James B. Comey
Director
Federal Bureau of Investigation

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

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

Remarks as delivered.

Good morning. It's an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to express my tenure in terms of months, and I joke that I have eight years and 11 months to go, as if I'm incarcerated. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed—that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the core of the FBI. It is the organization's spine.

But we confront serious threats—threats that are changing every day. So I want to make sure I have every lawful tool available to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk in a serious way about the impact of emerging technology on public safety. And within that context, I think it's important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect and the capabilities we have for collecting information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need to do without your trust and your support. We have no monopoly on wisdom.

My goal today isn't 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, and where we want to be, with respect to the authority of law enforcement.

The Challenge of Going Dark

Technology has forever changed the world we live in. We're online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data—you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.

Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "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 court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Let's talk about court-ordered interception first, and then we'll talk about challenges posed by different means of encryption.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained 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, and countless means of communicating. We have laptops, smartphones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they're doing. And that makes it tough for us to keep up.

If a suspected criminal is in his 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 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—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that 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 some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to 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 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 this 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 can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren't 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 intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

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 designed to increase security and privacy.

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 the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

At the outset, Apple says something that is reasonable—that it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud" and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And 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 is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. 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 that can't be cracked. And my question is, at what cost?

Correcting Misconceptions

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this 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 into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end—all in the name of privacy and network security.

Another misperception is that we can somehow guess the password or break into the phone with a so-called "brute force" attack. Even a supercomputer would have difficulty with today's high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the phone to produce the password?" Likely, no. And even if we could compel them as a legal matter, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt sentence for refusing to comply with a court order to produce his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or e-mail or the apps you use every day. I'm guessing most of you would feel rather lost and left behind. Kids call 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...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case—from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation—where critical evidence came from smartphones, hard drives, and online communication.

Let's just talk about cases involving the content of phones.

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

In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages stored on her parents' cell phones to one another and to their family members proved the mother caused this young girl's death and that the father knew what was happening and failed to stop it. Text messages stored on these devices also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses—and five deaths—including several high school students.

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 their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later. Using "red light cameras" near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years to life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

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

My Thoughts

I'm deeply concerned about this, 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'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone 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 someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away...willing to leave victims in search of justice?

There will come a day—and it comes every day in this business—where it will matter a great deal to innocent people that we in law enforcement can't access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of government power. I am. This country was founded by people who were worried about government power—who knew that you cannot trust people in power. So they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the "papers and effects" of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an example of government operating in the way the founders intended—that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.

Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at 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 of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve—in every investigation.

Where Do We Go from Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that's the beauty of American life—that smart people can come to the right answer.

I've never been someone who is a scaremonger. But I'm in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains and what we all stand to lose.

We in the FBI will continue to throw every lawful tool we have at this problem, but it's costly. It's inefficient. And it takes time.

We need to fix this problem. It is 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 for lawless conduct. We need to find common ground. We care about the same things. I said it because I meant it. These companies are run by good people. And we know an adversarial posture won't take any of us very far down the road.

We understand the private sector's need to remain competitive in the global marketplace. And it isn't our intent to stifle innovation or 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 still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.

We also need a regulatory or legislative fix 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 have entrusted us to do, in the way you would want us to.

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, with a reasoned and practical approach. And we have to get there together. I don't have the perfect solution. But I think it's important to start the discussion. I'm happy 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 we need.

Thank you for having me here today.