Department of Justice

STATEMENT OF

SALLY QUILLIAN YATES
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

AND

JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"GOING DARK: ENCRYPTION, TECHNOLOGY, AND THE BALANCE BETWEEN PUBLIC SAFETY AND PRIVACY"

PRESENTED

JULY 8, 2015

Statement of
Sally Quillian Yates
Deputy Attorney General
Department of Justice

and

James B. Comey
Director
Federal Bureau of Investigation

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"

Presented
July 8, 2015

Good morning, Chairman Grassley, Ranking Member Leahy, and Members of the Judiciary Committee. Thank you for the opportunity to testify today about the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as "Going Dark".

We would also like to thank this Committee more generally for its continued support for the mission of the Department of Justice. We know that you, like us, take very seriously the role of the Department in protecting the public in a manner that upholds the Constitution and the rule of law.

Introduction

In recent years, new methods of electronic communication have transformed our society, most visibly by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to

secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cybersecurity. The Department is on the frontlines of the fight against cybercrime and we know first-hand the damage that can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety.

American citizens care deeply about privacy and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance—not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private communications contain evidence of a crime, then the government can conduct a limited search for that evidence. For example, by having a neutral arbiter—the judge—evaluate whether the government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' Constitutional rights.

The Department of Justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly-authorized warrant issued by a Federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is "in motion" over electronic networks, or "at rest" on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party.

Threats

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications.

When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root

out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence.

These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from State to State and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that

phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker.

In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully-authorized access to their data, the jury would not have been able to consider that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

Legal Framework

We would like to emphasize that the "Going Dark" problem is, at base, one of technological *choices and capability*. We are not asking to expand the Government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the Department of Justice fully complies with those protections. The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?

We would like to describe briefly the law and the extensive checks, balances, and safeguards that it contains. In addition to the Constitution, two statutes are particularly relevant to the Going Dark problem. Generally speaking, in order for the Government to conduct *real-time—i.e.*, data in motion—electronic surveillance of the content of a suspect's communications, it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as "Title III" or the "Wiretap Act") or the Foreign Intelligence Surveillance Act of 1978 (or "FISA"). Title III authorizes the Government to obtain a court order to conduct surveillance of wire, oral, or electronic communications when it is investigating Federal felonies. Generally speaking, FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court (FISC), to approve surveillance directed at foreign intelligence and international terrorism threats. Regardless of which statute governs, however, the standards for the real-time electronic surveillance of United States persons' communications are demanding. For instance, if Federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a Federal district court judge must find:

- That there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;

- That alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and

- That there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

The law also requires that before an application is even brought to a court, it must be approved by a high-ranking Department of Justice official. In addition, court orders allowing wiretap authority expire after 30 days; if the Government seeks to extend surveillance beyond this period it must submit another application with a fresh showing of probable cause and

investigative necessity. And the Government is required to minimize to the extent possible its electronic interceptions to exclude non-pertinent and privileged communications. All of these requirements are approved by a Federal court.

The statutory requirements for electronic surveillance of U.S. persons under FISA are also demanding. To approve that surveillance, the FISC, must, among other things, find probable cause to believe:

- That the target of the surveillance is a foreign power or agent of a foreign power; and

- That each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

Similarly, when law enforcement investigators seek access to electronic information *stored—i.e.*, data at rest—on a device, such as a smartphone, they are likewise bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

Collectively, these statutes reflect a concerted Congressional effort, overseen by an independent judiciary, to validate the principles enshrined in our Constitution and balance several sometimes-competing, yet equally-legitimate social interests: privacy, public safety, national security, and effective justice. The evolution and operation of technology today has led to recent trends that threaten this time-honored approach. In short, the same ingenuity that has improved our lives in so many ways has also resulted in the proliferation of products and services where providers can no longer assist law enforcement in executing warrants.

Provider Assistance

Both Title III and FISA include provisions mandating technical assistance so that the Government will be able to carry out activities authorized by the court. For example, Title III

specifies that a "service provider, landlord…or other person shall furnish [the Government]…forthwith all…technical assistance necessary to accomplish the interception." As the communications environment has grown in volume and complexity, technical assistance has proven to be essential for interception to occur. These provisions alone, however, have not historically been sufficient to enable the Government to conduct electronic surveillance in a timely and effective manner.

In the early 1990s, the telecommunications industry was undergoing a major transformation and the Government faced a similar problem: determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA requires "telecommunications carriers" to develop and deploy intercept solutions in their networks to ensure that the Government is able to intercept electronic communications when lawfully authorized, although it does not require a carrier to decrypt communications encrypted by the customer unless the carrier provided the encryption and possesses the information necessary to decrypt. Specifically, it requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as "pen register information" or "dialing and signaling information"). CALEA regulates the capabilities that covered entities must have and does not affect the process or the legal standards that the Government must meet in order to obtain a court order to collect communications or related data.

While CALEA was intended to keep pace with technological changes, its focus was on telecommunications carriers that provided traditional telephony and mobile telephone services, not Internet-based communications services. Over the years, through interpretation of the statute by the Federal Communications Commission, the reach of CALEA has been expanded to include facilities-based broadband Internet access and Voice over Internet Protocol (VoIP) services that

are fully interconnected with the public switched telephone network. Although that expansion of coverage has been extremely helpful, CALEA does not cover popular Internet-based communications services such as email, Internet messaging, social networking sites, or peer-to-peer services.

At the time CALEA was enacted, Internet-based communications were in a fairly early stage of development, and digital telephony represented the greatest challenge to law enforcement. However, due to the revolutionary shift in communications technology in recent years, the Government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.

The harms resulting from the inability of companies to comply with court-ordered surveillance warrants are not abstract, and have very real consequences in different types of criminal and national security investigations.

Going Forward

Mr. Chairman, the Department of Justice believes that the challenges posed by the Going Dark problem, are grave, growing, and extremely complex. At the outset, it is important to emphasize that we believe that there is no one-size-fits-all strategy that will ensure progress. We have been asked what we should do going forward. We believe we will need to pursue multiple paths:

All involved must continue to ensure that citizens' legitimate privacy interests can be effectively secured, including through robust technology and legal protections.

We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe. The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently

implemented poses real barriers to law enforcement's ability to seek information in specific cases of possible national security threat.

We also cannot lose sight of the international implications of this issue. It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection. It is also true that other countries—particularly those without our commitment to the rule of law—are using this debate as a cynical means to create trade barriers, impose undue burdens on our companies and undermine human rights. We should be clear that any steps that we take here in the United States may impact the decisions that other nations take—both our closest democratic allies and more repressive regimes. In addition, any next steps we identify will be more effective if we are working together with our allies, and made more difficult if we are isolated.

We should also continue to invest in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the "Going Dark" problem. In limited circumstances, this investment may help mitigate the risks posed in high priority national security or criminal cases, although it will most likely be unable to provide a timely or scalable solution in terms of addressing the full spectrum of public safety needs.

We don't have any silver bullet, and the discussions within the Executive Branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with Congress, industry, academics, privacy groups and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

Conclusion

Mr. Chairman and Ranking Member Leahy, we would like to thank you and the members of this Committee again for your attention to this subject of national importance. While technology may change, our basic commitment at the Department to upholding the rule of law and our constitutional traditions does not. Our goal at the Department is to work collaboratively

and in good faith with interested stakeholders to explore approaches that protect the integrity of technology and promote strong encryption to protect privacy, while still allowing lawful access to information in order to protect public safety and national security.

We would be happy to answer any questions that you may have.