Court-Ordered Access to Smart Phones: In Brief

Kristin Finklea
Specialist in Domestic Security

Richard M. Thompson II
Legislative Attorney

Chris Jaikaran
Analyst in Cybersecurity Policy

February 23, 2016

Congressional Research Service
7-5700
www.crs.gov
R44396

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The tension between the benefits and challenges of encryption has been an issue for law enforcement and policymakers since the 1990s, and was reinvigorated in 2014 when companies like Apple and Google implemented automatic enhanced encryption on mobile devices and certain communications systems. Companies using such strong encryption do not maintain "back door" keys and, therefore, now cannot easily unlock, or decrypt, the devices—not even when presented with a valid legal order. Law enforcement concerns about the lack of back door keys were highlighted by the November and December 2015 terrorist attacks in Paris, France, and San Bernardino, CA. Questions arose as to whether the attackers used strong encryption and, more importantly, if they did, whether and how this might have hindered investigations.

Following the December 2, 2015, terrorist attack in San Bernardino, CA,, U.S. investigators recovered a cell phone reportedly used by one of the shooters. Federal Bureau of Investigation (FBI) Director James B. Comey testified before Congress two months later, indicating that the Bureau was still unable to access the information on that 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 order directs Apple's assistance to feature three components:

- bypass or disable the iPhone's auto-erase after 10 incorrect passcode attempts function (even if the function has not been enabled);
- enable the FBI to electronically input passcodes for testing; and
- ensure there is no added delay between passcode attempts.

The order is not for Apple to decrypt the device itself, something which Apple has publicly stated it cannot do. Instead, this order would enable the FBI to automate the attempts of every possible passcode for the device until the right combination of characters is hit upon by pushing a software update to the iPhone in question's operating system.

Apple is contesting the order, which will require the magistrate judge, and perhaps the district and appeals courts, to assess whether the All Writs Act (28 U.S.C. §1651) can be interpreted broadly to grant the relief the government seeks. The All Writs Act, enacted as part of the first Judiciary Act of 1789, provides a residual source of legal authority to federal judges to enforce the orders of their courts. Whether the All Writs Act can be read to include such an order will largely depend on two inquiries: first, whether a reviewing court would view the FBI's request as an "unreasonable burden" on Apple under the 1977 Supreme Court case *United States v. New York Tel. Co.*; and, second, whether such a command is consistent with the intent of Congress. This is a fact-intensive inquiry, the contours of which are uncertain.

Policymakers may ask a number of questions with respect to the order from the Central District of California and the larger ongoing encryption debate. Apple has indicated that it is possible to develop an alternate operating system for the iPhone in question that would accomplish the items in the court order. As such, a main question now is whether it *should* be done. Will doing so effectively create a "back door" to the encryption? What precedent might be set by Apple providing the court-ordered assistance? If Apple develops an alternate operating system to comply with this order, would Apple and other companies have to comply with similar requests in other law enforcement investigations? In addition, as a multinational corporation, would Apple need to comply with requests from other national governments?

Contents

Contacts

Encryption and Law Enforcement Investigations

Encryption and other technologies can foster increased privacy and heightened security. Simultaneously they have been cited as presenting hurdles for law enforcement and intelligence officials.[1] On the one hand, some contend that technological developments have resulted in a "golden age of surveillance" for law enforcement; the large amount of information that investigators have at their fingertips—access to location data, information about individuals' contacts, and a range of websites—collectively form "digital dossiers" on individuals.[2] On the other hand, some argue that law enforcement is "going dark" as their capabilities are outpaced by the speed of technological change, and thus they cannot access certain information they are otherwise legally authorized to obtain.[3]

The tension between the benefits and challenges of encryption is not new. It started in the 1990s and was reinvigorated in 2014 when companies like Apple and Google implemented automatic full-device encryption for mobile devices and automatic encryption for certain communications systems.[4] Companies using such strong encryption assert they do not maintain encryption keys and therefore cannot unlock, or decrypt, the devices or communications—not even when presented with a court authorized wiretap order.

Law enforcement concerns about the lack of encryption keys were highlighted by the November and December 2015 terrorist attacks in Paris, France, and San Bernardino, CA.[5] Questions arose as to whether the attackers used strong encryption and, more importantly, if they did, whether and how this might have hindered investigations. These questions have reopened larger discussions on how encryption and quickly advancing technologies could impact law enforcement operations.

This report specifically examines certain encryption issues that have been raised in the investigation of the December 2, 2015, terrorist attack in San Bernardino, CA. Following the attack, U.S. investigators recovered a cell phone reportedly used by one of the shooters. Federal Bureau of Investigation (FBI; Bureau) Director James B. Comey testified before Congress two months later, indicating that the Bureau was still unable to access the information on the device.[6] This report highlights certain issues that policymakers may examine as they follow the ongoing dispute between law enforcement and technology companies. While this is a fast-moving issue with many components, this report focuses on questions related to the government's request. The topics discussed are based on developments in the case as of the date of this report.

[1] For more information on this tension, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea.

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

[3] Federal Bureau of Investigation, *Going Dark Issue*, https://www.fbi.gov/about-us/otd/going-dark-issue.

[4] For more information on the Crypto Wars of the 1990s, see also CRS Insight IN10440, *Renewed Crypto Wars?*, by Kristin Finklea.

[5] 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.

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

Access to San Bernardino iPhone

On February 16, 2016, the U.S. District Court for the Central District of California ordered Apple, Inc. under the All Writs Act[7] to provide "reasonable technical assistance to assist law enforcement agents in obtaining access to the data" on the cell phone for which the government had already obtained a probable cause warrant.[8] The order directs Apple's assistance to feature three components:

- bypass or disable the iPhone's auto-erase after 10 incorrect passcode attempts function (even if the function has not been enabled);
- enable the FBI to electronically input passcodes for testing; and
- ensure there is no added delay between passcode attempts.

In other words, it essentially asks Apple to create an operating system update that will allow the FBI to (1) enter more than 10 passcodes without the risk of the data being wiped after the tenth incorrect try; (2) automate the entry of those passcode combinations rather than entering them manually; and (3) try back-to-back passcode attempts without the gradually increasing delays between attempts that is currently programmed into the system.[9] This would allow the FBI to try and "brute force" open the iPhone by continuously entering passcode attempts until the correct one is identified.[10] Notably, the order is not asking Apple to provide an encryption key or to break the encryption on the device.

The company sees this as "an overreach by the U.S. government" and is opposing the order.[11] An operating system allowing law enforcement to use brute force to open the phone in this case could potentially be replicated and used to open other phones in cases where law enforcement demonstrates lawful need. If the technology then falls into the wrong hands, it could potentially be exploited by criminals and other malicious actors.

Encryption and the iPhone

There is much debate over whether the government's request in the San Bernardino case would constitute the creation of a so-called "back door" or "master key" to the iPhone's encryption. Apple views the government's order as directing a back door be built into its product. It sees the access of any entity, including a government agency, to encrypted user data without the user's explicit authorization, as a back door.[12] In Apple's view, the government is a third party, and only those who are authorized by either the owner/sender of the information (first party) or the recipient of the information (second party) have a right to that information. Apple's view is shared by other technology companies.[13] The government, however, does not consider its request to

[7] *See* All Writs Act, *infra* pp. 2-4.

[8] *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 19, 2016)..

[9] Peter Bright, "Encryption Isn't At Stake, The FBI Knows Apple Already Has The Desired Key," *ARS Technica*, February 18, 2016.

[10] Ibid.

[11] Letter from Apple CEO, Tim Cook, A Message to Our Customers (February 16, 2016), *available at* http://www.apple.com/customer-letter/.

[12] Apple views this specific request as a back door. See letter from Apple CEO, Tim Cook, A Message to Our Customers (February 16, 2016), *available at* http://www.apple.com/customer-letter/.

[13] Nick Wingfield and Mike Isaac, "Apple Letter on iPhone Security Draws Muted Tech Industry Response," *The New*
(continued...)

enable a back door.[14] The order does not request that Apple create a master key, or create a new decryption key in the software that can be used against any iPhone. It narrowly limits the request to Apple's assistance to the specific phone, with the updated operating system only being applicable to the iPhone with the serial number and other unique identifiers in this case.

Since 2014, Apple has enabled full disk encryption on iPhones. This ensures the data on a given phone are safe from unauthorized disclosure while *at rest*. This is different from the encryption of iMessage communications, which ensures the data *in transit* are safe from authorized disclosure. Examples of information protected on the iPhone with full-disk encryption[15] include geographic location data (where the phone has been) as well as contacts and pictures that were not backed up to an online service.

Longer passwords offer more potential combinations, and thus it can be potentially more time-consuming to identify the correct password. Using an automated password guesser, and given the hardware limits of the iPhone 5c, if the phone has a four-digit passcode, it would take about 13 minutes to guess every possibility (10,000 passcode combinations). If that passcode is six-digits, it would take roughly 22 hours to guess all of the one million combinations. If the phone is secured with an eight-character password (letters and numbers, upper and lower case), it would take over 500,000 years to guess every combination.[16]

To accomplish what is requested in the court order, the FBI needs Apple, rather than a different entity, to develop this software update. This is because of the method Apple uses to ensure the integrity of all the software that runs when an iPhone is turned on. iPhones look for an Apple certificate which is cryptographically signed before it will boot into the operating system. Without that certificate of assurance, the data would remain encrypted on the device and inaccessible. While it is possible to reverse engineer a software update to the operating system in order to enable unlimited passcode attempts, it is computationally expensive (i.e., time and energy) to recreate that cryptographically signed certificate. Some have suggested that if Apple chooses not to comply, the FBI could likely employ hackers to develop a system.[17]

Of note, the court order does not request or compel Apple to compromise implementation of encryption on all iPhones. The order directs Apple to insert a weakness into the implementation—unlimited passcode attempts and no danger of the phone being wiped because of incorrect guesses—only for the iPhone in question.

(...continued)

York Times, February 18, 2016. Accessible online at http://www.nytimes.com/2016/02/19/technology/tech-reactions-on-apple-highlight-issues-with-government-requests.html

[14] Cory Bennett, "White House Denies FBI Seeking "Back Door" to Apple iPhones," *The Hill*, February 17, 2016.

[15] The iPhone (such as the iPhone 5c which is the subject of the court order) uses Advanced Encryption Standard (AES) with 256 bit keys to encrypt the contents of the phone. AES-256 is regarded as a very secure encryption method, suitable for classified information, according to the National Security Agency (available online at https://www.nsa.gov/ia/programs/suiteb_cryptography/).

[16] CRS calculations based on the iPhone 5c running the cryptographic calculation of combining the users' input (passcode or password) with the unique identifiers embedded in the phone and a maximum processing time of 80 milliseconds per attempt.

[17] Peter Bright, "Encryption Isn't At Stake, The FBI Knows Apple Already Has The Desired Key," *Ars Technica*, February 18, 2016.

Mandated Assistance under the All Writs Act

The legal question in the San Bernardino case turns primarily on whether the All Writs Act can be interpreted broadly enough to require Apple to help the government in accessing the data on the device against its wishes.[18] The All Writs Act, enacted as part of the Judiciary Act of 1789,[19] provides that federal courts "may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[20] The Supreme Court has observed that "[t]he All Writs Act is a residual source of legal authority to issue writs that are not otherwise covered by statute."[21] A writ is a court order to do or not do something. Although the All Writs Act was penned 226 years ago, the debate in the San Bernardino case, and similar past litigation, has centered on a much more recent, although pre-digital 1977 case, *United States v. New York Tel. Co*.[22]

Relying on the All Writs Act, the Court in *New York Tel. Co*. upheld an order directing the New York Telephone Company to assist the government in installing a pen register—a device for recording the outgoing numbers dialed on a telephone—for which it already obtained a probable cause warrant to do so.[23] The Court observed that the act extends "to persons who, though not parties to the original action or engaged in any wrongdoing, are in a position to frustrate the implementation of the order or the proper administration of justice."[24] While the Court accepted that the All Writs Act can apply to third parties, it observed that "unreasonable burdens may not be imposed."[25] To determine the reasonableness of the order in that case, the Court assessed a seemingly *non*-exhaustive list of factors, including (1) the company was not "so far removed from the underlying controversy" to avoid compliance; (2) the order required only "meager assistance" from the company; (3) the telephone company was a "highly regulated public utility with a duty to serve the public"; (4) the company had not proffered a "substantial interest in not providing assistance"; the use of the pen register was not "offensive" to the company; (5) the company regularly employed such devices for billing purposes: (6) the company had previously promised to provide the FBI instructions on how to install its own pen register; (7) the order was in no way "burdensome"; (8) the order provided the company be fully reimbursed for its efforts; (9) compliance with the order required "minimal effort" by the company; and (10) there were "no disruptions to its operations."[26] Additionally, the Court observed that the order was "consistent with the intent of Congress."[27] As noted by one commentator, although the Court established a list of factors to consider, it is not clear, among other things, how much weight should be given to

[18] Since the Government obtained a valid probable cause warrant in this case, Apple is not contesting the search of the device under the Fourth Amendment. Thus, any privacy interest involved must derive from some other constitutional, statutory, or extra-constitutional source.

[19] Act of Sept. 24, 1789, 1 Stat. 81-82.

[20] 28 U.S.C. §1651(a).

[21] Pennsylvania Bureau of Correction v. U.S. Marshals Service, 474 U.S. 34, 43 (1985).

[22] United States v. New York Tel. Co., 434 U.S. 158 (1977).

[23] *Id.* at 161-62.

[24] *Id.* at 174.

[25] *Id.* at 172.

[26] *Id.* at 174-75

[27] *Id.* at 172.

each factor, or how these factors might apply to future cases, like the request before the Central District of California.[28]

In recent years, courts have been required to apply the All Writs Act and the *New York Tel. Co.* factors to requests by the government to access data stored on various locked electronic devices. For instance, in an unreported 2014 ruling, the Southern District of New York (S.D.N.Y.) read *New York Tel. Co.* and subsequent lower court case law to *require* an unnamed company to unlock a smart phone.[29] However, in a pending case in the Eastern District of New York, a magistrate judge issued a preliminary ruling in October 2015 *rejecting* the government's request to unlock an iPhone 5c running an earlier version of iOS.[30] In the latter case, the magistrate judge was largely persuaded by the fact that "Congress has done nothing that would remotely suggest an intent to force Apple, in the circumstances of this case, to provide the assistance the government now requests."[31]

While the San Bernardino case is not the first in which Apple has been ordered to assist the government in unlocking an iPhone, it appears to be the first time Apple has been asked to write and install unique software on a specific device. Without congressional action, the Central District of California and future courts must apply the *New York Tel. Co.* factors, with minimal guidance provided by lower court case law. Of the *New York Tel. Co.* factors, two appear especially relevant to the San Bernardino case.

First, is whether a reviewing court would view the "unreasonable burden" test as including an assessment of not only the burden on Apple in creating and installing new software on this particular phone, but also the burden on Apple's business as a whole. While one factor from *New York Tel. Co* is the extent to which the legal order would "disrupt[] … the operations" of the business in question, it is not certain whether the focus should be on the disruption posed by the immediate need to unlock the phone, or the potentially larger disruption to Apple's financial bottom line. Apple has acknowledged that it has the technical capacity to unlock the device, but asserts that the desire to protect the privacy and security of its customers is sufficient to warrant its opposition to the court's order.[32]

Second, is how much weight, if any, a reviewing court should place on the fact that Congress has debated, but not enacted, a law mandating forced decryption on U.S technology companies. The Supreme Court has noted that "where a statute *specifically addresses the particular issue at hand*, it is that authority, and not the All Writs Act, that is controlling."[33] The question here is whether the Communications Assistance for Law Enforcement Act (CALEA)[34] can be read as "specifically address[ing]" the relief the government seeks. Although Congress failed to include

---

[28] Orin Kerr, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 2, the All Writs Act*, THE VOLOKH CONSPIRACY (February 19, 2016), *available at* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/19/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-2-the-all-writs-act/.

[29] *In re* Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by this Court by Unlocking a Cell Phone, No. 14-2258, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014).

[30] *In re* Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. 1:15-01902, 2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015).

[31] *Id.* at *5.

[32] Letter from Apple CEO, Tim Cook, A Message to Our Customers (February 16, 2016), *available at* http://www.apple.com/customer-letter/.

[33] Pennsylvania Bureau of Correction v. U.S. Marshals Service, 474 U.S. 34, 43 (1985).

[34] For more information on CALEA, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea.

companies like Apple in CALEA's mandate that a "telecommunications carrier" must assist the government in "intercept[ing]" communications carried by the provider,[35] this issue was on Congress's radar in 1994 during passage of CALEA.[36] Congress explicitly excluded "information services" from CALEA's scope.[37] The government takes the position, however, that unless and until Congress actually *enacts* legislation on this issue, congressional silence does not suffice to limit the authority of the federal courts to require Apple to help the government access potentially vital information on this and other devices.[38]

Apple has informed the court that it will contest the February 16 order. Its motion and opposition to the government's brief are due by February 26, 2016, and a court hearing with both parties is to be held on March 22, 2016.[39]

Questions Going Forward

In response to this legal debate, policymakers may ask a number of questions with respect to the order from the Central District of California and the larger ongoing encryption debate. Apple has indicated that it is possible to develop an alternate operating system for the iPhone in question that would accomplish the items in the court order. [40] As such, the focus now has been on whether it *should* be done. Will doing so effectively create a "back door" to the encryption?

Creating a one-time software update is not without risks. Apple employees and others who have access to the software used to reduce the security of the iPhone may use that knowledge for malicious purposes later. The insider threat has long been considered the greatest threat to cybersecurity—an authorized employee who has access and knowledge of the company has the ability to do far greater harm than someone from the outside.[41] Once Apple creates such a software update to inhibit its encryption implementation, it exists in the world and there is no guarantee that a disgruntled employee or one who is bought would not leak the code to an adversary who may use it against the U.S. or its interests in the future. And even though this particular case is for the iPhone (limited by its unique identifiers), it is conceivable that those

[35] 47 U.S.C. §1002(a)(1).

[36] H. R. Rep. 103-827 (1994) ("Also excluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line."); ("The term 'information services' includes messaging services offered through software such as groupware and enterprise or personal messaging software, that is, services based on products (including but not limited to multimedia software) of which Lotus Notes (and Lotus Network Notes), Microsoft Exchange Server, Novell Netware, CC: Mail, MCI Mail, Microsoft Mail, Microsoft Exchange Server, and AT&T Easylink (and their associated services) are both examples and precursors. It is the Committee's intention not to limit the definition of 'information services' to such current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of 'information services.' By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill.").

[37] 47 U.S.C. §1002(b)(2)(A).

[38] *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 24-25 (C.D. Cal. February 19, 2016) (government's motion to compel Apple, Inc. to comply with this court's February 16, 2016, order compelling assistance in search).

[39] *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 (C.D. Cal. February 19, 2016) (scheduling order).

[40] Letter from Apple CEO, Tim Cook, Answers to Your Questions About Apple and Security, *available at* http://www.apple.com/customer-letter/answers/.

[41] Dawn M. Cappelli, Akash G. Desai, and Andrew P. Moore, et al., *Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks*, Software Engineering Institute, March 2007.

identifiers can be swapped with other identifiers in the future to make the compromised operating system more widely applicable to the universe of iPhones in the world.

If Apple develops an operating system update to comply with the court order, what precedent does this set for Apple and other companies' compliance with future 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.[42] Would Apple, Google, and others need to help the FBI develop operating systems to circumvent security features in every case where the FBI requests assistance?

If Apple complies with the U.S. court order to help the FBI, would this set a precedent for Apple to help law enforcement in other countries? Apple is a multi-national corporation that manufactures phones sold around the world. Would Apple now need to help international law enforcement entities with similar requests? What burden might this place on Apple and other companies going forward?

Author Contact Information

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

Chris Jaikaran
Analyst in Cybersecurity Policy
cjaikaran@crs.loc.gov, 7-0750

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

[42] 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.