Congressional Research Service
Informing the legislative debate since 1914

Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations

Kristin Finklea
Specialist in Domestic Security

February 18, 2016

Congressional Research Service
7-5700
www.crs.gov
R44187

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Because modern-day criminals are constantly developing new tools and techniques to facilitate their illicit activities, law enforcement is challenged with leveraging its tools and authorities to keep pace. For instance, interconnectivity and technological innovation have not only fostered international business and communication, they have also helped criminals carry out their operations. At times, these same technological advances have presented unique hurdles for law enforcement and officials charged with combating malicious actors.

Technology as a barrier for law enforcement is by no means a new issue in U.S. policing. In the 1990s, for instance, there were concerns about digital and wireless communications potentially hampering law enforcement in carrying out court-authorized surveillance. To help combat these challenges, Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414), which among other things, required telecommunications carriers to assist law enforcement in executing authorized electronic surveillance.

The technology boundary has received renewed attention as companies have implemented advanced security for their products—particularly their mobile devices. In some cases, enhanced encryption measures have been put in place resulting in the fact that companies such as Apple and Google cannot unlock devices for anyone under any circumstances, not even law enforcement.

Law enforcement has concerns over certain technological changes, and there are fears that officials may be unable to keep pace with technological advances and conduct electronic surveillance if they cannot access certain information. Originally, the going dark debate centered on law enforcement's ability to intercept real-time communications. More recent technology changes have potentially impacted law enforcement capabilities to access not only communications, but stored data as well.

There are concerns that enhanced encryption may affect law enforcement investigations. For instance, following the December 2, 2015, terrorist attack in San Bernardino, CA, investigators recovered a cell phone belonging to one of the suspected shooters. FBI Director Comey testified before Congress two months later and indicated that the bureau was still unable to unlock the device. On February 16, 2016, the U.S. District Court for the Central District of California ordered Apple to provide "reasonable technical assistance to assist law enforcement agents in obtaining access to the data" on the cell phone. The outcome of this case may have implications for how law enforcement and policy makers respond to the broader conversation on enhanced encryption.

If evidence arises that investigations are hampered, policy makers may question what, if any, actions they should take. One option is that Congress could update electronic surveillance laws to cover data stored on smartphones. Congress could also prohibit the encryption of data unless law enforcement could still access the encrypted data. They may also consider enhancing law enforcement's financial resources and manpower, which could involve enhancing training for existing officers or hiring more personnel with strong technology expertise.

Some of these options may involve the application of a "back door" or "golden key" that can allow for access to smartphones. However, as has been noted, "when you build a back door ... for the good guys, you can be assured that the bad guys will figure out how to use it as well." This is often maintained to be an inevitable tradeoff. Policy makers may debate which—if either—may be 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.

Contents

Figures

Contacts

Fast-changing technology creates a challenging environment for crime-fighting.[1] According to former Attorney General Eric Holder, "[r]ecent technological advances have the potential to greatly embolden online criminals, providing new methods ... to avoid detection."[2] Technology is a two faced creature. On the one hand, it has enhanced the speed and ease of communication and legitimate business, providing a bridge across international borders. On the other, it has opened the doors for potential exploitation by a range of malicious actors.[3]

Just as the growth of technology offers advances and challenges, so does its security. The stronger the security features of our technology, the less vulnerable the technology may be. However, if the security is sufficiently strong, the technology and its associated information may become inaccessible to legitimate law enforcement investigations. This is one aspect of the current debate surrounding smartphone and other mobile technology and security.

Smartphone ownership is on the rise, with 64% of adult Americans owning a smartphone as of October 2014.[4] Smartphones have become valuable targets for hackers because, in part, of the breadth of personal information they contain.[5] Because of this, manufacturers regularly update their devices' security features, and experts have encouraged consumers to take advantage of these features—such as locking smartphones with a passcode and encrypting the contents.[6] One current concern is that such strong security measures could not only keep out potential malicious actors, but legitimate individuals as well, including users who forget their passcodes or law enforcement with a lawful search warrant.

This report provides an overview of the perennial issue involving technology outpacing law enforcement and discusses how policy makers and law enforcement officials have dealt with this issue in the past. It discusses the current debate surrounding smartphone data encryption and how this may impact U.S. law enforcement operations. The report also discusses existing law enforcement capabilities, the debate over whether law enforcement is "going dark" because of rapid technological advances, and resulting issues that policy makers may consider.

The Technology Boundary: A Perennial Issue

Technology as a boundary for law enforcement is by no means a new issue in U.S. policing. In the 1990s, for instance, there were concerns that increasing adoption of technologies such as digital communications and encryption could hamper law enforcement's ability to investigate crime. More specifically, concerns have been whether these technologies could interfere with surveillance or the interception and understanding of certain communications.

[1] CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[2] U.S. Department of Justice, "Remarks by Attorney General Holder at the Biannual Global Alliance Conference Against Child Sexual Abuse Online," press release, September 30, 2014.

[3] See, for example, National Crime Prevention Council, *Evolving With Technology*; Reese Jones, "Criminals and Terrorists in a Borderless, Technological Arms Race," *Forbes*, July 14, 2012; and CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[4] PewResearch, *Mobile Technology Fact Sheet*, January 2014. This is up from 35% of American adults owning smartphones in May 2011, according to PewResearch, *Device Ownership Over Time*, October 2014.

[5] Kaspersky Lab and INTERPOL, *Mobile Cyber Threats*, October 2014.

[6] Roberto Baldwin, "Don't Be Silly. Lock Down and Encrypt Your Smartphone," *Wired*, October 26, 2013.

Communications Assistance for Law Enforcement Act (CALEA)

In the 1990s, there were "concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance."[7] Specifically, the Government Accountability Office (GAO; then, the General Accounting Office) cited the increasing use of digital, including cellular, technologies in public telephone systems as one factor potentially inhibiting the Federal Bureau of Investigation's (FBI's) wiretap capabilities.[8]

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 executing authorized electronic surveillance. There are several notable caveats to this requirement, however:

- Law enforcement and officials are *not* authorized to require telecommunications providers (as well as manufacturers of equipment and providers of support services) to adopt "specific design of equipment, facilities, services, features, or system configurations." 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]

A decade after the passage of CALEA, federal law enforcement officials were again concerned that their ability to conduct electronic surveillance was constrained because of constantly emerging technologies. Not all telecommunications providers had implemented CALEA-compliant intercept capabilities. As such, 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.[11] Subsequently, the FCC administratively expanded CALEA's requirements to apply to both broadband and VoIP providers.[12]

Notably, CALEA is not viewed as applying to email or data while stored on smartphones and similar mobile devices. Reportedly, there has been "intense debate" about whether it should be expanded to cover this content.[13] For instance, there have been reports over the past several years

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

[8] U.S. General Accounting Office, *FBI: Advanced Communications Technologies Pose Wiretapping Challenges*, IMTEC-92-68BR, July 17, 1992.

[9] 42 U.S.C. § 1002(b)(1).

[10] 42 U.S.C. § 1002(b)(3).

[11] 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.

[12] 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 Patricia Moloney Figliola.

[13] David E. Sanger and Brian X. Chen, "Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.," *The New York*
(continued...)

that the Administration has considered legislative proposals to amend CALEA to apply to a wider range of communications service providers such as social networking companies.[14]

Crypto Wars

Also in the 1990s, what some have dubbed the "crypto wars" pitted the government against data privacy advocates in a debate surrounding the use of data encryption.[15] This tension was highlighted by the federal investigation of Philip Zimmermann, the creator of Pretty Good Privacy (PGP) encryption software, the most widely used email encryption platform.[16] When PGP was released, it "was a milestone in the development of public 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."[17] When someone released a copy of PGP on the Internet, it proliferated, 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.[18]

Law Enforcement Use of Cell Phone Data

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. As cell phones have advanced from being purely cellular telecommunications devices into mobile computers that happen to have cell phone capabilities, the scope of data produced by and saved on these devices has morphed. In addition to voice communications, this list can include

- call detail records, including cell phone records that indicate which cell tower was used in making or receiving a call;[19]
- Global Positioning System (GPS) location points, stored both on the device and in some of its applications, indicating the location of a particular device;

(...continued)

Times, September 26, 2014.

[14] Ellen Nakashima, "Administration Seeks Ways to Monitor Internet Communications," *The Washington Post*, September 27, 2010.

[15] 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.

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

[17] 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.

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

[19] The range of any given cell tower can vary based on a variety of factors. See, for instance, "What is a Cell Tower's Range?" *The Washington Post*, June 27, 2014. See also Tom Jackman, "Experts Say Law Enforcement's Use of Cellphone Records Can Be Inaccurate," *The Washington Post*, June 27, 2014.

- data—such as email, photos, videos, and messages—stored directly on a mobile device;
- data backed up to the "cloud" and stored off a mobile device.

Cell phones "are potentially rich sources of evidence" for law enforcement.[20] Where these data are stored varies based on factors such as default smartphone settings, users' personalized settings, and telecommunications providers' policies.

When law enforcement accesses, or attempts to access this information, it is often gathered through authorized wiretaps or search warrants. It's not always clear, however, exactly how often law enforcement gathers or relies upon these data in their investigations. Data exist on the number of wiretap requests and intercept orders[21] that are issued in investigations of felonies as well as on how often law enforcement encounters encryption in carrying out these orders. These data provide a snapshot of law enforcement use of wiretaps and possible encryption barriers.

- In 2014, judges authorized 3,554 wiretaps, of which about 36% (1,279 orders) were under federal jurisdiction.[22]
- Notably, 96% (3,409) of total authorized intercept orders were for portable devices.[23]
- From the 1,279 federally authorized intercept orders, they produced an average of 5,724 intercepts, including an average of 886 "incriminating intercepts."[24]

In 2001, the Administrative Office of the U.S. Courts began collecting data on whether law enforcement encountered encryption in the course of carrying out wiretaps as well as whether officials were able to overcome the encryption and decipher the "plain text" of the encrypted information.[25] Law enforcement has reported encountering encryption in at least one instance each year, with the exception of 2006 and 2007.[26] The first known, reported instance of an authorized wiretap being stymied by encryption came in 2011.[27] In 2014, there were 4 such instances—lower than the 10 known instances from 2013 in which encryption foiled officials. [28] From the 3,554 total authorized wiretaps in 2014—of which 25 contained encrypted

[20] Christal Chan, Glenn Kolomeitz, and Tom Ralph, et al., National Association of Attorneys General, "Mobile Devices: Challenges and Opportunities for Law Enforcement," *NAAGazette*, vol. 8, no. 2.

[21] 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 for law enforcement to take measures to intercept these communications, as authorized under 18 U.S.C. § 2510-2522.

[22] Administrative Office of the U.S. Courts, *Wiretap Report 2014.* The federal statute authorizing wire, oral, or electronic communications interception is 18 U.S.C. § 2510-2522. Of note, 91% of federal intercept orders were granted for suspected narcotics violations. These data do not include those interceptions of wire, oral, or electronic communications that are regulated by the Foreign Intelligence Surveillance Act of 1978.

[23] Administrative Office of the U.S. Courts, *Wiretap Report 2014.*

[24] Administrative Office of the U.S. Courts, *Wiretap Report 2014,* Table 4. These incriminating intercepts may produce evidence implicating an individual in criminal activity.

[25] These data are reported pursuant to P.L. 106-197, the Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act.

[26] Administrative Office of the U.S. Courts, *Wiretap Report Archive.*

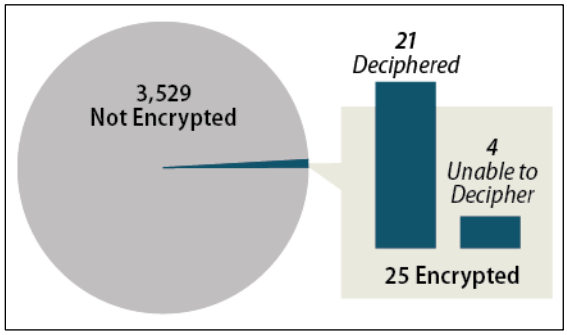
[27] This was reported as part of the U.S. Courts *Wiretap Report 2012*. Information provided to CRS by the Administrative Office of the U.S. Courts.

[28] In 2013, there were nine reported instances of officials being stymied by the encryption. In 2014, one additional instances (that had occurred in 2013) was reported. Information provided to CRS by the Administrative Office of the U.S. Courts.

communications—officials could not decipher the plain text in 4 instances (or 0.11% of authorized wiretaps).[29] Notably, these numbers relate to lawful wiretaps of certain suspected or actual criminal offenses, as authorized by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[30] The data do not include wiretaps as authorized by the Foreign Intelligence Surveillance Act of 1978 (FISA)—the law which authorizes surveillance primarily of foreign intelligence and international terrorism threats. See **Figure 1** for an illustration of the 2014 data.

As noted, law enforcement has reported encountering encryption nearly every year since 2001, though law enforcement has only encountered encryption it could not circumvent since 2011. The number of instances in which this has occurred, however, has fluctuated and has been relatively low, such that analysts cannot make claims as to whether or not this number is on a specific trajectory. The presence of reported surveillance attempts wherein encryption could not be circumvented by law enforcement may have contributed to claims that advances in encryption have outpaced law enforcement's (and others') ability to crack it.

Figure 1. Authorized Wiretaps Encountering Encryption, 2014



Source: Administrative Office of the U.S. Courts, *Wiretap Report 2014*.

Notes: These data do *not* include those interceptions of wire, oral, or electronic communications that are authorized by the Foreign Intelligence Surveillance Act of 1978.

Current Debate

In September 2014, Apple released a major update to its mobile operating system, iOS 8. In the accompanying privacy policy, Apple noted that personal data stored on devices running iOS 8 are protected by the user's passcode. Moreover, the company stated, "Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."[31] The company has also stated with respect to certain communications—namely, iMessage and FaceTime—that "Apple has no way to decrypt iMessage and FaceTime data when it's in transit between devices ... Apple doesn't scan your communications, and we wouldn't be able to comply with a wiretap order even if we wanted to."[32]

Similarly, Google's Android 5.0 mobile operating system, which launched in November 2014, includes default privacy protections such as automatic encryption of data that is protected by a passcode.[33] When devices running Android 5.0 are locked, data on them are only accessible by

[29] Administrative Office of the U.S. Courts, *Wiretap Report 2012*. Administrative Office of the U.S. Courts, *Wiretap Report 2013*. There were also 52 encryption instances newly reported for 2012, though law enforcement was able to decipher all of these.

[30] 18 U.S.C. § 2516.

[31] Apple, "Privacy: Government Information Requests," as of the date of this report.

[32] Apple, "Privacy: Privacy Built In," as of the date of this report.

[33] Android Official Blog, "A Sweet Lollipop, With a Kevlar Wrapping: New Security Features in Android 5.0," October 28, 2014.

entering a valid password, to which Google does not have a key. Thus, like Apple, Google is not able to unlock encrypted devices.[34]

Apple's Elimination of a Back Door "Key"

In earlier versions of Apple's mobile operating system—prior to iOS 8—Apple maintained a "key" that allowed the company to unlock any device without the passcode. As such, when presented with a search warrant or a wiretap order, Apple had the ability to unlock devices for law enforcement. While this back door key was able to assist in legitimate law enforcement investigations, it was also vulnerable to exploitation by hackers, criminals, and others. iOS 8 enhanced automatic encryption and eliminated the back door key. Along with this was the elimination of Apple's ability to unlock the device for anyone under any circumstance.

Enhanced data encryption, in part a response to privacy concerns following Edward Snowden's revelations of mass government surveillance, has opened the discussion on how this encryption could impact law enforcement investigations.[35] Law enforcement officials have likened the new encryption to "a house that can't be searched, or a car trunk that could never be opened."[36] There have been concerns that malicious actors, from savvy criminals to terrorists to nation states, may rely on this very encryption to help conceal their illicit activities. There is also concern that law enforcement may not be able to bypass the encryption, their investigations may be stymied, and criminals will operate above the law. Critics of these concerns contend that law enforcement maintains adequate tools and capabilities needed for their investigations.[37]

Major Components: Communications and Stored Data

Developments in encryption—and companies' implementation of enhanced data protections—have reinvigorated the debate regarding the balance between privacy needs and information access. Most recently, the conversation has largely been in the context of smartphones and mobile devices. These devices present a unique discussion point because they bridge the realms of communications and stored data.

Real Time Access to Encrypted Communications

CALEA requires that telecommunications carriers (including broadband Internet access and VoIP providers) assist law enforcement in executing authorized electronic surveillance of real time communications. However, some developments in the communications landscape have allowed some communications to be exempt from being wiretap-ready, as is otherwise mandated by CALEA.

- First, some companies, for instance Apple, have implemented text messaging systems—Apple's is the iMessage—that are not readable by telecommunications (or broadband or VoIP) providers. Therefore, these communications fall outside of CALEA mandates.

[34] Craig Timberg, "Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police," *The Washington Post*, September 18, 2014.

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

[36] Devlin Barrett and Danny Yadron, "New Level of Smartphone Encryption Alarms Law Enforcement," *The Wall Street Journal*, September 22, 2014.

[37] See, for example, Ken Gude, "The FBI Is Dead Wrong: Apple's Encryption Is Clearly in the Public Interest," *Wired*, October 17, 2014.

- Also, Apple has implemented end-to-end encryption of messages sent through the iMessage system between Apple devices and does not maintain a key to decrypt these messages. CALEA exempts from its requirements encrypted communications for which telecommunications carriers (as well as manufacturers and service providers such as Apple) do not have a key.[38]

As evolving technology changes how communication takes place, not all communications may be readily accessible to law enforcement, regardless of whether law enforcement presents a warrant for a wiretap.[39] If technology companies do not retain the ability to decrypt certain communications, they, in turn, may be unable to help law enforcement conduct court-authorized electronic surveillance of these communications.

Encryption of Data Stored on Smartphones

In addition to encryption's effect on access to communications data generated and received by smartphones, encryption also directly affects access to data stored on these mobile devices (as well as data stored elsewhere that may be retrieved via the mobile device). If companies like Apple and Google provide for encryption of data on locked mobile devices—and do not maintain the keys to unlock these devices—the companies may be unable to assist law enforcement in carrying out court-authorized searches of content stored on the device—even if the police possess a warrant.[40] As these companies have noted, because they *cannot* break the encryption of a locked device, they also *cannot* provide decrypted information to authorities.

Some have questioned how challenges for police in cracking encryption to obtain information on smartphones compare to those in obtaining information stored in other types of containers such as home safes and safe deposit boxes.

Master Keys

Technology companies like Apple and Google are not required under federal law to maintain a key to unlock the encryption of their devices sold to consumers. If they did maintain a key, however, they may be required to provide this key to unlock devices for law enforcement presenting a valid search warrant.

Similarly, safe manufacturers are not required under federal law to maintain the combination or key to safes sold to consumers. However, if manufacturers voluntarily maintained such a master key, they, too, may be required to provide assistance to law enforcement to access the safe. In addition, if law enforcement presents a warrant to search an individual's safe deposit box, a bank may assist law enforcement by providing a master key for the box.[41]

[38] Notably, if a message is sent between an Apple device and a non-Apple device, law enforcement may be able to intercept it because (1) it would involve a telecommunications carrier on the end of the non-Apple device and (2) the message may not be encrypted on the end of the non-Apple device.

[39] Generally, law enforcement needs a warrant to execute a wiretap.

[40] Notably, while law enforcement generally does not need a warrant to search items found on suspects at the time of arrest, the Supreme Court (in *Riley v. California*) has ruled that this exception does not apply to digital information on cell phones; police need a warrant to search these devices. See *Riley v. California*, 13-132 (2013). See also CRS Legal Sidebar WSLG987, *Supreme Court Says "Get a Warrant" Before Searching Cell Phones*, by Richard M. Thompson II.

[41] Instances of this assistance exist. See, for example, United States v. Scolnick, United States Court of Appeals Third Circuit.

Cryptanalytic Attack

Since some companies may not retain a key to open a locked mobile device, one option for law enforcement in attempting to obtain information on a device for which they have a valid search warrant may be to use a cryptanalytic attack. One such form of cryptanalytic attack has been referred to as "brute force."[42] Using this method, law enforcement would likely use software to try every possible combination of keys in an attempt to unlock the device. The success of this method may depend, among other things, on the amount of time available to try and unlock a device and on the number of keys used in the passcode. FBI Director Comey has cited barriers to law enforcement relying upon brute force tactics to break encryption. One challenge he has noted is increasingly advanced encryption techniques that even "supercomputers" may not be able to crack. In addition, "some devices have a setting whereby the [data] is erased if someone makes too many attempts to break the password, meaning no one can access that data."[43]

Just as police may use brute force to try and break encryption when executing a search warrant, they are authorized to break other locks—such as those to physical buildings—in order to carry out a lawful search with a warrant. The Supreme Court has noted that "[i]t is well established that law officers constitutionally may break and enter to execute a search warrant where such entry is the only means by which the warrant effectively may be executed."[44]

Going Dark or Going Forward?

As modern technology has developed, there has arguably been an evolving gap between law enforcement's investigative authorities and capabilities to carry out authorized activities. This is not a new phenomenon; rather, as experts have noted, "[l]aw enforcement has been complaining about 'going dark' for decades now."[45] The FBI, for instance, established a Going Dark initiative in an attempt to maintain law enforcement's ability to conduct electronic surveillance in a rapidly changing technology environment.[46]

Originally, the "going dark" debate centered on law enforcement's ability to intercept real-time communications. As communications technologies evolved, so did questions about whether or how law enforcement could work within existing electronic surveillance laws to carry out court-authorized surveillance on real time communications. Experts, officials, and stakeholders debated whether certain laws such as CALEA should be expanded to require additional entities—such as all VoIP and Internet service providers—to assist law enforcement in accessing this real-time information. The most recent encryption enhancements by companies like Apple and Google "highlight the continuing challenge for law enforcement in responding to new technologies. Other innovations, such as texting, instant messaging and videogame chats, created hurdles to

[42] See Matt Curtin, *Brute Force: Cracking the Data Encryption Standard* (Springer Science & Business Media, 2007). See also Jeremy Kirk, "Four-Digit Passcodes are a Weak Point in iOS 8 Data Encryption," *ComputerWorld*, October 8, 2014.

[43] Federal Bureau of Investigation, "James B. Comey, FBI Director, before the Brooking Institution, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*," press release, October 16, 2014.

[44] Dalia v. United States, 441 U.S. 238, 247, 99 S. Ct. 1682, 1688, 60 L. Ed. 2d 177 (1979). See also 18 U.S.C. § 3109.

[45] Bruce Schneier, "Stop the Hysteria Over Apple Encryption," *Schneier on Security*, October 3, 2014.

[46] Electronic Frontier Foundation, Expanding CALEA and Electronic Surveillance Laws, FBI "Going Dark" FOIA Documents – Release 1, Part 1, https://www.eff.org/document/fbi-going-dark-foia-documents-release-1-part-1. The FBI's FY2010 budget request specified an "Advanced Electronic Surveillance, otherwise known as the FBI's Going Dark Program. This program supports the FBI's electronic surveillance (ELSUR), intelligence collection and evidence gathering capabilities, as well as those of the greater Intelligence Community (IC)."

monitoring communication," though some contend that law enforcement has found means to overcome many of these technological challenges.[47] Others, however, are concerned about law enforcement's ability to keep pace with advancing technology, particularly "the expansion of online communication services that—unlike traditional and cellular telephone communications—lack intercept capabilities because they are not required by law to build them in."[48]

Concerns over "going dark" have become two–pronged. More recent technology changes have potentially impacted law enforcement capabilities to access not only communications, but stored data. As a result, current law enforcement concerns around "going dark" now involve how, in practice, encryption of stored data, as currently implemented by technology companies may affect law enforcement investigations. Analysts have not yet seen data on whether or how encryption has affected law enforcement access to stored data or influenced the outcome of cases. In the past, Congress has requested that similar information be collected and reported. P.L. 106-197 required the Administrative Office of the U.S. Courts to report on whether law enforcement encountered encryption in the course of carrying out wiretaps, as well as whether officials were prevented from deciphering the "plain text" of the encrypted information. While current data collection and reporting requirements on encryption relate to real time *communications*, policy makers may debate the potential utility of asking law enforcement to report on encryption relating to *stored data* as well.

While some contend that law enforcement is "going dark," others have argued that law enforcement and intelligence agencies are in a "golden age of surveillance," with more robust surveillance capabilities.[49] They contend that police access to location data, information about individuals' contacts, and a host of websites that collectively create "digital dossiers" on a person all enhance law enforcement surveillance.[50] Those who see the current technology environment as a golden age of surveillance may believe that, while technology advances (such as encryption) may slow or stymie law enforcement access to certain information, these advances can also create alternate opportunities for information access that law enforcement can learn to harness.

One particular case has recently highlighted this debate. Following the December 2, 2015, terrorist attack in San Bernardino, CA, investigators recovered a cell phone belonging to one of the suspected shooters. FBI Director Comey testified before Congress two months later and indicated that the bureau was still unable to unlock the device.[51] On February 16, 2016, the U.S. District Court for the Central District of California ordered Apple to provide "reasonable technical assistance to assist law enforcement agents in obtaining access to the data" on the cell phone.[52] The outcome of this case may have implications for how law enforcement and policy makers respond to the broader conversation on enhanced encryption.

---

[47] Devlin Barrett and Danny Yadron, "New Level of Smartphone Encryption Alarms Law Enforcement," *The Wall Street Journal*, September 22, 2014.

[48] Ellen Nakashima, "Proliferation of New Online Communications Services Poses Hurdles for Law Enforcement," *The Washington Post*, July 26, 2014.

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

[50] Ibid.

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

[52] United States District Court for the Central District of California, In 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, *Order Compelling Apple, Inc. to Assist Agents in Search*, February 16, 2016.

Evaluating a Need for Action

If there is evidence that investigations are hampered or that lives are at risk because of law enforcement's inability to access critical encrypted information, will there need to be some sort of compromise between law enforcement and the technology industry?[53] What might be the congressional role? Policy makers may weigh whether aiding federal law enforcement will involve incentives or requirements for communications and technology companies to provide specified information to law enforcement, enhanced investigative tools, bolstered financial and manpower resources to help law enforcement better leverage existing authorities, or combinations of these and other options.

Requirements for Communications and Stored Data Access

In debating law enforcement's need to access certain real time communications and stored data, Congress could move to update CALEA and related laws to cover a broader range of communications and data. Currently, requirements under CALEA apply to telecommunications carriers as well as facilities-based broadband Internet access and interconnected Voice over Internet Protocol (VoIP) providers. Proposals have reportedly been floated that would extend CALEA requirements to apply to a wider range of technology services and products such as instant messaging, video game chats, and real-time video communications like Skype.[54] Proponents of expanding CALEA mandates may believe that it would enhance law enforcement's abilities to carry out existing authorities to intercept real time communications. Opponents to CALEA expansion proposals, however, may contend that mandating other communications services and technology manufacturers to build in intercept capabilities could be costly, both financially and in terms of security. Financially, companies may need to dedicate resources to reengineer their products; they may need to add or allocate personnel to liaise with law enforcement to facilitate wiretap requests. On the security front, companies would necessarily need to build in a "back door" to allow for authorized access, and any means of access necessarily opens the doors to exploitation.

If policy makers are interested in requiring technology companies to assist law enforcement carry out authorized surveillance and searches, legislators may consider options other than amending CALEA. One such option may be to directly mandate that technology companies build in "back door" access for law enforcement into specified communications products sold in the United States. One unintended consequence of this could be that U.S. consumers, in search of privacy, might buy more products from

The Back Door Tradeoff

Back doors, also referred to as front doors or golden keys, are essentially holes in security. They can be in systems intentionally or unintentionally. As experts have noted, "[w]hen you build a back door ... for the good guys, you can be assured that the bad guys will figure out how to use it as well."[55] This is the tradeoff. Policy makers may debate which is more advantageous for the nation on the whole: (1) increased security coupled with potentially fewer data breaches and possibly greater impediments to law enforcement investigations, or (2) increased access to data paired with potentially greater vulnerability to malicious actors.

[53] Editorial Board, "Compromise Needed on Smartphone Encryption," *The Washington Post*, October 3, 2014.

[54] See, for example Ben Adida, Collin Anderson, and Annie Anton, et al., "CALEA II: Risks of Wiretap Modifications to Endpoints," May 17, 2013.

[55] John Backus, "Commentary: Don't Let the FBI Wiretap Your Smartphone Apps," *The Washington Post*, July 7, 2013.

overseas, and consumers outside the United States might decline to buy certain U.S. products that conform with these requirements.

Law Enforcement Tools

While placing requirements on technology companies may be one route to assisting law enforcement, policy makers may also debate options that could enhance the tools available to law enforcement. These could include making it a crime for an individual (when presented with a court authorized warrant) to fail to turn over his passcode or other information that would allow law enforcement to decrypt a given device. However, those in support of encryption note that a search warrant is "an instrument of permission, not compulsion."[56] In other words, individuals need not proactively reveal or open hiding places for investigators presenting a search warrant. Additionally, judges may in some cases be able to hold individuals in contempt for failure to turn over information that would help law enforcement unlock certain electronic devices.

Although technology companies like Apple and Google may not have the ability to unlock and thus reveal some information stored *on* locked, encrypted smartphones, they generally retain the ability to turn over information on unencrypted communications and data stored *off* the devices in locations such as the "cloud."[57] As such, some supporting encryption may contend that regardless of what data in motion may be encrypted or what data is encrypted on locked devices, law enforcement still has effective tools to retrieve digital data. Encryption proponents may also suggest that stronger digital security could benefit law enforcement by helping prevent malicious activity, including hacks and data breaches.

Law Enforcement Capabilities

Combating malicious actors (including cybercriminals and those who exploit technology to conceal their crimes) is an issue that cuts across the investigative, intelligence, prosecutorial, and technological components of law enforcement. Because clear data on how technological advances such as enhanced encryption of communications and stored data on mobile devices may impact law enforcement capabilities to combat these bad actors do not exist, policy makers may be hesitant to take any significant legislative actions to "fix" a problem of an unknown magnitude. Even if policy makers believe there is a significant problem with law enforcement's ability to carry out authorized activities, they may debate whether expanding requirements for certain technology companies and communications services or adding to law enforcement's toolbox of authorities may be the more appropriate options. Some have argued that another option may be to enhance law enforcement's financial resources and manpower. This could involve enhancing training for existing officers or hiring individuals with bolstered technology expertise.

[56] Kevin Poulsen, "Apple's iPhone Encryption is a Godsend, Even if Cops Hate It," *Wired.com*, October 8, 2014.

[57] This ability is subject to various statutory restrictions and may depend on the location of the server.

Author Contact Information

Kristin Finklea
Specialist in Domestic Security
kfinklea@crs.loc.gov, 7-6259