Encryption and the "Going Dark" Debate

(name redacted)
Specialist in Domestic Security

July 20, 2016

Congressional Research Service
7-....
www.crs.gov
R44481

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Changing technology presents opportunities and challenges for U.S. law enforcement. Some technological advances have arguably opened a treasure trove of information for investigators and analysts; others have presented unique hurdles. While some feel that law enforcement now has more information available to them than ever before, others contend that law enforcement is "going dark" as their investigative capabilities are outpaced by the speed of technological change. These hurdles for law enforcement include strong, end-to-end (or what law enforcement has sometimes called "warrant-proof") encryption; provider limits on data retention; bounds on companies' technological capabilities to provide specific data points to law enforcement; tools facilitating anonymity online; and a landscape of mixed wireless, cellular, and other networks through which individuals and information are constantly passing. As such, law enforcement cannot access certain information they otherwise may be authorized to obtain. Much of the current debate surrounds how strong encryption contributes to the going dark issue, and thus it is the focus of this report.

The tension between law enforcement capabilities and technological change has received congressional attention for several decades. For instance, in the 1990s the "crypto wars" pitted the government against technology companies, and this tension was highlighted by proposals to build in back doors to certain encrypted communications devices as well as to restrict the export of strong encryption code. In addition, Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414) in 1994 to help law enforcement maintain their ability to execute authorized electronic surveillance as telecommunications providers turned to digital and wireless technology.

The going dark debate originally focused on data in motion, or law enforcement's ability to intercept real-time communications. However, more recent technology changes have impacted law enforcement capabilities to access not only communications but stored content, or data at rest. As such, a central element of the debate now involves determining what types of information law enforcement is able to access and under what circumstances. Cell phones have advanced from being purely cellular telecommunications devices into mobile computers that happen to have phone capabilities; concurrently, the scope of data produced by and saved on these devices has morphed. In addition to voice communications, this range of data can include call detail records, Global Positioning System (GPS) location points, data stored on the devices (including emails and photos), and data stored in the "cloud." Some of these data can be obtained directly from telecommunications providers or individuals, and some may be obtained without going through such a middle man.

The Administration has taken steps to urge the technology community to develop a means to assist law enforcement in accessing encrypted data and has taken steps to bolster law enforcement capabilities. In addition, policymakers have been evaluating whether legislation may be a necessary or appropriate element in the current debate on going dark—particularly on the encryption aspect. A range of legislative options exist that could impact law enforcement capabilities or resources. Legislation could also place certain requirements on technology companies or individuals utilizing certain communications systems and devices. In debating these options, policymakers may consider a number of questions, including the following:

- How effective might mandating law enforcement access to products or services manufactured, sold, or otherwise used in the United States be, given the borderless nature of modern communications?

- Is it possible to create a system with sufficiently narrow and protected access points that these points can only be entered by authorized entities and not exploited by others?
- What is the appropriate balance for personal privacy and data security with public safety and national security?
- What precedents might be set for U.S. companies operating both domestically and internationally if the United States mandates the ability for law enforcement to access encrypted data and communications?

Contents

Contacts

Rapidly evolving technology presents opportunities and challenges for U.S. law enforcement. Some technological advances have arguably opened a treasure trove of information for investigators and analysts; others have presented unique hurdles. On the one hand, some argue that today's technology age has fostered a "golden age of surveillance"[1] for law enforcement. Investigators have a large body of information at their fingertips. They can use information such as location data, personal contacts, and social media websites to create digital profiles of individuals.[2] On the other hand, some posit that law enforcement is "going dark" as their investigative capabilities are outpaced by the speed of technological change. As such, law enforcement cannot access certain information they otherwise may be authorized to obtain.

Those asserting that law enforcement is going dark have cited strong encryption as one tool contributing to this issue[3]—specifically, what law enforcement has referred to as "warrant-proof" encryption.[4] Notably, while encryption is only one element of the current going dark debate, it is a central element of the conversation; as such, it is the principal focus of this report. Other factors influencing law enforcement's ability to obtain information, and thus contributing to the going dark debate, include provider limits on data retention; bounds on companies' technological capabilities to produce specific data points for law enforcement; tools facilitating anonymity online; and a landscape of mixed wireless, cellular, and other networks through which individuals and information are constantly passing.[5]

The ideas of law enforcement (1) being in a golden age of surveillance and (2) going dark may not be mutually exclusive. Rather, law enforcement may exist at the intersection of the two, and this may blur the policy debate. Policymakers have long been faced with the challenge of balancing technological change, law enforcement tools and authorities, information security, and individual privacy. This balance has come under renewed scrutiny over the past several years as technology companies have implemented automatic end-to-end encryption on certain devices and communications systems. For instance, companies such as Apple and Google who employ such strong encryption stress that they do not hold encryption keys. This means they may not be readily able to unlock, or decrypt, the devices or communications—not even for law enforcement presenting an authorized search warrant or wiretap order.[6]

One broad question is whether—and how—strong encryption and other evolving technologies might impact law enforcement investigations. Might law enforcement be able to circumvent "warrant-proof" encryption or employ other policing tactics in order to access certain communications and/or stored data? Are they losing critical information that could help prevent or solve crimes? Policymakers have been examining existing statutes, law enforcement practices, and the relationship between law enforcement and technology companies. They have been

[1] Peter Swire and Kenesa Ahmad, *"Going Dark" Versus a "Golden Age for Surveillance*," Center for Democracy and Technology, November 28, 2011.

[2] Ibid.

[3] See testimony before U.S. Congress, Senate Committee on the Judiciary, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 114th Cong., 1st sess., July 8, 2015.

[4] Warrant-proof communications are those where only the end user has access and thus may hinder a lawful court order or search warrant. See Andrea Peterson, "The Government and Privacy Advocates Can't Agree on What 'Strong' Encryption Even Means," *The Washington Post*, October 7, 2015; Herb Lin, "The Rhetoric of the Encryption Debate," *Lawfare*, October 12, 2015.

[5] See, for example, International Association of Chiefs of Police, *Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*, November 2015. See also testimony before U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives*, 114th Cong., 2nd sess., April 19, 2016.

[6] See, for instance, Apple, "Privacy: Government Information Requests."

evaluating whether legislation may be a necessary or appropriate element in the current debate on going dark—particularly on the encryption aspect. A range of legislative options exists that could impact law enforcement capabilities or resources. Legislation could also place certain requirements on technology companies or individuals utilizing certain communications systems and devices.

This report provides historical context for legislation addressing the tension between evolving technology—specifically relating to encrypted communications—and law enforcement capabilities. The report also outlines the current environment and discussion around legislation impacting law enforcement access to encrypted data and communications. It concludes with a discussion of selected issues that Congress may confront should it consider potential legislation in this arena.

History and Trajectory of Legislation on the Going Dark Debate

Technology has afforded law enforcement tools and opportunities to gather and utilize information to which it previously did not have access. Simultaneously, it has created certain barriers for law enforcement. This dichotomy has received congressional attention for several decades and remains a central point of contention between law enforcement and technology companies.

Communications Assistance for Law Enforcement Act (CALEA)

The 1990s brought "concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance."[7] Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414) to help law enforcement maintain its ability to execute authorized electronic surveillance in a changing technology environment. Among other things, CALEA requires that telecommunications carriers assist law enforcement in intercepting electronic communications for which it has a valid legal order to carry out.

There are several noteworthy caveats to the requirements under CALEA:

- Law enforcement and officials are *not* authorized to require a provider of wire or electronic communications service (as well as manufacturers of equipment and providers of support services) to implement "specific design of equipment, facilities, services, features, or system configurations."[8] Similarly, officials may *not* prohibit "the adoption of any equipment, facility, service, or feature" by these entities.[9]
- Telecommunications carriers are not responsible for "decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[10]

[7] Federal Communications Commission, *Communications Assistance for Law Enforcement Act*, January 8, 2013.

[8] 47 U.S.C. §1002(b)(1)(A).

[9] 47 U.S.C. §1002(b)(1)(B).

[10] 47 U.S.C. §1002(b)(3).

- CALEA applies to telecommunications carriers but specifically does not apply to "information services."[11]

These caveats play principal roles in the current debate. For one, officials and policymakers have been questioning whether to require additional entities to build their products and services such that law enforcement could more easily access communications and data when presenting a lawful wiretap order or warrant. They have also been debating the utility of requiring these entities to ensure that devices and communications could be unlocked and decrypted. These issues are discussed in more detail below.

A decade after the passage of CALEA, changing technology continued to concern law enforcement officials. Not all telecommunications providers had implemented CALEA-compliant intercept capabilities.[12] The FCC administratively expanded CALEA's requirements to apply to certain broadband and Voice over Internet Protocol (VoIP) providers.[13] Since this administrative expansion, there have been reports of the Administration considering various legislative proposals to further expand it.[14] However, they have not been officially introduced. One way of looking at these proposed expansions is in two broad categories:

1. Expansions that would broaden the range of communications or information service providers covered under the CALEA umbrella. Some have been interested in making CALEA more technology neutral such that it could, given the rapidly changing technology landscape, apply to a wider range of communications or information service providers.
2. Expansions that would broaden the requirements—such as maintaining the ability to decrypt communications—placed on entities covered by CALEA.

A perennial concern of these proposals is that requiring access points for third parties such as law enforcement has often been thought of as building in a form of "master key" or "back door"—a door that, while maybe useful to law enforcement officials executing authorized surveillance and searches, could also be vulnerable to exploitation by hackers, criminals, and other malicious actors. This is also a current issue for policymakers debating legislation in this area (see the section of this report on "Exceptional Access").

[11] 47 U.S.C. §1002(b)(2). According to 47 U.S.C. §1001(6), "The term 'information services' (A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and (B) includes—(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network."

[12] The Department of Justice (DOJ), FBI, and Drug Enforcement Administration (DEA) filed a Joint Petition for Expedited Rulemaking asking the Federal Communications Commission to extend CALEA provisions to a wider breadth of telecommunications providers. It was expanded to cover facilities-based broadband Internet access and interconnected Voice over Internet Protocol (VoIP) providers. Joint Petition for Expedited Rulemaking from United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration to Federal Communications Commission, March 10, 2004. "Interconnected" VoIP services are those that, among other things, use the Public Switched Telephone Network. See 47 C.F.R. §9.3.

[13] Federal Communications Commission, Second Report and Order and Memorandum Opinion and Order, ET Docket No. 04-295, May 3, 2006. For more information on CALEA and its administrative changes, see archived CRS Report RL30677, *The Communications Assistance for Law Enforcement Act*, by (name redacted) .

[14] See, for example, Charlie Savage, "U.S. Is Working To Ease Wiretaps On the Internet," *The New York Times*, September 27, 2010; Charlie Savage, "U.S. Weighs Wide Overhaul of Wiretap Laws," *The New York Times*, May 7, 2013.

Conceptualizing "Back Door" Access

Rhetoric around the encryption debate has focused on the notion of preventing or allowing "back door" or exceptional access to communications or data.[15] Many view a back door as the ability for access by any entity, including a government agency, to encrypted user data without the user's explicit authorization. From a technical standpoint, this may be seen as a security vulnerability.[16] Using this conceptualization, a number of encrypted products and services have built-in back doors. Many email service providers, for instance, encrypt email communications and also maintain a key to those communications stored on their servers. This is also the case for cloud providers that maintain keys to the data stored on their servers. This technique is how such companies are able to comply with law enforcement requests for information. Strong end-to-end encryption where companies do not maintain keys, however, does not automatically contain the same opportunities for access. This does not mean that back doors, or vulnerabilities, will not be discovered by technology companies, security researchers, government investigators, malicious actors, or others, though. There is debate as to whether there is a means to secure a back door such that it can only be accessed in lawful circumstances. Researchers have yet to demonstrate how this would be possible.[17]

Crypto Wars

Around the time that policymakers were passing CALEA, a larger discussion on encryption was taking place. The so called "crypto wars" pitted the government against data privacy advocates in a debate on the use of data encryption.[18] This tension was highlighted by proposals to build in back doors to certain encrypted communications devices as well as to block the export of strong encryption code.

Clipper Chip. During the Clinton Administration, encryption technology, known as the Clipper Chip, was introduced.[19] This technology used a concept referred to as "key escrow." The idea was that the Clipper Chip would be inserted into a communications device, and at the start of each encrypted communication session, the chip would copy the encryption key and send it to the government to be held in escrow, essentially establishing a back door for access. With authorization—such as a court authorized wiretap—government agencies would then have the ability to access the key to the encrypted communication. Vulnerabilities in the system design were later discovered, showing that the system could be breached and the escrow capabilities disabled.[20] As such, this system was not adopted.

Encryption Export. The federal government opened an investigation into Philip Zimmermann, the creator of Pretty Good Privacy (PGP) encryption software, a widely used email encryption platform.[21] When PGP was released, it "was a milestone in the development of public

[15] Herb Lin, "The Rhetoric of the Encryption Debate," *Lawfare*, October 12, 2015.

[16] See, for instance, Center for Democracy and Technology, *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, March 3, 2016.

[17] Ibid. See also Harold Abelson, Ross Anderson, and Steven M. Bellovin, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Massachusetts Institute of Technology, July 6, 2015.

[18] See http://fortune.com/2014/09/27/apple-and-the-fbi-re-enact-the-90s-crypto-wars/; http://archive.wired.com/wired/archive/5.05/cyber_rights_pr.html. The term "crypto wars" has been used by the Electronic Frontier Foundation to describe this debate.

[19] For more information on the Clipper Chip, see Matt Blaze, *Key Escrow from a Safe Distance*, 2011. See also Sean Gallagher, "What the Government Should've Learned About Backdoors From the Clipper Chip," *ArsTechnica*, December 14, 2015, and Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 12, 1994.

[20] Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, AT&T Bell Laboratories, August 20, 1994.

[21] Robert J. Stay, "Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann," *Georgia State University Law Review*, vol. 13, no. 2 (1996), Article 14. See also John Markoff, (continued...)

cryptography. For the first time, military-grade cryptography was available to the public, a level of security so high that even the ultra-secret code-breaking computers at the National Security Agency could not decipher the encrypted messages."[22] PGP proliferated when someone released a copy of it on the Internet, sparking a federal investigation into whether Zimmerman was illegally exporting cryptographic software (then considered a form of "munitions" under the U.S. export regulations) without a specific munitions export license. Ultimately the case was resolved without an indictment. Courts have since been presented with the question of how far the First Amendment right to free speech protects written software code—which includes encryption code.[23]

Renewed Crypto Wars?

There were several decades of discussions around amending CALEA, though no legislation moved. In addition, aside from several hearings,[24] the broader notion of law enforcement "going dark" had been a relatively dormant legislative issue. Interest, however, was reinvigorated in 2014 as technology companies like Apple and Google began implementing automatic end-to-end encryption on mobile devices and certain communications systems.[25] These moves reopened the public discussion on how encryption and quickly advancing technologies could impact law enforcement investigations.[26]

The going dark debate originally focused on data in motion, or law enforcement's ability to intercept real-time communications. However, as communications technologies have evolved, so has the rhetoric on going dark. More recent technology changes have potentially impacted law enforcement capabilities to access not only communications but stored content, or data at rest. A central element of the debate now involves determining what types of information law enforcement is able to access and under what circumstances.

What Can Law Enforcement Obtain Now?

As cell phone—and now smartphone—technology has evolved, so too has law enforcement use of the data generated by and stored on these devices. Cell phones have advanced from being purely cellular telecommunications devices into mobile computers that happen to have phone capabilities; concurrently, the scope of data produced by and saved on these devices has morphed.

(...continued)

"Federal Inquiry on Software Examines Privacy Programs," *The New York Times*, February 21, 1993.

[22] Robert J. Stay, "Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann," *Georgia State University Law Review*, vol. 13, no. 2 (1996), Article 14, pp. 584-585.

[23] Bernstein v. U.S. Department of Justice; https://www.eff.org/deeplinks/2010/09/government-seeks.

[24] See, for example, U.S. Congress, House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, 112th Cong., 1st sess., February 17, 2011. The issue was also brought up during some FBI oversight hearings.

[25] For example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, *Addressing Remaining Gaps in Federal, State, and Local Information Sharing*, 114th Cong., 1st sess., February 26, 2015; U.S. Congress, Senate Select Committee on Intelligence, *Counterterrorism, Counterintelligence, and the Challenges of "Going Dark"*, 114th Cong., 1st sess., July 8, 2015; U.S. Congress, Senate Committee on the Judiciary, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 114th Cong., 1st sess., July 8, 2015; and U.S. Congress, Senate Committee on the Judiciary, *Oversight of the Federal Bureau of Investigation*, 114th Cong., 1st sess., December 9, 2015.

[26] See, for example, Pamela Brown and Evan Perez, "FBI Tells Apple, Google Their Privacy Efforts Could Hamstring Investigations," *CNN*, October 12, 2014.

In addition to voice communications, this list can include call detail records, Global Positioning System (GPS) location points, data stored on mobile devices (including emails and photos), and data stored in the "cloud." Some of these data can be obtained directly from telecommunications providers or individuals, and some may be obtained without going through such a middle man.

Communications Content

Law enforcement can attempt to access voice communications by obtaining a court authorized wiretap order.[27] Wiretap requests are submitted by law enforcement to judges, requesting permission to intercept certain wire, oral, or electronic communications. Intercept orders given by judges authorize/approve wiretap requests, which allow law enforcement to proceed.[28] In 2015, judges authorized 4,148 wiretaps, of which about 34% (1,403 orders) were under federal jurisdiction.[29]

As technology has evolved, some companies have implemented automatic end-to-end encryption on certain communications. It has been employed on some messaging systems and telephone calls. For instance, Apple has this type of encryption on its iMessage systems and on FaceTime calls.[30] The real-time content of these messages and calls reportedly cannot be accessed while in transit between devices (though users may elect to store iMessage content in the cloud). Apple notes the result of this is that the company cannot comply with wiretap orders for iMessage and FaceTime communications.[31] In addition, WhatsApp—an online messaging service facilitating text and phone communications—has implemented default "end-to-end encryption to every form of communication on its service."[32] This applies to phone calls, messages, photos, videos, and files shared, and it impacts communications on about 1 billion devices. Law enforcement has reported instances of having trouble accessing certain real-time communications (including at least one communication transmitted through WhatsApp).[33]

The Administrative Office of the U.S. Courts collects data on whether law enforcement encountered encryption in the course of carrying out wiretaps and whether officials were able to overcome the encryption and decipher the "plain text" of the encrypted information. Of the total 4,148 wiretap orders in 2015, there were 13 reported instances in which encrypted communications were encountered, and 11 of these 13 instances involved encryption foiling law enforcement officials.[34] Notably, these data do not capture instances in which law enforcement

---

[27] For more information on legal authorities surrounding wiretapping in criminal cases, see CRS Report 98-327, *Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by (name redacted) and (name redacted), and CRS Report R41734, *Privacy: An Abridged Overview of the Electronic Communications Privacy Act*, by (name redacted)

[28] These activities are authorized under 18 U.S.C. §2510-2522.

[29] Administrative Office of the U.S. Courts, *Wiretap Report 2015*. The federal statute authorizing wire, oral, or electronic communications interception is 18 U.S.C. §2510-2522. These data do not include those interceptions of wire, oral, or electronic communications that are regulated by the Foreign Intelligence Surveillance Act of 1978. These are the most recent data available.

[30] Apple, *Privacy: Our Approach to Privacy*.

[31] Ibid.

[32] Cade Metz, "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People," *Wired.com*, April 5, 2016. For more information, see "End-To-End Encryption," *WhatsApp Blog*, April 5, 2016.

[33] Ibid.

[34] Administrative Office of the U.S. Courts, *Wiretap Report 2015*. For more information on these data and how they compare to prior years, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by (name redacted)

officials know they will encounter "warrant-proof" encryption, and thus they elect not to attempt intercepting and breaking the encryption on the communication.

- Federal Bureau of Investigation (FBI) Director Comey has used one particular case as evidence of active law enforcement investigations being stymied by encryption. In May 2015, two Islamic State-inspired gunmen opened fire outside an event featuring cartoons of Mohammed in Garland, TX. Director Comey has noted that one gunman had "exchanged 109 messages with an overseas terrorist" the morning that the shooting occurred and that law enforcement has "no idea what he said because those messages were encrypted."[35] However, despite not being able to retrieve the exact content of these communications, encryption did not prevent law enforcement from accessing metadata connected to the attack (e.g., who the gunmen were communicating with, when, and how frequently) and learning that one of the gunmen was communicating with a known terrorist and was interested in the Garland event. The morning of the shooting, the FBI sent a bulletin to the Garland Police Department indicating that one of the gunmen may show up at the event.[36]
- The November and December 2015 terrorist attacks in Paris, France, and San Bernardino, CA, sustained the going dark debate. Questions arose as to whether the attackers used encryption and, more importantly, whether this encryption had prevented law enforcement and intelligence officials from concentrating on the attackers and potentially thwarting the attacks. While some have highlighted the possibility that encrypted communications in these attacks might have shielded certain communications from law enforcement, others have denied that there is any direct evidence that encryption hindered law enforcement efforts leading up to the incidents.[37]

Call Detail Records

Law enforcement may request, with a subpoena or valid court order, certain call detail records from telecommunications providers. These records can include information such as the sending and receiving telephone numbers, whether or not the call was completed, call duration, and which cell towers were used in making or receiving the call[38] (of note, call detail records do not contain the content of telephone calls). Law enforcement can obtain these records retrospectively. Notably, companies vary in the length of time they maintain call detail records.[39] They also vary in the length of time they hold on to other types of data such as GPS location information.[40]

[35] FBI Director Comey before U.S. Congress, Senate Committee on the Judiciary, *Oversight of the Federal Bureau of Investigation*, 114th Cong., 1st sess., December 9, 2015.

[36] Scott Shane, "F.B.I. Says It Sent Warning on One Gunman in Attack at Texas Gathering," *The New York Times*, May 7, 2015.

[37] Kim Zetter, "After the Paris Attacks, Here's What the CIA Director Gets Wrong About Encryption," *Wired.com*, November 16, 2015; Seung Lee, "Did the San Bernardino Shooters Use Advanced Encryption or Not?," *Newsweek*, December 21, 2015.

[38] Matt Blaze, "How Law Enforcement Tracks Cellular Phones," *Crypto.com*, December 13, 2013.

[39] See, for example, Steven Nelson, "Here's How Long Cellphone Companies Store Your Call Records," *U.S. News & World Report*, May 22, 2015.

[40] See, for example, ibid.

With a valid court order, call detail information may also be available in real time. Through a "pen register" and "trap and trace," as they are called, law enforcement can obtain information about outgoing and incoming calls, respectively.[41] The same information that is available in a retrospective call detail record request can be obtained directly at the time of a call; similarly, a pen register or trap and trace cannot provide call content information.

- One of the tools that law enforcement has used to determine the locations of particular cell phones is a cell site simulator, commonly referred to by one of the brand names, "stingray." They are mobile devices that emit a strong signal (stronger than nearby cell towers) and thus attract mobile devices to connect to the stingray rather than a cell tower.[42] These "controversial devices are also capable of recording numbers for a mobile phone's incoming and outgoing calls, as well as intercepting the content of voice and text communications."[43] DOJ guidance instructs investigators to obtain a pen register and trap and trace order before employing this technology.[44]

Stored Data

In addition to call detail records, location information, and real time communications, law enforcement may also be interested in data stored in the cloud or on electronic devices. They may attempt to obtain this information with a warrant or subpoena.[45]

In a cloud-based system of storing data, individuals using the cloud "can use that storage capacity on demand, from anywhere in the world, as they wish, without the intervention of the service provider."[46] Ease of law enforcement access to cloud-based data may depend on a number of factors. These include the location of the cloud server and the service provider, as well as the length of time information has been stored in the cloud.[47] If the server is located overseas, for instance, law enforcement can employ the Mutual Legal Assistance process to try to obtain the data from a partner nation.[48] It is not clear whether federal law enforcement can require U.S.-based companies to turn over data stored on their servers that happen to be located abroad.

- An ongoing case between the United States and Microsoft Corporation highlights this issue. In December 2013, federal prosecutors produced a warrant requesting Microsoft to turn over emails associated with a specified account. These emails were stored on a Microsoft server located in Dublin, Ireland. Microsoft denied the request, arguing that the warrant did not apply to servers located outside the

[41] Matt Blaze, "How Law Enforcement Tracks Cellular Phones," *Crypto.com*, December 13, 2013.

[42] Kim Zetter, "Turns Out Police Stingray Spy Tools Can Indeed Record Calls," *Wired.com*, October 28, 2015.

[43] Ibid.

[44] American Civil Liberties Union of Northern California, *ACLU v. DOJ (StingRays)*, January 13, 2016.

[45] For legal distinctions on when law enforcement needs a warrant or a subpoena for this information, see CRS Report R43015, *Cloud Computing: Constitutional and Statutory Privacy Protections*, by (name redacted) .

[46] The Chertoff Group, *Law Enforcement Access to Evidence in the Cloud Era*, May 2015, p. 3.

[47] The Stored Communications Act (SCA; Title II of P.L. 99-508) details whether law enforcement needs a warrant or a subpoena to access stored data, based on how long it has been stored. For more information, see CRS Report R44036, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*, by (name redacted) and (name redacted).

[48] Mutual Legal Assistance Treaties "allow generally for the exchange of evidence and information in criminal and related matters." U.S. Department of State, *2016 International Narcotics Control Strategy Report*. See also Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Global Network Initiative, January 2015.

United States. However, the U.S. Court rejected this argument and ordered Microsoft to comply. Microsoft appealed the case to the District Court for the Southern District of New York, which ruled in favor of the United States. Microsoft has since appealed the case to the Second Circuit, which has not yet ruled.[49]

Just as there are potential limits to the breadth of data/information/evidence located in any environment, there are factors that may limit the scope of data stored in the cloud (and subsequently available to law enforcement).[50] For instance, not all individuals store data in or back up their devices to the cloud. In addition, the full range of the data on a device may not be backed up to the cloud because of features including device backup schedules and cloud storage space available to a given user.[51]

On electronic devices, data may be stored in various formats, and law enforcement may present warrants to search these devices. The content on or access to the devices themselves, however, may be locked and encrypted. This has reportedly slowed and/or obstructed law enforcement access.

- In the aftermath of the December 2, 2015, San Bernardino, CA, terrorist attack, investigators recovered an Apple iPhone belonging to one of the shooters. Law enforcement hoped that the device would contain valuable information on who the shooters may have been communicating with to plan the attacks, where the shooters may have traveled prior to the attack, and the potential involvement of others in the attack.[52] However, FBI Director Comey testified before Congress two months later and indicated that the FBI was unable to access information on the device. Through the courts, the FBI requested that Apple assist investigators in accessing these data.[53] Apple refused to comply. After a back and forth legal battle, the FBI ultimately found assistance from a third party entity, was able to access the contents of the phone, and dropped the case with Apple.[54]
- In April 2015, Brittany Mills was killed in her home in Baton Rouge, LA. Police have been unable to access the contents of her iPhone. While they were able to obtain call detail records and data stored in the cloud, her phone was last backed up to the cloud two months prior to her death, and thus the cloud is missing two months of data. Further, while police have no idea what might be stored on the phone, they believe it could have valuable information relating to Ms. Mills's death.[55]

[49] CRS Legal Sidebar WSLG1184, *Email Privacy: District Court Rules that ECPA Warrants Apply to Electronic Communications Stored Overseas*, by (name redacted); Alex Ely, "Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview," Lawfare, September 10, 2015.

[50] See testimony of Cyrus R. Vance, Jr. before the U.S. Congress, Senate Committee on the Judiciary, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 114th Cong., 2nd sess., July 8, 2015.

[51] Ibid.

[52] *See In re* Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451, at 1-2 (C.D. Cal. February 16, 2016).

[53] Ibid.

[54] For more information about this case and related legal and policy debates, see CRS Report R44396, *Court-Ordered Access to Smart Phones: In Brief*, by (name redacted), (name redacted), and (name redacted) ; and CRS Report R44407, *Encryption: Selected Legal Issues*, by (name redacted) and (name redacted) .

[55] Cat Zakrzewski, "Encrypted Smartphones Challenge Investigators," *The Wall Street Journal*, October 12, 2015; Aarti Shahani, "Mom Asks: Who Will Unlock Murdered Daughter's iPhone?," *NPR All Tech Considered*, March 30, (continued...)

There are a number of similar cases pitting law enforcement against technology companies such as Apple.[56] These cases highlight a central policy question. This question is not whether technology companies like Apple *can* assist law enforcement in gaining access to certain mobile devices, but whether these companies *should*. Policymakers may consider this in debating whether to take up legislation on the going dark issue. Depending on the answer, they may opt to respond to the question through legislation or have it play out in the courts.

Evolving Administration Positions

In addition to Members of Congress, the Obama Administration has also been debating whether to push for legislation addressing the going dark question. In particular, discussions have been around whether to require technology companies to build back door access points into encryption. At an October 1, 2015, Cabinet meeting, the Administration reportedly decided against pursuing such legislation.[57] This decision followed the National Security Council reportedly drafting a paper outlining strategic options for confronting issues arising from encryption on communications devices.[58] The three options offered in this paper, while differing in strength and timeline, all have the same immediate implication: *the Administration will not push a legislative framework requiring technology companies to make changes to their encryption systems*. The options include "explicitly rejecting a legislative mandate, deferring legislation and remaining undecided while discussions continue."[59]

These options are not entirely dissimilar from other official recommendations the Administration has received on the encryption issue. Previously, the President's Review Group on Intelligence and Communications Technologies released a report and recommendations on protecting national security as well as privacy and innovation.[60] With respect to global communications technology, and more specifically encryption technology, the Review Group concluded that

> The US Government should take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.[61]

Essentially, the Review Group concluded that the Administration should avoid repeating the crypto wars of the 1990s.

(...continued)

2016.

[56] See Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 15-MC-1902 (E.D.N.Y. February 29, 2016).

[57] Ellen Nakashima and Andrea Peterson, "Obama Administration Opts Not to Force Firms to Decrypt Data—For Now," *The Washington Post*, October 8, 2015.

[58] This draft paper was released by *The Washington Post*. Ellen Nakashima and Andrea Peterson, "Obama Faces Growing Momentum to Support Widespread Encryption," *The Washington Post*, September 16, 2015.

[59] Ellen Nakashima and Andrea Peterson, "Obama Faces Growing Momentum to Support Widespread Encryption," *The Washington Post*, September 16, 2015.

[60] *Liberty and Security in a Changing World*, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, December 12, 2013.

[61] Ibid., p. 22.

Administration Actions

Law enforcement and intelligence officials have posited that the threat of going dark is a current national security issue.[62] Rather than pushing for legislation that would address these concerns from the technology end, through diluting encryption, the Administration has taken steps to urge the technology community to develop a workaround solution and has taken steps to bolster law enforcement capabilities.

In the realm of expanded cooperation between law enforcement and technology sectors, for instance, President Obama and a number of top Administration officials met in January 2016 with the leadership from prominent technology companies to discuss means to counter radicalization and terror threats online; encryption was reportedly an agenda item.[63] In addition to discussions with the technology community, the Administration has employed the legal system to try to mandate that technology companies such as Apple assist law enforcement in accessing encrypted information that they have been authorized to obtain.[64]

In the realm of bolstering law enforcement capability, the Administration has requested an additional $38.3 million for FY2017 for the FBI's going dark program to enhance the bureau's "tools for electronic device analysis, cryptanalytic capability, and forensic tools."[65] It is unclear whether this funding would go to augmenting in-house tools, supporting external entities that could provide the FBI with needed technology support, or some combination of the two. Additionally, some experts have suggested that the government should continue to support strengthening encryption and simultaneously give law enforcement resources to bolster their capabilities to conduct investigations in an environment of strong encryption.[66] This could involve increasing both the number of agents with technology expertise and the depth of their knowledge. It could also include supporting partnerships—such as those with hackers or security researchers—such that law enforcement could source needed tools. For instance, the FBI paid hackers to find a software flaw that the bureau was then able to leverage to ultimately crack into the iPhone in the San Bernardino case.[67] Policymakers may question whether and how meeting the Administration's request would assist law enforcement in developing the tools they could use to investigate cases more effectively given the speed of technology change.

Developing Law Enforcement Tools to Obtain Data

Law enforcement has been utilizing existing technology in addition to developing new tools and paths to obtaining information they have been authorized to try to access. In the current landscape with strong encryption, law enforcement has been exploring tools to discover and exploit vulnerabilities in technology so they can try to uncover information that might otherwise be inaccessible.

---

[62] See testimony before U.S. Congress, Senate Select Committee on Intelligence, *Global Threats*, 114th Cong., 2nd sess., February 9, 2016.

[63] Ellen Nakashima, "Obama's Top National Security Officials to Meet with Silicon Valley CEOs," *The Washington Post*, January 7, 2016.

[64] See, for instance, Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451 (C.D. Cal. February 16, 2016).

[65] U.S. Department of Justice, *U.S. Department of Justice, FY2017 Budget Request, National Security*, p. 6.

[66] See, for example, testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016.

[67] Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *The Washington Post*, April 12, 2016.

For example, individuals may use a number of available tools to obscure their physical location and anonymize their activity—both legal and illegal—online. This can make it more difficult for law enforcement to attribute certain malicious activity to specific actors. Tor (short for The Onion Router) is one such software tool that anonymizes activity by bouncing encrypted information between multiple computers, or "relays," before that information reaches its destination.[68] Law enforcement has been developing exploits to bypass anonymity protections of software such as Tor.[69]

- The FBI has been developing Network Investigative Techniques (NITs), or exploits, to identify and locate individuals operating on the Dark Web. It reportedly seized the server hosting a large child pornography forum on the Dark Web in early 2015. It then ran the site from its own servers and used an NIT to identify individuals frequenting certain portions of the site.[70]
- In 2013, the FBI reportedly took control of Freedom Hosting—a website hosting service operating on the Tor network and reportedly home to more than 40 child pornography websites—and infected it with "custom malware designed to identify visitors."[71] Since 2002, the FBI has supposedly been using some form of a "computer and internet protocol address verifier"—consistent with the malware in the Freedom Hosting takeover—to "identify suspects who are disguising their location using proxy servers or anonymity services, like Tor."[72]

Going Dark Legislation Issues for Consideration

While the Administration and many policymakers have held off on pushing specific legislation on the current going dark debate (particularly with respect to encryption), the issue has made its way to the courts. The courts have addressed it in several cases involving a dispute between federal law enforcement and technology companies (namely Apple).[73] Policymakers may choose to let this debate play out in court, or they may elect to take legislative action on the issue.

Legislative options could take a number of forms. These include mandating that technology companies build in a "back door" or some other form of access point to their products[74] (or prohibiting such a mandate),[75] establishing criminal penalties for individuals who refuse to

[68] For more information on how Tor works, see https://www.torproject.org/. For more information on anonymizing activity on various layers of the Internet, and resulting issues for law enforcement, see CRS Report R44101, *Dark Web*, by (name redacted)

[69] See, for example, Joseph Cox and Sarah Jeong, "FBI Is Pushing Back Against Judge's Order to Reveal Tor Browser Exploit," *Motherboard*, March 29, 2016.

[70] Ibid. See also Catalin Cimpanu, "Is the FBI Hiding a Firefox Zero-Day?," *Softpedia*, April 15, 2016.

[71] Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired.com*, September 13, 2013.

[72] Ibid.

[73] See the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451 (C.D. Cal. February 16, 2016); and Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 15-MC-1902 (E.D.N.Y. February 29, 2016). For more information on these and other cases, see CRS Report R44407, *Encryption: Selected Legal Issues*, by (name redacted) and (name redacted) .

[74] See the draft legislation by Senators Burr and Feinstein that would require that companies comply with court orders to help law enforcement access, in intelligible formats, encrypted information from certain devices. Senator Dianne Feinstein, "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill," press release, April 13, 2016.

[75] See, for example the ENCRYPT Act of 2016 (H.R. 4528) and the Protect Our Devices Act of 2016 (H.R. 4839).

provide their passcode to law enforcement, and supporting law enforcement efforts to create new surveillance capabilities that can keep pace with developing technology. Whether or not Congress elects to take action on the going dark debate, there are a number of implications for consideration.[76]

Legislation Applicability

As policymakers consider legislative options to amend CALEA or otherwise impact law enforcement access to communications and devices protected by strong encryption, such legislation would generally apply to entities and products operating, sold, or used in the United States. As some have noted, the legislation "could not bind device-makers and software engineers overseas."[77] Therefore, one question is whether legislation would be effective if it can only impose requirements on products imported, manufactured, or sold in the United States.

As experts have noted, "crypto has no borders."[78] The issue has been highlighted with the recent introduction of state-level proposals to ban the sale of smartphones and devices with strong encryption lacking a back door that can be unlocked.[79] California and New York, for instance, have introduced such proposals.[80] If some states were to adopt laws prohibiting certain strong encryption platforms, companies such as Apple and Google would be faced with options including ceasing to sell fully encrypted products in jurisdictions with prohibitions, creating separate products with varying levels of encryption based on the jurisdiction in which they are sold, or ceasing to create and sell products without back doors into the encrypted systems.[81] A similar scenario would arguably be at play if national legislation with encryption limitations were to be adopted. How might this impact companies operating internationally? Would they need to stop selling certain products in certain countries, develop country-specific products to comply with the relevant encryption-related laws, or produce only products with back doors for government access? None of the resulting options for technology companies, however, would necessarily stop individuals from crossing jurisdictional boundaries and obtaining products and services with the desired privacy capabilities.

Because crypto has no borders, this challenges crypto-related legislation that does not span jurisdictional boundaries. Individuals could readily obtain products from other jurisdictions, they could download applications with the desired capabilities, and they could modify software after purchase.

Exceptional Access

In considering future legislation on or regulation of encrypted systems and communications, the issue of exceptional access has been raised: is it possible to create a system with sufficiently

[76] There are a number of implications that are outside the law enforcement scope of this report. For instance, some have questioned whether there could be economic implications of requiring companies to construct products or software that could allow law enforcement access to smart phones and mobile devices. See, for example, Klint Finley, "Apple's Noble Stand Against the FBI Is Also Great Business," *Wired.com*, February 17, 2016.

[77] Ellen Nakashima and Barton Gellman, "As Encryption Spreads, U.S. Grapples With Clash Between Privacy, Security," *The Washington Post*, April 10, 2015.

[78] Andy Greenberg, "Proposed State Bans on Encryption Make Zero Sense," *Wired.com*, January 27, 2016.

[79] Ibid.

[80] Of note, legislation has been introduced in the House (H.R. 4528) intended "[t]o preempt State data security vulnerability mandates and decryption requirements."

[81] Andy Greenberg, "Proposed State Bans on Encryption Make Zero Sense," *Wired.com*, January 27, 2016.

narrow and protected access points that these points can only be entered by authorized entities and not exploited by others? Experts have generally responded, no. For instance, one group of computer scientists and security experts contends that requiring exceptional access "will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend."[82] As was the case during the crypto wars of the 1990s, new technology (the Clipper Chip) was introduced that was intended to only allow access to certain communications under specified conditions. Researchers were soon able to expose vulnerabilities in the proposed system, thus halting the implementation of the Clipper Chip.

One current concern is that if new technology were introduced to provide exceptional access to officials, malicious actors may find a way to obtain and exploit this technology more quickly than companies could detect and secure vulnerabilities. These malicious actors could range from criminals looking to profit from the sale of intellectual property to business competitors or nation states seeking proprietary information. In addition, the insider threat has been cited as the largest cybersecurity issue—an employee with access and knowledge of the company could potentially do greater harm than someone from the outside. For example, Apple employees and others with access to software Apple may create to reduce the security of the iPhone could leverage their position and knowledge for malicious purposes.[83]

This is the tradeoff. Policymakers may debate which is more advantageous for the nation on the whole: increased security coupled with potentially fewer data breaches and possibly greater impediments to law enforcement investigations, or increased access to data paired with potentially greater vulnerability to malicious actors.

Pitting Privacy Against Security

Much of the ongoing discussion has pitted the notions of encryption and personal privacy against security, and this is largely the debate reinvigorated after the terrorist attacks in Paris and San Bernardino. In this dichotomy, security is framed as that provided by intelligence and law enforcement if able to access encrypted communications. This security, however, does not have a clearly defined metric. This is in part because there have not been publicly available data establishing the number of cases in which law enforcement access to encrypted communications and content has led to the prevention of a crime or to its solution.

Some have posited that the debate should not necessarily be framed as privacy versus security, but rather security versus security.[84] As some have noted, "[s]ecurity *enables* security, offline or online. That's why we close and lock the doors and windows in our homes."[85] In addition, security enables privacy, both offline and online. Locking doors and windows helps maintain both

[82] Harold Abelson, Ross Anderson, and Steven M. Bellovin, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Massachusetts Institute of Technology, July 6, 2015, pp. 24-25.

[83] Scott Stewart, *When Cyber Security Is an Inside Threat*, Stratfor Security Weekly, February 18, 2016.

[84] Alexander Howard, "After Paris, What We're Getting Wrong In 'Privacy vs. Security' Debate," *The Huffington Post*, November 16, 2015; Michael McCaul and Mark Warner, "How to Unite Privacy and Security—Before the Next Terrorist Attack," *The Washington Post*, December 27, 2015. Testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016.

[85] Alexander Howard, "After Paris, What We're Getting Wrong In 'Privacy vs. Security' Debate," *The Huffington Post*, November 16, 2015.

the security and privacy of one's home; encrypting devices and communications helps maintain the security and privacy of data.[86]

Government officials from law enforcement and intelligence have themselves supported strong encryption. Because of this, some have suggested that rather than pushing for loosened encryption standards, the government should encourage strong encryption and simultaneously support law enforcement efforts to bolster their technological capabilities to gain access to encrypted devices and communications.[87]

Setting Precedents and Examples

As noted, disputes between law enforcement and technology companies have made their way to the courts. Whether policymakers choose to take legislative action on the issues or let them be settled by the courts, the outcome could set a precedent for future law enforcement investigations and standards for other countries.

Take the recent dispute between Apple, Inc. and the FBI, for example.[88] If Apple is ultimately required to develop an operating system to assist law enforcement in accessing encrypted data on locked devices in certain investigations (terrorism cases or drug trafficking cases, for instance), what precedent does this set for Apple and other companies' compliance with other law enforcement investigations? The FBI has indicated that encryption is not only an issue in terrorism investigations, but in cases against kidnappers, murderers, drug traffickers, and others.[89] Would Apple, Google, and others need to help the FBI develop operating systems to circumvent security features in every case where the FBI or another law enforcement entity requests assistance? Indeed, some law enforcement officials have noted they would rely upon Apple to assist law enforcement in other cases.[90] Further, would companies such as Apple need to assist foreign law enforcement entities with similar requests? These are the kind of questions that Congress may choose to address through legislation or allow to be decided by the courts.

Policymakers may also question the example that the United States seeks to set for other countries, particularly authoritarian regimes, regarding access to individuals' communications and data.[91] In support of maintaining strong encryption, one expert noted that "United States support for human rights is a cornerstone of U.S. foreign policy. It includes strong support for private and secure communications, for such capabilities are a necessity for human rights workers in repressive nations."[92] Similar conversations have been held around other tools facilitating secure communications, such as anonymizing browsers like Tor.[93] Individuals may rely upon such secure

[86] Ibid. Alexander Howard and Lorenzo Ligato, "Former DHS Director Chertoff: 'You Can't Have Privacy Without Security'," *The Huffington Post*, October 3, 2015.

[87] See, for example, testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016.

[88] For more information on this debate in the context of the San Bernardino case, see CRS Report R44396, *Court-Ordered Access to Smart Phones: In Brief*, by (name redacted), (name redacted), and (name redacted)

[89] U.S. Congress, Senate Committee on the Judiciary, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 114th Cong., 1st sess., July 8, 2015.

[90] See, for example, Katie Benner and Matt Apuzzo, "Narrow Focus May Aid F.B.I. in Apple Case," *The New York Times*, February 22, 2016.

[91] Spencer Ackerman, "Apple Encryption Case Risks Influencing Russia and China, Privacy Experts Say," *The Guardian*, February 17, 2016.

[92] Testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016.

[93] More information on Tor is available at https://www.torproject.org/. Tor is the most widely used anonymous (continued...)

communications to access content that might be blocked in certain parts of the world or to express political dissent in areas where such communication could threaten individual safety.[94] If restrictions are placed on encrypted data and communications in the United States, what message might that send to other nations where human rights have been viewed by some as a concern?

Congressional Commissions and Working Groups on Going Dark

It appears as though officials are still deciding how best to simultaneously protect the privacy of encrypted communications and support legitimate law enforcement access. As such, the discussion will likely continue both in the courts and on the policy stage. Legislators, for instance, have proposed a national commission to study today's security and technology challenges. Representative Michael McCaul and Senator Mark Warner have introduced legislation that would establish a "National Commission on Security and Technology Challenges."[95] This commission would "bring together leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economics, and the national security community to examine the intersection of security and digital security and communications technology in a systematic, holistic way, and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace."[96] It would be required to submit to relevant congressional committees a report (at 6 months and 12 months after the commission's establishment) assessing several issues, including various security interests in the digital world, the economic and commercial value of cryptography and digital security and communications technology, the role of cryptography and digital security and communications technology in national security and crime prevention and their effects on law enforcement investigations, and potential costs of weakening cryptography and digital security and communications technology standards. The commission would also be required to provide policy recommendations and legislative options for consideration.

Members of the House Judiciary and Energy and Commerce Committees have established an Encryption Working Group, which "will identify potential solutions that preserve the benefits of strong encryption—including the protection of Americans' privacy and information security—while also ensuring law enforcement has the tools needed to keep us safe and prevent crime."[97] The working group's goal is to complete its evaluation and present findings and recommendations to the House by the end of the 114th Congress.[98]

(...continued)

network. See also CRS Report R44101, *Dark Web*, by (name redacted)

[94] Tor Project, *Tor: Overview*, https://www.torproject.org/about/overview.html.en.

[95] Digital Security Commission Act of 2016 (S. 2604/H.R. 4651).

[96] Ibid.

[97] House Judiciary Committee, "Goodlatte, Conyers, Upton, and Pallone Announce Bipartisan Encryption Working Group," press release, March 21, 2016.

[98] House Judiciary Committee and House Energy and Commerce Committee, Encryption Working Group, "Bipartisan Encryption Working Group Releases Roadmap," press release, April 21, 2016.

Author Contact Information

(name redacted)
Specialist in Domestic Security
[redacted]@crs.loc.gov, 7-....