car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from a cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they're taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended -- even more unfairly -- to law enforcement that is working to obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that law enforcement -- and especially the FBI -- has these phenomenal capabilities to access any information at any time -- that we can get what we want, when we want it, by flipping a switch. That is the product of too much television. It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information in a lawful way to bring people to justice. We do that pursuant to the rule of law with clear guidance and strict oversight. But even with lawful authority, the going dark problem is we may not be able to access the evidence and the information that we need.

Current law governing the interception of communications requires that telecommunications carriers and broadband providers build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance [for] Law Enforcement Act, or CALEA, was enacted 20 years ago -- a lifetime in the Internet age. And it doesn't cover at all new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What that means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some companies can't comply because they've not developed the capabilities. Other providers want to provide assistance, but they have to take the time to build interception capabilities, which takes not just time but a lot of money.

The issue is whether companies not subject currently to CALEA should be required to build lawful intercept capabilities for law enforcement. Now, to be clear we are not seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to collect. And if the challenges of real-time data interception threaten to leave us in the dark, encryption threatens to lead us all to a very, very dark place.

Here's what I mean by that. Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse with recent default encryption settings and encrypted devices and networks -- all in the name of increased security and privacy. For example, with Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means that the companies themselves will not be able to unlock phones, laptops, and tablets to reveal photos, or documents, or e-mail, or stored texts, or recordings in those...instruments.

Look, both companies are run by good people who care deeply about public safety and national security -- I know that -- and they're responding to a market demand that they perceive. But the place that this is leading us is one that I suggest we should not go without careful thought and debate as a country.

At the outset, the good folks at Apple say something that's reasonable, which is, "Look, it's not that big a deal, because law enforcement can still get the data from 'the cloud'" -- 'cause folks are going to back up their devices to the cloud and the FBI with lawful authority can still access the cloud. But here's the problem with that. Uploading to the cloud doesn't include all of the stored data on the bad guy's phone, first, which has the potential to create a black hole in and of itself.

But second, if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it's the people most worried about what's on the device who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.

Encryption just isn't a technical feature; it's part of a marketing strategy. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened, a safe deposit box that can't be opened, a safe that can't ever be cracked. And my question to facilitate this -- this conversation is: At what cost?

Let me try to correct some misimpressions that I think are connected to this. The first is that, folks say -- good folks say, "Look, you're still going to have access to metadata, which includes telephone records and location information stored with the telecommunications carriers." And that is absolutely true. But metadata does not provide the content of any communication. It's incomplete information, and even that is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.

There is a misconception that building a lawful intercept solution is all about building a "back door," one that foreign adversaries or hackers could exploit. That also is not true. We are not seeking a back door approach. We want to use the front door, with clarity and transparency. We want clear guidance provided by law. We are completely comfortable with court orders and legal process -- front doors that provide us the evidence and information we need to investigate crime and prevent attacks.

Cyber adversaries -- there's no doubt -- are going to try to exploit any vulnerability they find. But we think it makes more sense to address any security risks by developing intercept solutions at the front end, in the design phase, rather than resorting to patchwork solutions when law enforcement comes knocking after the fact. And with this sophisticated encryption, there may be no solution at all, leaving the government at a total dead end -- again, all in the name of -- of privacy and network security.

Another misperception that I've seen is -- folks sometimes say, "But you could guess the password or break it with a (so-called) brute force attack." Here's the truth: Even with a supercomputer we would have difficulty with today's high-level encryption, and some devices have a setting where the encryption key itself is erased after too many attempts to break the password -- meaning no one, no matter how big their computer, can access the data.

And sometimes I've also heard reasonable folks ask this question: "Can't you just compel the owner of the device to provide you the password?" And the answer is, "That's a reasonable question, but unfortunately no." Even if we could compel them as a legal matter, think about the choice that that bad guy has to make. Imagine a child predator in custody choosing between a 30-day contempt sentence for refusing to comply with the direction from a court to hand over the password, or a 30-year sentence for the production and distribution of child pornography -- and that choice is not hard to predict.

So let me talk about some case examples that I hope will illustrate what I'm worried about. Think about your life without your smartphone, without Internet access, or without texting and emailing, or the apps used everyday. I'm guessing most of you would feel lost or left behind. I'm told that people much, much cooler than I -- which is nearly everyone -- calls this "Fomo" or "Fear of missing out." With going dark, those of us in law enforcement and public safety have a major fear of missing out -- missing out on predators who exploit the most vulnerable among us, on violent criminals, on terrorist cells, and a whole lot of other bad people.

The more we as a society rely on these devices, the more important they are to law enforcement and public safety officials for reasons that, I think, make sense to you. We have seen case after case -- from homicides and car crashes to drug trafficking, child abuse, child exploitation and exoneration -- where critical evidence came from smartphones, hard drives, and online communication. But let me just give you some examples of cases that involve the content of smartphones.

In Louisiana, a known sex offender posed recently as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet this supposed young girl. The predator posed as a taxi driver. He took this young boy, murdered him, and then tried to alter and delete evidence on both his and the victim's cell phones to cover up the crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. And that suspect was sentenced to death in April of this year.

In Louisiana -- excuse me, that was in Louisiana -- In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head; and there were no witnesses. Text messages stored on her parents' cell phones, between the two of them and with other family members, proved that the mother had caused the young girl's death and that the father knew what was happening and failed to stop it. The text messages stored on their devices also proved that they failed to seek medical attention for the little girl for hours after she convulsed; that they went so far as to paint her with blue paint to cover her bruises before calling 911. Confronted with the evidence from the phones, both parents pled guilty.

In Kansas City, the DEA investigated recently a drug trafficking organization tied to heroin distribution, homicides, and to robberies. And the DEA got search warrants for the smartphones used by some members of the group.

And they found stored on the phone text messages that outlined the distribution chain and tied that group to the supply of lethal heroin that had caused 12 overdoses and five deaths in high school students in that area.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them -- killing all four dogs instantly, and severing the young man's leg, and leaving the young woman in critical condition. The driver fled and that young guy died several days later. Using "red light cameras" near the scene, the California Highway Patrol identified and arrested a suspect and seized his smartphone. The GPS data stored on that phone placed the suspect at the scene of the accident and showed that he fled California right afterwards. He was convicted and is serving a 25-years-to-life term for second degree murder.

And lastly, I mentioned ways in which we've used it to prosecute. It has been used to exonerate innocent people. In Kansas, data from a cell phone was used, not long ago, to prove the innocence of several teens accused of rape. Without access to the phone, or the ability to recover a deleted video from that phone, several innocent young men could have been wrongly convicted.

These are cases, just a few examples that I pulled together, in which we had access to the evidence we needed. But we're seeing more and more where we believe significant evidence is on that phone or on that laptop, and we can't crack the password. If this becomes the norm, I suggest to you that homicide cases could be stalled, suspects walked free, child exploitation not discovered and prosecuted. Justice may be denied, because of a locked phone or an encrypted device.

So here are my personal thoughts about this. I am deeply concerned about it, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do and how we do it.

I hope you know that I am a huge believer in the rule of law. But I also believe that no one in this country should be beyond the law. There should be no "law-free zones" in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or the contents of their cell phone.

But the notion that the marketplace could create something that would prevent the closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it's time to ask: So where are we as a society? Are we no longer a country that is passionate both about the rule of law, and, about there being no zones in this country beyond the reach of that rule of law? Have we become so mistrustful of government, and law enforcement in particular, that we are willing to let bad guys walk away, willing to leave victims in search of justice? I know there will come a day where it will matter a great deal to innocent people that we in law enforcement cannot access certain types of data or information, even with court authority. We have to have discussions about this before those days come.

I believe that people should be skeptical of government power. I am. I think this country was founded by people who were, who knew you could not trust people in power. And so they divided the power among three branches, to set interest against interest. And then they wrote a Bill of Rights to ensure that the "papers and effects" of the people are secure from unreasonable searches.[1]

But the way I see it, the means by which we conduct surveillance through telecommunications carriers or Internet service providers who have developed lawful intercept solutions is an example of a government operating the way the Founders designed it -- with the Executive, the Legislative, and Judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law. I suggest that it's time that the post-Snowden pendulum be seen as having swung too far in one direction -- in a direction of fear and mistrust. I think it's time to have an open and honest debate about liberty and security.

Some have suggested that there is a conflict between liberty and security. You have to give up a little of one to get some of the other. And I reject that framework. I think when we are at our best in law enforcement, in national security and public safety we are looking to enhance security and liberty. When a city posts police officers on a dangerous playground, security has promoted liberty -- the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn't a question for us of conflict. We care deeply about protecting liberty through due process, while also safeguarding the citizens that we're here to protect.

So where do we go? These are tough issues. Finding the space and time in our busy lives to understand them is hard. (So, I'm so grateful to Ben and to Brookings for carving out some space for us.) Intelligent people can and do disagree, and that's what's awesome about a democracy. That is what is great about American life -- smart people disagreeing to come to the best answer.

I have never been -- I don't think -- anyone who is a scaremonger. But I'm in a dangerous business. So I prefer that we discuss the impact of limiting the court-authorized law enforcement tools we use, and that we talk about what are the losses associated with our inability to collect information pursuant to law. We in the FBI are going to continue to throw everything we have at this challenge. It's costly. It's inefficient. It takes time. But we are going to work to make sure that whenever we can we're able to execute court authority.

But we need to fix this problem. It's long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven. We need to find common ground. We care about the same things. I said it 'cause I meant it. The companies that we've talked about, that we've talked to are run by good people who care about the same things. We know an adversarial posture is not going to help any of us to make progress here.

We understand the private sector's need to remain competitive in the global marketplace. It is not our intent to stifle innovation or to undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while protecting privacy rights and network security. We need our private sector partners to take a step back, to pause, to consider -- I hope -- a change of course.

But we also need a regulatory and legislative fix, here -- to create a level playing field, so that all communication service providers are held to the same standard; and so that those of us in law enforcement, national security, and public safety can continue to do the job you've entrusted us to do, in the way you want us to do it.

Perhaps most importantly, we need to make sure the American public understands the work we do and the means by which we do it.

I really do believe we can get there. I really do believe that we can find a reasoned and practical approach, and that we can do it together. I do not have a perfect solution to suggest to you, but I think it's important to start the discussion. I am very happy -- in fact eager to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer -- to find the balance that we need, to find both liberty and security.

So thank you for being here today to participate in this conversation, and thank you for caring about these issues. I look forward to your questions.

---

[1] A specific reference to the 4th Amendment of the Bill of Rights which avers: "The right of the people to be secure in their persons, houses, **papers, and effects**, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (emphasis added)