Congressional Research Service
Informing the legislative debate since 1914

Encryption: Selected Legal Issues

name redacted
Legislative Attorney

name redacted
Analyst in Cybersecurity Policy

March 3, 2016

Congressional Research Service
7-....
www.crs.gov
R44407

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

In 2014, three of the biggest technology companies in the United States—Apple, Google, and Facebook—began encrypting their devices and communication platforms by default. These security practices renewed fears among government officials that technology is thwarting law enforcement access to vital data, a phenomenon the government refers to as "going dark." The government, speaking largely through Federal Bureau of Investigations (FBI) Director James Comey, has suggested that it does not want to ban encryption technology, but instead wants Silicon Valley companies to provide a technological way to obtain the content stored on a device for which it has legal authority to access. However, many in the technology community, including technology giants Apple, Google, and Facebook, and leading cryptologists have argued that it is not technologically feasible to permit the government access while continuing to secure user data from cyber threats. This problem is exacerbated by the fact that some suspects may refuse to unlock their device for law enforcement.

The current debate over encryption raises a wide range of important political, economic, and legal questions. This report, however, explores two discrete and narrow legal questions that arise from the various ways the government has attempted to access data stored on a smartphone. One method has been to attempt to compel a user to either provide his password or decrypt the data contained in a device pursuant to valid legal process. This prompts the first question: whether the Fifth Amendment right against self-incrimination would bar such a request. Generally, documents created independent of a government request (e.g., a photo stored on a camera) are not entitled to Fifth Amendment protection because their creation was not "compelled" by the government as required under the text of the Amendment. However, the act of unlocking the device may have testimonial content of its own (e.g., it may demonstrate that a suspect had access to the device), which may trigger Fifth Amendment protection. While there are a handful of lower court rulings and a growing body of academic literature on this issue, there is only one appellate case applying the Fifth Amendment to compelled decryption and, as of the date of this report, no Supreme Court case law.

The other method is going to the company and requesting its assistance in unlocking a device, which prompts the second question: whether the All Writs Act—a federal statute that provides federal courts with residual authority to enforce its orders—can be interpreted broadly enough to cover compelled assistance on the part of the device and software manufacturer. This question is the subject of ongoing litigation—including government requests to access the iPhone used by the San Bernardino shooter—in various federal district courts and is likely to engender similar litigation in the future. This inquiry will largely hinge on whether the request would impose an unreasonable burden on the company and whether it would be consistent with the intent of Congress.

This report first provides background to the ongoing encryption debate, including a primer on encryption basics and an overview of Apple, Google, and Facebook's new encryption policies. Next, it will provide an overview of the Fifth Amendment right to be free from self-incrimination; survey the limited case law concerning the compelled disclosure of encrypted data; and apply this case law to help determine if and when the government may require such disclosures. The next section of the report will provide background on the All Writs Act; explore both Supreme Court and lower court case law, including a discussion of *United States v. New York Tel. Co.*; and apply this case law to the San Bernardino case and potential future requests by the government to access a locked device.

Contents

Tables

Contacts

Introduction

In September 2014, Apple announced that its new operating system, iOS 8, would encrypt most data stored on iPhones—such as iMessages, photos, calendars, and apps—by default.[1] This was after Apple, Inc. started to encrypt iMessage and iCloud data sent among Apple servers and users.[2] Apple asserts that under this new practice it can no longer comply with government requests for data off iDevices,[3] even with a valid probable cause warrant, as it no longer has access to the inputs needed to decrypt such data.[4] Google, maker of the popular Android operating system, announced a similar policy shortly thereafter.[5] Likewise, the popular Facebook-owned messaging system Whatsapp announced in November 2014 that it would offer end-to-end encryption on its service.[6]

This move by Apple, Google, and Facebook—three of the biggest technology companies in the United States—has renewed fears among government officials that technology is preventing law enforcement access to vital data, a phenomenon the government refers to as "going dark."[7] The government, speaking largely through Federal Bureau of Investigations (FBI) Director James Comey, has suggested that it does not want to ban encryption technology, but instead wants Silicon Valley companies to provide a technological way to obtain the content of data stored on a device for which it has legal authority to access.[8] However, many in the technology community, including American technology giants Apple, Google, and Facebook, and leading cryptologists have argued that it is not technologically feasible to permit the government access while continuing to secure user data from cyber threats.[9]

The current debate over encryption raises a wide range of important political, economic, and legal questions.[10] This report, however, explores two discrete and narrow legal questions that arise

---

[1] Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), *available at* https://www.washingtonpost.com/business/technologynology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

[2] Greg Kumparak, "Apple Explains Exactly How Secure iMessage Really Is," *TechnologyCrunch*, February 27, 2014, available online at: http://technologycrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/.

[3] iDevices include iPhones, iPads, and iPods.

[4] *See* Apple, iOS Security Whitepaper (Sept. 2015), *available at* https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[5] Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), *available at* https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[6] Andy Greenberg, *Whatsapp Just Switched on End-to-End Encryption For Hundreds of Millions of Users*, WIRED (Nov. 18, 2014, *available at* http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

[7] *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary*, 112th Cong. (Feb. 17, 2011).

[8] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing before the Senate Judiciary Committee*, 114th Cong. (July 8, 2015) (written statement by James Comey, Director, Federal Bureau of Investigations).

[9] Ellen Nakashima, *Tech Giants Don't Want Obama to Give Police Access to Encrypted Phone Data*, WASH. POST. (May 19, 2015), *available at* https://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html

[10] *See generally* CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by (name redacted); Steven Bucci, et al., *Encryption And Law Enforcement Special Access: The U.S. Should Err on the Side of Stronger Encryption*, THE HERITAGE FOUNDATION (Sept. 4, 2015), *available at* http://www.heritage.org/research/reports/2015/09/encryption-and-law-enforcement-special-access-the-us-should-err-on-the-side-of-stronger-encryption#_ftn1; Urs Grasser, *Don't Panic. Making Progress on the "Going Dark" Debate*, (continued...)

from the various ways the government has attempted to access data stored on a smartphone. One method has been to attempt to compel a user to either provide his password or decrypt the data contained in a device pursuant to valid legal process. This prompts the first question: whether the Fifth Amendment right against self-incrimination would bar such a request. Generally, documents created independent of a government request (say, a photo stored on a camera) are not entitled to Fifth Amendment protection because their creation was not "compelled" by the government as required under the text of the Amendment. However, the act of unlocking the device may have testimonial content of its own (e.g., it may demonstrate that a suspect had access to the device), which may trigger Fifth Amendment protection. While there are a handful of lower court rulings and a growing body of academic literature on this issue, there is only one appellate case applying the Fifth Amendment to compelled decryption, and, as of the date of this report, no Supreme Court case law.

The other method is going to the company and requesting its assistance in unlocking a device, which prompts the second question: whether the All Writs Act—a federal statute that provides federal courts with residual authority to enforce its orders—can be interpreted broadly enough to cover compelled assistance on the part of the device and software manufacturer. This question is the subject of ongoing litigation—including government requests to access the iPhone used by the San Bernardino shooter—in various federal district courts and is likely to engender similar litigation in the future. This inquiry will largely hinge on whether the request would impose an unreasonable burden on the company and whether it would be consistent with the intent of Congress.

This report first provides background to the ongoing encryption debate, including a primer on encryption basics and an overview of Apple and Android's new encryption policies. Next, it will provide an overview of the Fifth Amendment right to be free from self-incrimination; survey the limited case law concerning the compelled disclosure of encrypted data; and apply this case law to help determine if and when the government may require such disclosures. The next section of the report will provide a background to the All Writs Act; explore both Supreme Court and lower court case law, including a discussion of *United States v. New York Tel. Co.*; and apply this case law to the San Bernardino case and potential future requests by the government to access a locked device.

Background

Encryption Basics

Encryption is a process to secure information from unwanted access or use. Encryption uses the art of cryptography, which comes from the Greek words meaning "secret writing," to change information which can be read (plaintext) and make it so that it cannot be read (ciphertext). Decryption uses the same art of cryptography to change that ciphertext back to plaintext.[11]

Encryption can be applied to a variety of "plaintexts." Data is encrypted at a host to be sent *in transit* between a user and a web server with which they are communicating (e.g., for online

(...continued)

THE BERKMAN CENTER FOR THE INTERNET & SOCIETY, HARVARD UNIVERSITY (Feb. 1, 2016), *available at* https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[11] Matt Bishop, "Chapter 9: Basic Cryptography," in *Computer Security: Art and Science* (Boston, MA: Addison-Wesley, 2003), pp. 217-240.

shopping). Data can also be encrypted at a host for transit between two users chatting with each other (e.g., iMessage or Telegram). Data that is stored on a drive is considered data *at rest* and may also be encrypted. Data on a drive may be encrypted by putting the file into an encrypted container (e.g., a file folder) so that only the files in that container are encrypted while the rest of the drive is in plaintext. Or, the entire drive may be encrypted, known as full-disk encryption, so that all the data on the drive is encrypted (e.g., encrypting the user-accessible space on a cell phone so that the contents of that cell phone are encrypted).

There are five elements needed for encryption to work: (1) the encryption function;[12] (2) the decryption function; (3) the key; (4) the plain text; and (5) the ciphertext. In *symmetric* encryption, the key used to encrypt and decrypt a message is the same. In *asymmetric* encryption, the keys used to encrypt and decrypt the message are different.

Much of the recent debate over encryption stems from new security policies released by Apple, Google, and Facebook. In September 2014, Apple released a new iOS operating system for iPhones, iPads, and iPod touch devices.[13] As described in an Apple Whitepaper:

> On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.[14]

The Whitepaper explains that each device has a unique ID (UID) "fused" directly into the hardware during manufacturing. When users set up a device for the first time, they are asked to set up a passcode for unlocking the device. That passcode becomes "entangled" with the device's UID to create the encryption key, of which Apple does not retain a copy. Thus, even if the government produces a valid warrant, Apple has claimed it cannot decrypt the data. Perhaps the biggest change brought about by iOS 8 is that encryption now operates by *default*, rather than requiring the user to affirmatively turn on encryption.[15]

> The iPhone uses a distinctive implementation of encryption which requires both a user's input (passcode or password) and a device-specific unique identification number (UID) to create the encryption key. The key is not stored on the device itself. Instead, when the user enters their passcode or password, the system combines that input with the UID and if the device decrypts, it was correct.

Shortly after Apple announced its new encryption policy, Google, which had been offering encryption in its devices since at least 2011, announced that the newest iteration of its Android operating system, Lollipop 5.0, would also employ full disk encryption by default.[16] Similarly, the popular Facebook-owned messaging system Whatsapp announced in November 2014 that it would offer end-to-end encryption on its service.[17] One observer noted the unprecedented nature of this security upgrade: "The result is practically uncrackable encryption for hundreds of

[12] A "function" is the mathematical process in use.

[13] Timberg, *supra* note 5.

[14] Apple Whitepaper, supra note 4.

[15] Apple, Inc., "iOS Security," press release, September 15, 2015, https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[16] Timberg, *supra* note 5.

[17] Greenberg, *supra* note 6.

millions of phones and tablets that have Whatsapp installed—by some measures the world's largest-ever implementation of this standard of encryption in a messaging service."[18]

The concept of "practically uncrackable" encryption is important to the encryption and cryptosystems. Assuming someone has intercepted the "ciphertext," but does not have the key and wants the plaintext, they could use a brute-force attack. A brute-force attack, that is guessing every possible iteration of the key until the key is discovered, is a long process. Cryptosystems are built to require processors to run through multiple instructions and multiple iterations of those instructions before something is encrypted or decrypted. This natural time delay slows down guessers, and this is before additional delays (e.g., times between key entry, or temporary locks after incorrect attempts) are enforced. Additionally, some cryptosystems allow for many possible keys. For instance, a 4-digit cell phone passcode has 10,000 possible combinations (0000 to 9,999). However, a 6-character, alpha-numeric password (upper and lowercase letters and numbers) that also allows a user to choose among 10 special characters offers more than 139 billion combinations. The possible combinations increase exponentially when 8-, 10-, or 14-character passwords are used.

Because of the large amount of possibilities, those seeking to use a brute-force attack do not just start at zero and add characters until they get to the key. Instead, they would attack other elements of the system. For instance, knowing that users choose simple passwords, the attacker could start guessing likely options to greatly reduce the time to find the key.

Or, an attacker could circumvent a cryptosystem entirely and insert themselves between the user and the information they are accessing. Data can only be encrypted while at rest (stored) or in transit (being sent). Once a user accesses the data, or is otherwise processing the data, it is in plaintext. So, rather than try to compromise the cryptosystem, an attacker may determine that it is better to compromise the device that employs the cyrptosystem (e.g., the computer or the cell phone). If the attacker has malware on the device that allows them access to what the user is viewing on the device, they could see what the user intends to encrypt before the cryptosystem is activated. So while the encryption is still sound, it does not protect against other forms of attack.

"Going Dark" Debate

The phenomenon of technologies preventing government access to communications and other data—the so-called "going dark" problem—is not new to law enforcement agencies. The shift to new electronic forms of telephone communications in the latter part of the 20th century hindered the ability of the government to intercept voice communications, even when it had the appropriate legal process to do so. This resulted in the passage of the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[19] CALEA provides that a "telecommunication carrier shall ensure that its equipment, facilities, or services ... are capable of ... expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area[.]"[20] In other words, telecommunications companies had to build into their systems a way for law enforcement to access data for which it has lawful legal process to obtain. As telephone communications were shifting from traditional land lines to the Internet, the Federal Communications Commission (FCC) extended CALEA in 2005 to cover "facilities-based

[18] *Id.*

[19] Communications Assistance for Law Enforcement Act, P.L. 103-414, 108 Stat. 4279 (1994).

[20] 47 U.S.C. § 1002(a); *see* Table I, p. 23, for a more detailed survey of CALEA.

broadband Internet access providers and providers of interconnected voice over Internet Protocol (VoIP) service."[21] Notably, CALEA does not apply to "information services" and explicitly provides that telecommunication carriers are not "responsible for decrypting, 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."[22]

Although the Administration has actively engaged industry on this issue, FBI Director James Comey stated at an October 8, 2015, hearing before the Senate Committee on Homeland Security that the "Administration is not seeking legislation at this time" to require companies to enable the government to access encrypted data.[23] However, this was not the Administration's only word on the issue. Robert Litt, general counsel of the Office of Director of National Intelligence (ODNI), stated that although the then-current political environment may not be best suited to scaling back encryption, Congress might be more receptive to such legislation "in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."[24]

This was the reaction of European leaders in response to the two terrorist attacks in Paris in 2015. Following the 2015 terrorist attacks of French newspaper *Charlie Hebdo*, British Prime Minister David Cameron called for the outlaw of any app—such as WhatsApp or iMessage—that permitted the transmission of communications that could not be read by government officials.[25] More recently, the Investigatory Powers Bill was introduced in the UK following the November 16 Paris attacks; while not calling for a complete ban of encryption technology, the bill would require the companies to create the means to allow the government to read encrypted messages.[26]

While the Obama Administration has stated that, at least for the time being, it will not introduce anti-encryption legislation, it has continued to push American technology companies to come up with a technology workaround to this problem. In early January 2016, the Administration sent a delegation of high-level government officials to Silicon Valley to discuss, among other things, how technology companies could help the government thwart individuals from utilizing encryption technology to engage in terrorist activities.[27] However, some in the technology community, including Apple CEO Tim Cook, continue to state that providing government exceptional access would necessarily render a device more susceptible to cyber threats.[28]

---

[21] *See* Fed. Communications Commission, In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd. 14989 (Sept. 23, 2005).

[22] 47 U.S.C. § 1002(b).

[23] *Threats to the Homeland: Hearing Before the Senate Committee on Homeland Security*, 114th Cong. 3 (2015) (statement of James B. Comey, Director, Federal Bureau of Investigation).

[24] Ellen Nakashima & Andrea Peterson, *Obama Faces Growing Momentum to Support Widespread Encryption*, WASH. POST (Sept. 16, 2015), *available at* https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html?postshare=9031442410909976.

[25] Katy Barnato, *Whatsapp, iMessage Face Ban in Terror Crackdown*, CNBC (Jan. 13, 2015), *available at* http://www.cnbc.com/2015/01/13/whatsapp-imessage-face-ban-in-terror-crackdown.html.

[26] Andrew Griffin, Investigatory Powers Bill Could Allow Government to Ban End-to-End Encryption, Technology Powering iMessage and Whatsapp, INDEPENDENT (Nov. 7, 2015), available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-bill-could-allow-government-to-ban-end-to-end-encryption-technology-powering-a6725311.html

[27] Jenna McLaughlin, *White House Raises Encryption Threat in Silicon Valley Summit*, THE INTERCEPT (Jan. 8, 2016), *available at* https://theintercept.com/2016/01/08/white-house-raises-encryption-threat-in-silicon-valley-summit/.

[28] Jenna McLaughlin, *Apple's Tim Cook Lashes Out at White House Officials for Being Wishy-Washy on Encryption*, THE INTERCEPT (Jan. 12, 2016), *available at* https://theintercept.com/2016/01/12/apples-tim-cook-lashes-out-at-white-

(continued...)

Likewise, several prominent computer scientists and technologists noted in a July 2015 report, *Keys Under Doormats*, that "law enforcement demands for exceptional access to private communications and data shows that such access will open the doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend."[29]

Undoubtedly, if Congress fails to enact legislation providing government access to encrypted data, law enforcement will face situations in which it cannot access encrypted data. One possible response would be to mandate the user to either provide his password, or decrypt the data contained in a device. However, mandating that an individual provide his passcode or decrypted data could implicate, among other possible legal protections, his Fifth Amendment right to be free from self-incrimination.

Compelled Decryption and the Right Against Self-Incrimination

Fifth Amendment Framework

The Fifth Amendment to the United States Constitution provides, in relevant part, that "[n]o person ... shall be compelled in any criminal case to be a witness against himself."[30] Known in common parlance as "pleading the Fifth," this right against self-incrimination protects a defendant from the "cruel trilemma" of offering incriminating evidence against oneself and risking a criminal conviction; lying to government officials and risking perjury; or keeping silent and risking contempt of court.[31] At one point, the Fifth Amendment was read to protect the compelled disclosure of *any* incriminating papers.[32] However, later cases held that a "person may be required to produce specific documents even though they contain incriminating assertions of fact" so long as the *creation* of the document was not compelled by the government.[33] Thus, under the modern interpretation of the Fifth Amendment, the following elements must be met for a Fifth Amendment privilege to be successfully asserted: (1) the statement must have been *compelled* by the government, (2) it must be *incriminating*,[34] and (3) it must be *testimonial*. The first two elements of a self-incrimination claim—compulsion and the incriminating nature of the documents—are rarely in question. Rather, most cases in this area concern whether a given statement should be considered "testimonial."

(...continued)

house-officials-for-being-wishy-washy-on-encryption/.

[29] Harold Abelson, et. al, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, MASS. INST. TECH. CYBERSECURITY AND INTERNET POLICY RESEARCH INITIATIVE (2015), *available at* https://www.schneier.com/cryptography/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

[30] U.S. CONST. amend V.

[31] Doe v. United States, 487 U.S. 201, 212 (1988) (quoting Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52, 84 (1988)).

[32] Boyd v. United States, 116 U.S. 616, 634-35 (1886).

[33] United States v. Hubbell, 530 U.S. 27, 35-36 (2000).

[34] Doe v. United States, 487 U.S. 201, 208 n.6 (1988) (noting that "'compelled testimony' need not itself be incriminating if it would lead to the discovery of incriminating evidence").

"Testimonial" and the Act of Production Doctrine

The Supreme Court has held that a statement is "testimonial" when the government compels the individual to use the contents of his own mind to explicitly or implicitly communicate some statement of fact.[35] The Fifth Amendment does not, however, protect documents existing before the government's request, as any incriminating statements contained in the document could not be said to be "compelled" by the government, for such a request came after the statement was uttered.[36] For example, even if an individual has an incriminating item on his smartphone—say, a text message or photo that links the user to a crime—that person cannot claim a Fifth Amendment privilege from handing it over to the government on the basis that the document is incriminating. While the content of the documents might not trigger a Fifth Amendment privilege, the *act* of producing that record may have testimonial implications of its own, meaning the *act* could communicate a statement of fact to the government.[37] This is known as the "act of production" doctrine.

The act of production doctrine originated in the 1976 case *Fisher v. United States* in which the Internal Revenue Service (IRS) had requested certain tax documents from the lawyers of two taxpayers. The Court noted that "the Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate a taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications."[38] Because the documents were created voluntarily, the Court held that they could not be considered "compelled testimonial evidence."[39] Accordingly, the taxpayer "could not avoid compliance with the subpoena merely by asserting that the item of evidence which he is required to produce contains incriminating evidence, whether his own or that of someone else."[40] But, the Court observed that "[t]he act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer."[41] The Court noted, however, that implicitly admitting the "existence and possession" of the papers by complying with the subpoena—the only possible testimonial aspects of disclosing these documents—should not be considered testimonial when the "existence and location" of the papers were a "foregone conclusion."[42] Put another way, because the IRS already knew the existence and location of the documents, the taxpayer's disclosure of those documents would not implicitly relay any incriminating fact to the government. This is known as the "foregone conclusion" exception to the act of production doctrine.

Foregone Conclusion Exception

The "foregone conclusion" exception to the act of production doctrine was elaborated on in the 2000 case *United States v. Hubbell*, which concerned the investigation of potential federal

[35] *Doe*, 487 U.S. at at 210.

[36] Fisher v. United States, 425 U.S. 391 (1976).

[37] *See* United States v. Hubbell, 530 U.S. 27, 40 (2000) ("The 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents.").

[38] Fisher v. United States, 425 U.S. 391, 409 (1976).

[39] *Id.* at 409-10.

[40] *Id.* at 409-10.

[41] *Id.* at 410.

[42] *Id.* at 411.

criminal violations relating to the Whitewater Development Corporation.[43] There, the Independent Counsel served the defendant with a subpoena requesting 11 categories of documents. Appearing before the grand jury, the defendant asserted his Fifth Amendment privilege against self-incrimination and refused to state whether he was in control or possession of any of the documents requested in the subpoena. The prosecutor then produced an order, previously obtained from the district court pursuant to 18 U.S.C. § 6003, a federal immunity statute, directing the defendant to respond to the subpoena and granting him immunity "to the extent allowed by law."[44] The defendant produced 13,120 pages of documents, which ultimately provided the Independent Counsel sufficient information to secure an indictment. The district court dismissed the indictment because all of the evidence that would have been offered against the defendant at trial derived either directly or indirectly from the testimonial aspects of his immunized act of producing those documents.

On appeal, the government claimed that the act of producing ordinary business records was insufficiently "testimonial" because the existence and location of the documents sought was a "foregone conclusion."[45] Rejecting this argument, the Court noted that government did not have "prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents" produced by the defendant.[46] It was *not* enough, the Court continued, that a businessperson "will always possess business and tax records."[47] Moreover, the Court found that it would be "unquestionably necessary for [the defendant] to make extensive use of the 'contents of his own mind' in identifying the hundreds of documents responsive to the request in the subpoena."[48] Ultimately, the Court concluded the act of producing these records was testimonial, at least with respect to the existence and location of the documents.

After *Hubbell* and *Fisher*, determining whether an act of production is testimonial appears to depend largely on "the government's knowledge regarding the documents before they are produced."[49] In *Fisher*, the government knew of the existence of the tax documents in question when it made its demand. In *Hubbell*, however, the government could not demonstrate its knowledge of the existence and location of the documents it sought.[50] The government need not "have actual knowledge of the existence of each and every responsive document."[51] The majority of circuit courts have held, nonetheless, that the government must establish its knowledge of the existence, possession, and authenticity of the requested documents with "reasonable particularity."[52] "It is the government's knowledge of the existence and possession of the *actual documents*," the Ninth Circuit has noted, and "not the information contained therein, that is central to the foregone conclusion inquiry."[53]

---

[43] *Hubbell*, 530 U.S. at 29.

[44] *Id.* at 31.

[45] *Id.* at 44.

[46] *Id.* at 45.

[47] *Id.* at 45.

[48] *Id.* at 43.

[49] *See* United States v. Ponds, 454 F.3d 313, 320 (D.C. Cir. 2006).

[50] *Hubbell*, 530 U.S. at 44-45.

[51] *In re* Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).

[52] *See Ponds*, 454 F.3d at 321-22; *In re* Grand Jury Subpoena, 383 F.3d at 910; *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); *In re* Grand Jury Subpoena Duces Tecum, 1 F.3d 87 (2d Cir. 1993).

[53] In re *Grand Jury Subpoena*, 383 F.3d at 910 (emphasis added).

Physical Acts

In addition to the foregone conclusion exception, the Supreme Court has held that certain *physical* acts are not considered testimonial for purposes of the Fifth Amendment. For instance, giving a blood sample[54] or providing a voice exemplar[55] have not been considered testimonial as they do not require the suspect "to disclose any knowledge he might have," or "to speak his guilt."[56] Put another way, it is "extortion of information from the accused; the attempt to force him to disclose the contents of his own mind, that implicates the Self–Incrimination Clause."[57]

Compelled Decryption Case Law

The Supreme Court has yet to address the issue of compelling an individual to disclose a passcode or decrypt data, but has provided some insight in dicta in how it might rule on this issue. The lower federal courts and some state courts are beginning to see more cases as law enforcement officials are increasingly encountering encrypted data.

Supreme Court

While the Supreme Court has yet to opine on how the Fifth Amendment should apply to the compelled production of a passcode, it has discussed the production of combination number and keys to traditional real-world safes. During the current decryption debate, many have attempted to employ this key/combo metaphor to access smartphones. This key/combo distinction appears to have originated in a dissent by Justice John Paul Stevens in the 1988 case *Doe v. United States*.[58] There, Justice Stevens noted that while a suspect "may in some cases be forced to surrender a key to a strongbox containing incriminating documents," he cannot be "compelled to reveal the combination to his wall safe—by word or deed."[59] His argument was premised on the idea that requiring someone to give up a safe combination required him to "use his mind to assist the prosecution in convicting him of a crime," whereas giving up a safe key would not.[60] The *Doe* majority appeared to accept this dichotomy when noting in a footnote that "we do not disagree with the dissent that '[t]he expression of the contents of an individual's mind' is testimonial communication for the purposes of the Fifth Amendment."[61] This dichotomy was later affirmed in *Hubbell*.[62]

Eleventh Circuit

Beyond the Supreme Court, the only circuit court to have addressed the issue of compelled decryption arose in a 2012 Eleventh Circuit Court of Appeals case addressing government access to data on an encrypted hard drive.[63] There, the government obtained a warrant to search the hotel

[54] Schmerber v. California, 384 U.S. 757, 764-65 (1966).

[55] United States v. Dionisio, 410 U.S. 1, 7 (1973).

[56] Does v. United States, 487 U.S. 201, 211 (1988).

[57] *Id.* at 211.

[58] Does v. United States, 487 U.S. 201, 211 (1988).

[59] *Id.* at 219 (Stevens, J., dissenting).

[60] *Id.*

[61] *Id.* at 210 n.9.

[62] United States v. Hubbell, 530 U.S. 27, 43 (2000) (citing *Doe*, 487 U.S. at 209, n.9)).

[63] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2004).

room and any electronic devices found on a John Doe, who was suspected of sharing explicit material of children on the Internet.[64] Because forensic examiners from the FBI were unable to access certain portions of the drive, a grand jury subpoena was issued to require Doe to produce the unencrypted contents of the hard drives. Upon Doe's claim that compliance with the subpoena would violate his Fifth Amendment privilege against self-incrimination, the government sought and received act-of-production immunity for such production. Although forensic examiners believed that there was encrypted information contained on the hard drive, because the drive was encrypted, an expert for the government could not determine what data was on the drive.

The government admitted that the material requested was compelled and incriminating; thus, the only question before the Eleventh Circuit was whether Doe's act of producing the unencrypted data would be testimonial under the Fifth Amendment. The court noted that this question ultimately turned on whether the government could show with "'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a 'foregone conclusion.'"[65] The court concluded that the testimony was not a "foregone conclusion" and that Doe had a valid Fifth Amendment privilege: "Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives."[66]

District Courts

In addition to the Eleventh Circuit, several district courts have also addressed the compelled decryption issue. Like the Eleventh Circuit case, these cases largely turned on the extent of the government's knowledge concerning the documents.

In the 2007 case *In re Boucher*, border patrol agents stopped Sebastien Boucher and his father as they attempted to cross the Canadian border into the United States.[67] One of the officers found a laptop computer in the backseat. Without needing to enter a password, he was able to access approximately 40,000 files on the laptop, some of which appeared to contain pornographic images. An ICE special agent then investigated further, finding thousands of images of pornography, including one file labeled in a way to suggest it as child pornography, but he was unable to open. The laptop was later powered down and could not be accessed again due to an encryption program installed on the laptop. Secret Service agents estimated that it would take years to crack the password using a brute force attack. To gain access to the data, the grand jury issued a subpoena requesting that Boucher provide "all documents, whether in electronic or paper form, reflecting any passwords" associated with the seized hard drives. Boucher moved to quash the subpoena on the grounds that it violated his Fifth Amendment right to self-incrimination.

The government conceded that Boucher could not be compelled to disclose his password as this would be inherently testimonial. Instead, the government asked that Boucher be compelled to enter his passcode. In granting his motion to quash the subpoena, the court noted that entering a

[64] *Id.* at 1339.

[65] *Id.* at 1346.

[66] *Id.*

[67] *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. 2007).

password implicitly communicates facts: "By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on [the hard drive]."[68]

The government later narrowed its request to requiring Boucher to produce an unencrypted version of the hard drive.[69] The magistrate judge determined that the "foregone conclusion" doctrine did not apply because the government had not viewed most of the files on the drive. The district court judge reversed this decision, however, noting that the government need not be aware of the specific contents of the files, but instead must be able to demonstrate with "reasonable particularity that it knows of the existence and location of subpoenaed documents."[70] Because the government had already viewed some of the files on the hard drive, and ascertained that they might contain child pornography, providing the government access to the hard drive "add[ed] little or nothing to the sum total of the Government's information."[71]

Like the government's first request in the *Boucher* case, the government in *United States v. Kirschner* requested that the defendant produce the passcode to his encrypted computers.[72] Relying on the Supreme Court's safe key/combination dichotomy from *Doe*, the district court found that revealing a passcode was the equivalent of revealing a safe combination, which would impermissibly require the defendant to reveal the contents of his mind.[73]

In *United States v. Fricosu*, the District Court for the District of Colorado rejected a Fifth Amendment claim made by a defendant who was ordered to produce the unencrypted contents of a hard drive found during the execution of a search warrant.[74] With little explanation, the court noted that because the government already had possession of the hard drive, "there is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production."[75] Moreover, the court found that the government had sufficiently demonstrated that the hard drive belonged to the defendant through independent evidence.[76]

Finally, in *In re Decryption of a Seized Storage System*, the District Court of Wisconsin initially rejected the government's request to compel the defendant to decrypt certain hard drives found in his home that contained files with names that were indicative of child pornography.[77] The court reasoned that although the government had proven that the drives actually contained data and that the defendant was in possession of the drive, it had not demonstrated he had "access to and control over the encrypted storage devices."[78] However, upon review, the court granted the government's renewed request to compel production of decrypted data as the government had offered additional evidence to demonstrate that the defendant had control and access to the drives,

[68] *Id.* at *3.

[69] *See In re* Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. 2009).

[70] *Id.* at *3.

[71] *Id.*

[72] United States v. Kirschner, 823 F. Supp. 2d 665, 666 (E.D. Mich. 2010).

[73] *Id.* at 669.

[74] United States v. Fricosu, 841 F. Supp. 2d 1232, 1234 (D. Colo. 2012).

[75] *Id.* at 1237.

[76] *Id.*

[77] *In re* Decryption of a Seized Storage System, No. 13-449 (D. Wis. April 19, 2013).

[78] *Id.* at 3.

such as showing that drive contained personal financial information and photographs of the defendant.[79]

State Courts

In addition to the federal courts, several state courts have addressed the scope of the right against self-incrimination in the context of encrypted data. In *Commonwealth v. Baust*, Virginia's Second Circuit Court addressed whether the government could force an individual to provide his smartphone passcode.[80] Relying on the safe key/combination dichotomy from *Doe*, the Virginia court held that revealing the passcode was like revealing a combination and therefore was considered testimonial.[81] However, the court also held that requiring the defendant to enter his fingerprint into the device would not be considered testimonial as this did "not require the witness to divulge anything from his mental processes."[82] Similarly, the Supreme Judicial Court of Massachusetts assessed whether requiring a defendant to enter his passcode in order to access an encrypted hard drive should be considered testimonial for purposes of his self-incrimination claim.[83] The Massachusetts High Court noted that the "act of complying with the government's demand could constitute testimonial communication where it is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence."[84] Nonetheless, the court rejected the defendant's claim, as he had already admitted to law enforcement officials that he had encrypted the device and had access to it. In doing this, the government did not need to rely on his production of the passcode to prove ownership or control of the laptop—depriving such production of any testimonial import.

Application of Fifth Amendment Analytical Framework to Compelled Disclosure

Applying the Fifth Amendment analytical framework and the recent federal court cases concerning compelled disclosure of electronic data, access can be broken down into at least three discrete government requests: (1) compelled disclosure of a user's passcode; (2) compelled entry of biometric password; and (3) compelled production of encrypted data.

Compelled Disclosure of Passcode

Based on the limited case law from the lower federal courts and dicta from the Supreme Court, there is a strong argument that the Fifth Amendment would bar the government from compelling an individual to disclose his passcode to the government. First, looking to the limited Supreme Court pronouncements on this subject, providing a passcode generally seems more akin to providing a safe combination, which the Court said in *Doe* would be considered testimonial,[85] and less like handing over a safe key, which would not be considered testimonial. This approach was applied in the encryption case *Kirschner*, in which the district court observed that "forcing the

[79] *In re* Decryption of a Seized Storage System, No. 13-449 (D. Wis. May 21, 2013).

[80] Commonwealth v. Baust, No. 14-1439 (Va. 2d Jud. Cir. 2014).

[81] *Id.* at 4-5.

[82] *Id.* at 5.

[83] Commonwealth v. Gelfgatt, 468 Mass. 512, 521 (2014).

[84] *Id.* at 521.

[85] Doe v. United States, 487 U.S. 201, 210 n.9 (1988).

Defendant to reveal the password for his computer communicates that factual assertion to the government, and thus, is testimonial—it requires Defendant to communicate 'knowledge,' unlike the production of a handwriting sample or voice exemplar."[86] Put another way, the target would be "forced to engage in cognition for the benefit of the state and to turn over the results of that mental process."[87] Likewise, the government conceded in *In re Boucher* that disclosing a passcode from the defendant would be considered testimonial.[88] It appears that these courts are treating the disclosure of a passcode as *inherently* testimonial, as it will always require the target to reveal something from his mind when disclosing the passcode.

Moreover, one leading Fifth Amendment theory supports this result. Several scholars posit that "testimonial" under the Fifth Amendment means "substantive cognition—the product of cognition that results in holding or asserting propositions with truth-value."[89] Breaking down this rule, they note that *cognition* "involves the acquisition, storage, retrieval, and use of knowledge."[90] The "paradigmatic example" of Fifth Amendment protection, they offer, is "the retrieval of information from memory in response to a question."[91] Recalling a passcode and relaying that information to the government would seem to squarely fit this description. First, it requires mental cognition on the part of the user—the retrieval of knowledge from one's mind. Second, such retrieval results in the assertion of a proposition with true-value—that is, that the passcode provided can either be correct or incorrect.

At least one author has argued that a statement is only testimonial when it involves "substantial cognitive content" and that providing a passcode does not rise to the level of substantial content.[92] However, even this author notes that the "[c]ourts have not yet framed the issue this way,"[93] and it is not at all clear how a court would make such a determination between substantial and insubstantial cognitive content.

Compelled Entry of Biometric Passcode

In addition to using alphanumeric passwords, many smartphones can be locked using either biometric data or some other physical act. Depending on the specific method required to open such a phone, employing such methods could alter the self-incrimination analysis.

As technology advances, smartphone manufacturers have developed new ways to open and lock their devices. Beginning with the iPhone 5s, Apple smartphones employ Touch ID, a system that can unlock a device using the user's fingerprint.[94] Similarly, various smartphones that employ the

[86] United States v. Kirschner, 823 F. Supp. 2d 665, 669 (2010).

[87] Caren Myers Morrison, *Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment*, 65 ARK. L. REV. 133, 147 (2012).

[88] *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. 2007).

[89] Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and its Future Predicted*, J. CRIM. L. & CRIMINOLOGY (2004).

[90] *Id.* at 267.

[91] *Id.* at 268.

[92] Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 N.W. L. REV. 1131 (2015).

[93] *Id.* at 1135.

[94] *See* iOS Security, *supra* note 4, at 7.

Windows operating system use iris scans to access the device.[95] And Android devices come equipped with Face Unlock, which uses facial recognition technology to unlock a device.[96]

If a court were to apply the key/combination distinction, it appears that the government could request a defendant to enter his biometric information into his smartphone to unlock it.[97] First, as noted by a Virginia state court addressing encryption,[98] a fingerprint is much more like a key than a combination, which the Supreme Court has said, albeit in dicta, is non-testimonial. However, unlike a key, providing biometric information that successfully decrypts a device suggests the target previously interacted with the device, which might indicate ownership or control. Second, when a user is asked to enter his fingerprint into a device, he is not asked to reveal the contents of his mind or reveal any information to the government. This makes a command to enter biometric information more like a command to give a voice exemplar or blood sample, which is not considered testimonial,[99] rather than a command to reveal knowledge to the government.

Compelled Production of Decrypted Data

If the government is not able to compel the production of a device's passcode, or if the device is not enabled with a biometric passcode, the other alternative is for the government to request the user to produce the decrypted data. Whether accessing such data would be considered testimonial for purposes of the Fifth Amendment will largely turn on application of the "foregone conclusion" doctrine—that is, whether knowledge of the testimonial content of providing the decrypted data would be a "foregone conclusion."

As noted by the Supreme Court in *Fisher* and *Hubbell*, a statement is deprived of testimonial content if knowledge of the existence and location of the documents were a "foregone conclusion."[100] As elaborated by the circuit courts, the government must be able to establish its prior knowledge of the existence, possession, and authenticity of the requested documents with "reasonable particularity."[101] What is not certain from the case law is whether the government would have to prove the existence and possession of the *smartphone* itself or the *files* contained on the device. Some scholars have argued that it is the device that the government must have knowledge of.[102] Under this theory, in many cases it would not be difficult for the government to

---

[95] Mauro Huculak, *How the Iris Scanner on the Lumia 950 and 950 XL Works*, WINDOWS CENTRAL (Oct. 8, 2015), *available at* http://www.windowscentral.com/how-iris-scanner-lumia-950-and-950-xl-works.

[96] Gary Muzo, *How to Set Up Face Unlock on Your Android Phone*, ANDROID CENTRAL (July 24, 2012), *available at* http://www.androidcentral.com/how-set-face-unlock-your-htc-one-x-or-evo-4g-lte.

[97] *See* Paul Roseinzweig, *Pass Phrases Protected; Fingerprints Not—Curiouser and Curiouser*, LAWFARE (Nov. 7, 2014) (noting that requiring entry of biometric passcode was "right doctrinal answer"), *available at* https://www.lawfareblog.com/pass-phrases-protected-fingerprints-not-curiouser-and-curiouser.

[98] Commonwealth v. Baust, No. 14-1439 (Va. 2d Jud. Cir. 2014).

[99] *See* "Physical Acts," *infra* pp. 9.

[100] *See* United States v. Hubbell, 530 U.S. 27, 44 (2000); Fisher v. United States, 425 U.S. 391, 411 (1976).

[101] *See Ponds*, 454 F.3d at 321-22; *In re* Grand Jury Subpoena, 383 F.3d at 910; *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); *In re* Grand Jury Subpoena Duces Tecum, 1 F.3d 87 (2d Cir. 1993).

[102] Orin Kerr, *Apple's Dangerous Game*, WASH. POST (Sept. 19, 2014), *available at* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/ ("Because people must know their passcodes to use their own phones, the testimonial aspect of decrypting a person's own phone—admitting that the phone belongs to them and they know the password—will be a 'foregone conclusion' whenever the government can show that the phone belongs to that person. If the phone's in the suspect's hand or in his pocket when the government finds it, that's not going to be hard to show."); Dan Terzian, *Force Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 N.W. L. REV. 56, 58 (2014) ("Where the government can 'independently confirm' the testimonial (continued...)

prove ownership and control if it can prove the suspect possessed the device at the time of seizure.[103] These scholars argue that the government's independent demonstration that the suspect owned or controlled the device is sufficient to deprive the act of producing the decrypted data of any testimonial content. However, even if the government can prove the suspect owned and possessed the device, this does not mean that the government can prove the defendant had *access* to the device or knew how to decrypt the data stored on it. In *In re Grand Jury Subpoena*, the Eleventh Circuit required the government to prove not only knowledge of the files contained on the encrypted hard drive, but also that the defendant had access to those files and the ability to decrypt. There are certainly instances where someone may own a smartphone—for instance, where a parent purchases a smartphone for a child—but may not have access to the device (when the child sets the password).

Moreover, some of the recent encryption cases focus not on whether the government already knew the suspect possessed the *device*, but rather whether the government could prove the existence and location of *specific files* on the hard drive. In *Hubbell*, the court noted that it was the existence and authenticity of the *documents* that was the crux of the inquiry:

> While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent.[104]

Likewise, in *In re Grand Jury Subpoena*, the court rejected the government's access to files stored on an encrypted hard drive as the government "failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the hard drives, the [the defendant] had access to those files, or that he is capable of decrypting the files."[105] The panel noted that although "the government physically possesses the media devices, ... it does not know what, if anything, is held on the encrypted drives."[106] To the contrary, in *Boucher*, the court compelled the defendant to produce the decrypted files, as the government had a prior opportunity to learn the existence and location of some of the incriminating files on the hard drive; thus, knowledge of their existence was a foregone conclusion.[107]

If a court treats the *device* as the relevant scope of inquiry—that is, whether the government can independently prove the defendant owned and controlled the device—the standard may not be difficult for the government to meet in many cases, especially where the device is found on the person of the suspect. However, if a reviewing court were to treat the *data* contained on the device as the relevant scope of inquiry, the government would have to prove it knew of the existence and location of the specific documents it seeks, preventing the government from going on a fishing expedition for incriminating evidence. It appears likely the government would be foreclosed from making the argument that it already knows the existence and location of documents on a smartphone—say, for example, texts, emails, photos, and calendars—based on

---

(...continued)

component (here, computer ownership) through specific 'prior knowledge' that goes beyond mere suspicion, it can still compel production.").

[103] Kerr, *supra* note 102.

[104] *Hubbell*, 530 U.S. at 45.

[105] In re *Grand Jury Subpoena*, 670 F.3d at 1349.

[106] *Id.* at 1347.

[107] In re *Boucher*, 2009 WL 424718, at *3.

the simple fact that smartphones generally hold such information. This argument was rejected in *Hubbell*, in which the court observed that it was not enough that a businessperson always possesses business and tax records.[108] Likewise, the Eleventh Circuit rejected an argument that the government already knows of the existence and location of the files simply because the data is in the government's *physical* possession (that is, that the information is stored on the device's physical memory).[109] The Eleventh Circuit noted that "[i]t is not enough for the Government to argue that the encrypted drives are *capable* of storing vast amounts of data, some of which may be incriminating."[110] Moreover, it noted that "categorical requests for documents the Government anticipates are likely to exist will not suffice."[111] Just how much particularity would be required if this latter approach is adopted would likely be resolved through litigation.

Compelled Assistance and the All Writs Act

In addition to requesting a smartphone *user* to provide his passcode or decrypted contents, the government has also sought assistance of *device manufacturers* in accessing a locked device.[112] The most prominent example is the cell phone used by one of the terrorists who caused the death of 14 people and injured 22 others in San Bernardino, CA, on December 2, 2015. Primarily, the government has utilized the All Writs Act to seek such relief. The legal question presented by such requests is 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 Apple's wishes.[113] The answer will likely depend on whether this mandate would pose an "unreasonable burden" on Apple and whether it is consistent with the intent of Congress.

Background

The All Writs Act, enacted as part of the Judiciary Act of 1789,[114] 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."[115] 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."[116] In other words, the act performs a gap-filling function that can be used "to effectuate and prevent the frustration of orders" of the court.[117] "[U]nless appropriately confined by Congress," the Court has noted, "a federal court may avail itself of all auxiliary writs" needed "to achieve the ends of justice entrusted to it."[118] However, and this is an important caveat, the Court has warned that the All Writs Act "does not authorize [courts] to issue ad hoc writs whenever compliance

[108] *Hubbell*, 530 U.S. at 45.

[109] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

[110] *Id.* at 1347.

[111] *Id.*

[112] For a brief overview of court-ordered access to smartphones, see CRS Report R44396, *Court-Ordered Access to Smart Phones: In Brief*, by (name redacted), (name redacted), and (name redacted) .

[113] 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.

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

[115] 28 U.S.C. § 1651(a).

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

[117] United States v. New York Tel. Co., 434 U.S. 159, 172 (1977).

[118] *Id.* at 172-73 (quoting Adams v. United States ex rel. McCann, 317 U.S. 269, 273 (1942)).

with the statutory procedures appears inconvenient or less appropriate."[119] Although the All Writs Act was penned 226 years ago,[120] 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*.[121]

All Writs Act and the Supreme Court: *United States v. New York Tel. Co.*

With minimal Supreme Court cases on point, most of the guidance in the San Bernardino case as to the All Writs Act questions derives from *New York Tel. Co.* In that case, a United States district court issued an order authorizing FBI agents to install and use two pen registers—a device for recording the outgoing numbers dialed on a telephone, but not the contents of the call—with respect to two telephone lines connected with a suspected gambling hall.[122] The agents had sufficiently demonstrated probable cause to engage in the search. The order directed the New York Telephone Co. to furnish the FBI "all information, facilities and technology assistance" necessary to employ the pen registers unobtrusively.[123] The FBI argued that it needed the company's assistance to successfully engage in the surveillance.[124]

The telephone company refused to comply with the court's order. The company informed the government agents of the location of the "appearance"—the spot where the specific telephone line emerges from the sealed telephone cable—to help the FBI install its own wires, but the company refused to provide a "leased line" to the FBI, a process the FBI argued was needed to ensure the unobtrusiveness of the surveillance device. The district court granted the government's order compelling the telephone company's assistance, but the Second Circuit Court of Appeals reversed. It found "that the most important factor weighing against the propriety of the order is that without Congressional authority, such an order could establish a most undesirable, if not dangerous and unwise, precedent for the authority of federal courts to impress unwilling aid on private third parties."[125] Further, the Second Circuit appeared to accept the company's argument

---

[119] Pennsylvania Bureau of Correction, 474 U.S. at 43.

[120] One might argue that because the All Writs Act was enacted 226 years ago it is ill-suited to address issues arising from government access to evidence in the digital era. Two things should be considered when assessing this assertion. First, courts apply old laws all the time. The Bill of Rights, including the Fourth Amendment, was ratified in 1791, two years after the All Writs Act was enacted, and the text has not changed since. The Fourth Amendment in particular is applied to ever-changing factual scenarios, including those involving new technologies, on a daily basis. Second, the All Writs Act, like other grants of judicial authority, was written broadly enough—"all writs necessary and *appropriate*"—to allow it sufficient flexibility to be applied to changing technological situations.

[121] United States v. New York Tel. Co., 434 U.S. 159 (1977).

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

> Pen registers do not "intercept" because they do not acquire the "contents" of communications, as that term is defined by 18 U.S.C. § 2510(8). Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Id. at 167.

[123] *Id.* at 161.

[124] *Id.* at 162-63.

[125] Application of U. S. in Matter of Order Authorizing Use of a Pen Register, 538 F.2d 956, 962 (2d Cir. 1976) *rev'd sub nom.* United States v. New York Tel. Co., 434 U.S. 159 (1977).

that a major reason for its opposition to the order was the "danger of indiscriminate invasions of privacy."[126]

In an opinion by Justice Byron White, the Supreme Court reversed the Second Circuit, rejecting both the innocent third party and privacy arguments.[127] As to the former, Justice White 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."[128] As to the latter, the Court noted the minimal privacy invasion caused through the use of a pen register, which again does not intercept the content of the communications, and the fact the government had obtained lawful process to install the device.[129]

While the Court ultimately held that the All Writs Act required the telephone company to comply with the court order, Justice White's opinion was not precise when articulating the appropriate test to be applied in future cases. After rejecting the view of the Second Circuit that third-party companies could not be forced to assist the government in surveilling a customer, Justice White noted that "[t]he power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed. We conclude, however, that the order issued here against respondent was clearly authorized by the All Writs Act and was consistent with the intent of Congress."[130] This passage suggests at least two inquiries in an All Writs Act analysis. First, whether the compelled assistance would pose an "unreasonable burden" on the company, and second, whether the order would be "consistent with the intent of Congress."[131] Additionally, the Court provided a third inquiry: whether the private party's assistance is *necessary* to carry out the court's order.[132]

> Under *New York Tel. Co.* and subsequent case law, a reviewing court should make three broad inquiries when faced with a government request for compelled assistance under the All Writs Act:
>
> Whether the command would be an "unreasonable burden" on the company forced to comply
>
> Whether such order would be "consistent with the intent of Congress"
>
> Whether the company's assistance is "essential to the fulfillment of the [government's] purpose"

As to the **burden** on the company, the Court applied a seemingly *non*-exhaustive list of factors. Some of the factors focused on the actual burden on the company in complying with the order. The Court observed, for example, that the order required only "meager assistance" from the company; the order was in no way "burdensome"; compliance with the order required "minimal effort" by the company; the company regularly employed such devices for billing purposes; and the order provided the company be fully reimbursed for its efforts.[133] An additional component of the unreasonable burden inquiry appears to be the level of the company's perception of the request. Justice White noted that the use of the pen register was not "offensive" to the company; the company had not proffered a "substantial interest in not providing assistance"; and the company

[126] *Id.*

[127] United States v. New York Tel. Co., 434 U.S. 159 (1977).

[128] *Id.* at 174.

[129] *Id.* at 168 ("It is clear that Congress did not view pen registers as posing a threat to privacy of the same dimension as the interception of oral communications and did not intend to impose Title III restrictions upon their use.").

[130] *Id.* at 172.

[131] *Id.* at 172.

[132] *Id.* at 175.

[133] *Id.* at 174-75.

had previously promised to provide the FBI instructions on how to install its own pen register.[134] Finally, the Court suggested that "disruptions to the company's operations" should be taken into consideration in an All Writs Act analysis.

Next, the Court inquired whether this application of the All Writs Act was **consistent with the intent of Congress**. Justice White observed that "Congress clearly intended to permit the use of pen registers by federal law enforcement officials" and without the assistance of the telephone companies "these devices simply cannot be effectively employed."[135] He continued:

> We are convinced that to prohibit the order challenged here would frustrate the clear indication by Congress that the pen register is a permissible law enforcement tool by enabling a public utility to thwart a judicial determination that its use is required to apprehend and prosecute successfully those employing the utility's facilities to conduct a criminal venture.[136]

Lastly, the Court assessed whether the company's assistance was **"essential to the fulfillment of the [government's] purpose,"** noting that "without the Company's assistance there is no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished"; this help was "essential to the fulfillment of the purpose—to learn the identities of those connected with the gambling operation—for which the pen register order had been issued."[137]

Lower Courts

Although it was handed down almost 40 years ago, there are relatively few cases applying the All Writs Act test articulated in *New York Tel. Co.*, and even fewer applying these principles to technological impediments to surveillance. However, a few lower courts have applied the All Writs Act to various requests from law enforcement for technology assistance in carrying out a warrant or order to engage in surveillance of some kind, including at least two specifically addressing encrypted devices.

Several of these cases, like *New York Tel. Co.*, involved a private company assisting the government in installing and operating various surveillance devices. In one case, the Ninth Circuit was asked "whether a district court, acting upon an application of the United States, possesses the power to issue an order compelling a duly licensed public utility ... to perform an in-progress trace of telephone calls by means of electronic facilities within its exclusive control."[138] The court ordered that the company be compensated for its assistance. Like the telephone company in *New York Tel. Co.* and Apple in the Central District of California case, the company did not claim that the order violated its Fourth Amendment rights, but rather argued that the ordered relief was beyond the reach of the All Writs Act.[139] Looking to Supreme Court case law, the Ninth Circuit observed that "the principles announced in *New York Telephone* compel the same result here." First, the assistance required was substantially similar to that required in New *York Tel. Co.* and was "virtually identical" in terms of its intrusive effect as the pen register in

[134] *Id.* at 174-75

[135] *Id.* at 176.

[136] *Id.*

[137] *Id.* (emphasis added).

[138] *See* Application of U. S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities, 616 F.2d 1122, 1123 (9th Cir. 1980).

[139] *Id.* at 1128.

New York Tel. Co.;[140] second, the company's assistance was necessary to carry out the court order;[141] third, on balance, the burden on the company did not rise to the level of unreasonableness;[142] and fourth, this application of the statute was consistent with congressional intent, as "Congress apparently believes that federal courts possess the authority to order the cooperation of private carriers in electronic surveillance."[143]

Other cases in the lower courts have approved assistance in the following situations:

- Ordering a provider of electronic communication services "to provide information, facilities, and technological assistance to facilitate the consensual recording of all electronic communication[s], ... and messaging, web trafficking, and text messaging, to and from" a cell phone.[144]
- Ordering a landlord of an apartment complex to provide access to videotapes from a security camera.[145]
- Ordering a defendant to produce the decrypted contents of a hard drive.[146]

Perhaps most relevant to the San Bernardino case are two recent cases applying the All Writs Act and the *New York Tel. Co.* factors to requests for access to data stored on various locked electronic devices. These two cases differ greatly in their level of analysis. In an unreported 2014 ruling, the government applied to the Southern District of New York under the All Writs Act for assistance in accessing a locked cell phone seized from a suspect incident to arrest.[147] In a short and cursory opinion, Magistrate Judge Gabriel Gorenstein held that based on *New York Tel. Co*., it was appropriate to order the manufacturer to attempt to unlock the phone and that "orders providing technological assistance of the kind sought here are often not deemed to be burdensome."[148]

In a more in-depth ruling, Magistrate Judge James Orenstein of the Eastern District of New York (EDNY) assessed whether the All Writs Act could support the government's request for assistance in unlocking an iPhone 5c running an earlier version of iOS.[149] On February 29, 2016, the court issued its ruling, holding that the government's request exceeded the court's authority to compel Apple's assistance against its wishes.[150] Judge Orenstein observed that the court cannot rely on the statute to do something that another statute already covers (but might have more stringent

[140] *Id.* at 1129.

[141] *Id.* ("To a greater extent than in New York Telephone, the refusal by Mountain Bell to cooperate would have completely frustrated any attempt to accomplish the tracing operation.").

[142] *Id.* at 1131.

[143] *Id.*

[144] *See In re* U.S. for an Order Directing a Provider of Communication Services to Provide Tech. Assistance to Agents of the U.S. Drug Enforcement Admin., No. 15-1242, 2015 WL 5233551, at *1 (D.P.R. Aug. 27, 2015).

[145] *See In re* Application of U.S. for an Order Directing X to Provide Access to Videotapes, No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) ("Here, the only cooperation required by the apartment complex is merely to provide access to surveillance tapes already in existence, rather than any substantive assistance, and nothing more. Therefore, the order directing the apartment complex to provide access to the security videotapes will not be burdensome for the apartment complex's business operations or its employees.").

[146] *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012).

[147] *See In re* XXX, Inc. No. 14-2258, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014).

[148] *Id.* at *2.

[149] *See In re* 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. Feb. 29, 2016).

[150] *Id.* at 1.

requirements) nor can the statute be used to request assistance that is explicitly or implicitly prohibited under another federal statute.[151]

First, Judge Orenstein set forth three elements the government must demonstrate based upon the *text* of the All Writs Act: (1) issuance of the writ must be in aid of the issuing court's jurisdiction; (2) the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and (3) the issuance of the writ must be "agreeable to the usages and principles of law."[152] Because the government "easily satisfies the first two elements," the court saved its more exacting scrutiny for the third element.[153] The court agreed with Apple that this inquiry must assess not only *enacted* legislation that either authorizes or prohibits certain government action (as the government argued), but also legislation that was *considered* but ultimately not adopted.[154] Judge Orenstein noted that a rule that only looked at enacted law "would transform the AWA from a limited gap-filling statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by Congress's superior ability to prohibit or preempt."[155] Because Congress has significantly debated, but ultimately decided not to include companies like Apple within CALEA's scope, the court concluded that extending the All Writs Act to the government's request would be against the "usages and principles of law."[156] The government had argued that CALEA does not speak to the current controversy as its scope only covers "telecommunication carriers" in relation to "data in transit," while the present controversy concerns "data at rest" and Apple is not considered a telecommunications carrier. Judge Orenstein rejected this argument, noting that when Congress wants to impose an obligation on a service provider concerning "data a rest," it has to affirmatively do so in enacted law, but has not done so here.[157]

Further, the opinion described "three additional factors" from *New York Tel. Co.* that must be assessed: "(1) the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction; (2) the reasonableness of the burden to be imposed on the writ's subject; and (3) the necessity of the requested writ to aid the court's jurisdiction."[158] As to the first element, the court noted that the fact that Apple merely leases, and does not sell, its iOS software to a device user is insufficient to provide the required "closeness of relationship."[159] Moreover, Judge Orenstein stated there was a significant legal difference between Apple's declining to offer assistance, which he held is

[151] *Id.* at 15.

[152] *Id.* at 11.

[153] *Id.* at 11-12.

[154] *Id.* at 21.

[155] *Id.* at 26.

[156] *Id.* at 14-16. Judge Orenstein's partial reliance on the term "usages and principles" to reject the government's request has been questioned by at least one scholar. *See* Orin Kerr, *The Weak Main Argument in Judge Orenstein's Apple Opinion*, The Volokh Conspiracy (March 2, 2019). However, his analysis of the "usages and principles" language is appears to be very similar to the "consistent with the intent of Congress" inquiry required by *New York Tel. Co. See "*All Writs Act and the Supreme Court: *United States v. New York Tel. Co.*," infra p. 19.

[157] For this proposition, Judge Orenstein cited 18 U.S.C. § 2703(f)(1), which provides that "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."

[158] *Id.* at 11.

[159] *Id.* at 36.

permissible, and thwarting a government investigation, which is not.[160] Under the second element, the court found that the rationales for upholding the order in *New York Tel. Co.* were "virtually all absent here," including the following:

1. Apple is not a highly regulated public utility with a duty to serve the public.
2. Apple has argued it is not in its best interest to comply with the order.
3. The assistance the government sought here is not something Apple would do in its normal course of business.
4. Apple has never offered the government the information needed to bypass an iPhone's passcode security on its own.
5. The burden on Apple in bypassing security of just one iPhone diverts many hours and hardware and software from Apple's normal business, which, based on the number of requests Apple has received to unlock other devices, could have a cumulative impact on Apple.[161]

In addition to these factors, perhaps the most important determination by Judge Orenstein was that a reviewing court could take into consideration not only the financial burden of complying with the specific request at hand, but also "more general considerations about reputations or the ramifications of compliance."[162]

Application of All Writs Act to San Bernardino Case

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. Specifically, on February 16, 2016, Magistrate Judge Sheri Pym of the Central District of California ordered Apple to provide the FBI with three forms of technical assistance:

- Allow the government to enter more than 10 passcodes without the risk of the data being wiped after the 10th incorrect try (i.e., shut off the auto-erase function)
- Automate the entry of those passcode combinations rather than have to enter them manually
- Try back-to-back passcode attempts without the gradually increasing delays between attempts that are currently programmed into the system

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.

Because of the limited case law, much of the litigation will likely depend on whether a reviewing court thinks the Supreme Court's interpretation of the All Writs Act in *New York Tel. Co.* can be read to cover Apple here or whether the burden on Apple is too great to force compliance.[163]

---

[160] *Id.* at 35-36.

[161] *Id.* at 38-41.

[162] *Id.* at 43 (citation omitted).

[163] As a threshold issue, like in *United States v. New York Tel. Co.*, 434 U.S. 159 (1977) ("It is undisputed that the order in this case was predicated upon a proper finding of probable cause, and no claim is made that it was in any way inconsistent with the Fourth Amendment."), the FBI in the San Bernardino case obtained a warrant to search the device (continued...)

Does the Order Impose an Unreasonable Burden on Apple?

A reviewing court would likely first assess whether the order would pose an unreasonable burden on Apple. This inquiry could largely rest on whether a reviewing court accepts Apple's argument that the "unreasonable burden" test includes an assessment of not only the burden on the company 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 technological 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.[164]

Moreover, there are distinct differences between the telephone company's reaction to the assistance required in *New York Tel. Co.* and Apple's perception of the order in the present case. First, while the New York Telephone Company had regularly employed pen registers as part of its billing practice, Apple has not created the type of software the government seeks here. Second, while installation of the pen register in *New York Tel. Co.* was not "offensive" to the company, the company had not proffered a "substantial interest in not providing assistance," and the company had previously promised to provide the FBI instructions on how to install its own pen register,[165] Apple has adamantly opposed altering its security features to allow the government access to the device, has proffered various financial and ethical reasons for not wanting to create such software, and has apparently never instructed the FBI on how to create such software on its own.[166]

Some might ask what *persuasive* value Judge Orenstein's decision from the E.D.N.Y. has in the San Bernardino case and potential future litigation.[167] There are a few technological differences between the assistance requested in the recent ruling from the E.D.N.Y. and the pending case in the Central District of California that might alter an All Writs Act analysis, especially with regard to the burden imposed on Apple.

First, the hardware and software of the devices in each case are different. In the E.D.N.Y. case the phone in question is an iPhone 5s running iOS 7. In the San Bernardino case, the phone in question is an iPhone 5c running iOS 8. This difference is notable because while the iPhone 5s has more advanced hardware, it is running an older operating system, one that does not encrypt the phone's storage by default. This distinction reduces the technological burden on Apple. Rather than rewrite their operating system (as is the request in the C.D. Cal. case), Apple already has the technological capability to access parts of a phone that is "locked" in the E.D.N.Y. case. While

(...continued)

in question, thus, vitiating any Fourth Amendment argument by Apple. Instead, the magistrate judge's order was contested on the grounds that it exceeds the All Writs Act.

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

[165] *Id.* at 174-75.

[166] *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 1-5 (C.D. Cal. February 25, 2016) (Apple Inc's motion to vacate order compelling Apple Inc. to assist agents in search, and opposition to government's motion compel assistance).

[167] Note that a magistrate's decision has no precedential value in other jurisdictions.

Apple could not access all information on the phone, they would have access to information stored within Apple's native applications on the device.[168]

Second, Apple contends that the government has not exhausted all its options before seeking to compel the company to take an action it would otherwise not.[169] The E.D.N.Y. phone in question is equipped with a Touch ID fingerprint scanner to unlock the device. In that case, the phone's owner had already pleaded guilty to the charges against him and is in government custody while incarcerated. Apple's response to the order asked why the government has not sought the fingerprint from the owner to fully unlock the device under penalty of contempt of court.[170]

Finally, Apple contends that because the iPhone in question in the E.D.N.Y. case runs iOS 7, the government could seek the assistance of a third party digital forensics company to perform the same services it seeks from Apple. Unlike the C.D. California case, Apple is not the only party that can accomplish the type of data extraction the government seeks.[171] Apple argues that as a private company, it should not be conscripted into government service when a market exists where the services the government requests may be hired and bought.

Is This Application of the All Writs Act Consistent with the Intent of Congress?

In addition to the potential burden on Apple, a reviewing court must assess whether compelling Apple's assistance would be "consistent with the intent of Congress."[172] This would appear to turn on what, if any, applicability CALEA has in the present case, and 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."[173] The question here is whether CALEA or any other federal law can be read as "specifically address[ing]" the relief the government seeks. The government takes the position 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.[174] Apple, supported by the *Feng* ruling from the Eastern

[168] "Apple, Inc.'s Reponses to Court's October 9, 2015 Memorandum and Order," available online at: https://www.eff.org/files/2015/10/23/2015-10-19_apple_response_brief.pdf.

[169] "Apple Inc.'s Supplemental Response to Court's October 9, 2015 Order and Opinion," available online at: https://www.eff.org/files/2015/10/23/e.d.n.y._1-15-mc-01902_16.pdf.

[170] See "Compelled Entry of Biometric Passcode," *infra* pp.13-14 for Fifth Amendment analysis of compelled use of fingerprint scanner.

[171] *Id.*

[172] United States v. New York Tel. Co., 434 U.S. 159, 172 (1977).

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

[174] *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 25, 2016) (Apple Inc's motion to vacate order compelling Apple Inc. to assist agents in Search, and opposition to government's motion compel assistance).

District of New York,[175] posits that should courts look not only to enacted law, but also to whether Congress considered, but declined to adopt, regulations on technology companies like Apple.[176]

As shown in **Table 1**, CALEA creates a broad requirement on a "telecommunications carrier" to help the government "intercept" various real-time communications, but includes several exceptions to this requirement.

Table 1. Communications Assistance for Law Enforcement Act (CALEA)

Category	Title	U.S. Code Section	Statutory text
1	Capability Requirements	47 U.S.C. § 1002(a)	"[A] telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of ... expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier ...."
2	Design of features and systems configurations	47 U.S.C. § 1002(b)(1)	"This subchapter does not authorize any law enforcement agency or officer— to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services."
3	Information services; private networks and interconnection services and facilities	47 U.S.C. § 1002(b)(2)	"The requirements of subsection (a) of this section do not apply to— information services; or equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers."
4	Encryption	47 U.S.C. § 1002(b)(3).	"A telecommunications carrier shall not be 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."

Source: Compiled by CRS.

[175] *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 15-MC-1902, at 15-16 (E.D.N.Y. Feb. 29, 2016).

[176] *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 15-19 (C.D. Cal. February 25, 2016) (Apple Inc's motion to vacate order compelling Apple Inc. to assist agents in Search, and opposition to government's motion compel assistance).

There appear to be two potential inquiries concerning CALEA's relationship to the All Writs Act. First, Apple argues that CALEA's *text* itself would make application of the All Writs Act here "inconsistent with the intent of Congress." To make this argument Apple relies primarily on category 2, which provides that the government cannot require a provider of an "electronic communication service" to adopt any specific equipment design or software configuration.[177] The government, citing category 1, has countered that CALEA does not apply at all in this case, as it only obligates a "telecommunications carrier" to help the government "intercept" communications—that is, access data "in transit," but does not cover "data at rest," which is what this case concerns.[178]

Note that the scope of the limitation in category 2 states that "this subchapter does not authorize any law enforcement agency or officer ... ," while the limitation in category 3 states that "the requirements of subsection (a) do not apply ...." One way to interpret this difference is that category 2 provides that the government cannot use CALEA to mandate a company adopt specific hardware or software designs, and that category 3 creates an exception for the obligations under subsection (a). Under this reading, the limitation in category 2 could be interpreted broadly to cover not only data subject to subsection (a)—that is, data in transit—but *explicitly precludes* the government from relying on CALEA to mandate that an electronic communication provider—which Apple asserts it is—from adopting specific features in relation to *any* data, at rest or in transit. If this reading is accurate, one could argue that mandating Apple here would be inconsistent with the intent of Congress expressed in CALEA. However, it should be noted that even under this reading, category 2 merely states the government cannot rely on CALEA to mandate providers of electronic communication service to adopt certain designs, but does not operate as a flat-out ban on the government mandating such designs. The government, in theory, could resort to another statute for such authority. Additionally, Apple argues that the exception in category 3 for "information services," which again Apple argues it is, indicates an intent by Congress not to bring it within the CALEA's umbrella.

The second inquiry is whether the fact that Congress has considered but failed to obligate companies like Apple to assist the government in decrypting data should preclude application of the All Writs Act here. Again, the government argues that any indication of congressional intent must come from enacted law, while Apple asserts that a reviewing court must also assess whether Congress considered but failed to adopt this type of proposal. If a court accepts Apple's view, there is evidence that Congress did in fact consider applying CALEA to companies like Apple, but declined to do so.[179] And, as noted by the Eastern District of New York, more recently Congress has significantly debated imposing obligations on technology companies to provide decryption assistance, but nothing has garnered sufficient support for passage. The government

[177] *Id.* at 16-17.

[178] *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, at 24-25 (Feb. 19, 2016) (government's motion to compel Apple, Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search).

[179] 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.").

argues, however, that CALEA, by its terms, applies to data in transit, not rest, so CALEA is inapplicable here, and, further, that there is no other enacted law prohibiting the relief it seeks here.

Is Apple's Assistance Necessary to Carrying out the Court's Order?

Lastly, a reviewing court must assess whether Apple's assistance is necessary to enforce the order. The FBI requires Apple's assistance in accessing the iPhone in question because of how Apple implemented its encryption. The encryption key is derived from a combination of user input (i.e., the passcode) and the device's UID. Even if the FBI had the passcode, they would need to enter it on the specific device because it needs to be combined with the UID to create the key. In order to accomplish the FBI's request of disabling security functions Apple designed, the FBI requires Apple to create an operating system without those functions. Apple's operating systems are digitally signed using a certificate generated through a cryptographic process to ensure the integrity of the software being loaded when the device is turned on. Recreating that cryptographically signed certificate would be as challenging as brute-force attacking an encryption key, as described above. Having Apple create the operating system allows the FBI a direct way into the phone and the opportunity to try to guess the passcode. Each pass at an attempt will be combined with the UID to create the key.

Moving forward, a hearing is scheduled in the San Bernardino case for March 22, 2016.

Potential Congressional Response

With technology companies moving toward more, not less, encryption for data transiting and stored on their devices, there are various potential responses by Congress:

- **Mandate Backdoor**. Congress could create a "CALEA 2.0" and require technology companies to have the technological means feasible to access data stored on locked devices, similar to the mandate on telecommunication providers contained in the original CALEA. DOJ suggested such a proposal in 2010,[180] and again in 2013,[181] but this measure was never introduced.[182] The Obama Administration has stated at congressional hearings and elsewhere that it is not seeking such legislation at this time.[183]
- **Criminal Penalty for Failure to Decrypt.** At least one commentator has suggested that Congress could make it a federal crime with severe penalties to refuse to enter in one's passcode when requested by a law enforcement officer.[184]

[180] Charlie Savage, *US Tries to Make it Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=0.

[181] Charlie Savage, *US Weighs Wide Overhaul of Wiretap Laws*, NY TIMES (May 7, 2013), *available at* http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?ref=charliesavage.

[182] Apple has raised both First Amendment and substantive due process claims that could, if valid, restrict Congress's ability to enact such legislation. 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 32-34 (C.D. Cal. February 25, 2016) (Apple Inc's motion to vacate order compelling Apple Inc. to assist agents in search, and opposition to government's motion compel assistance). This issue, however, is beyond the scope of this report.

[183] *See* Senate Hearing, *supra* note 8.

[184] Kerr, *supra* note 102.

However, if an individual has a valid Fifth Amendment privilege against self-incrimination, the government could not force the individual to turn over the passcode, without providing him use and derivative use immunity.[185]

- **Data retention laws**. Congress might require that companies retain certain categories of data, such as text messages, emails, or other content material, for a certain period of time.
- **Prohibit Encryption Mandates.** Alternatively, some Members have sought to prohibit any mandate on technology companies to be able to decrypt data on their devices. The Secure Data Act of 2015 (S. 135, H.R. 726) and the End Warrantless Surveillance of Americans Act (H.R. 2233), which contain identical provisions concerning anti-encryption mandates, would provide that "no agency may mandate or request that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency."[186] The bills contain an exception for any mandate under the Communications Assistance Law Enforcement Act (CALEA).
- **Create a National Encryption Panel**. Several Members recently introduced the Digital Security Commission Act of 2016 (S. 2604, H.R. 4651), which 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."[187] The commission would report to Congress not later than one year after the commission first convenes. Such a report would assess, among other things, the economic and commercial value of encryption technology, the effects of encryption on law enforcement and national security investigations, and potential changes to federal law to accommodate these varying interests.
- **Improve Law Enforcement's Capabilities to Investigate Despite Encryption.** In her testimony to the House Judiciary Committee, cybersecurity expert Susan Landau offered an alternative to the government choosing between strong encryption and weak encryption.[188] She suggests that the government help law enforcement develop and build the capability to conduct investigations through technical means and in accordance with the legal framework passed by Congress and enforced through the courts. This option would not weaken encryption, or reduce the adoption of encryption, but would attempt to provide a capability to continue investigations despite encryption.

[185] *See generally* United States v. Hubbell, 530 U.S. 27 (2000).

[186] S. 135, 114th Cong. (2015); H.R. 726, 114th Cong. (2015); H.R. 2233, 114th Cong. (2015).

[187] S. 2604, 114th (2016); H.R. 4651, 114th (2016).

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

Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov , 7-....

(name redacted)
Analyst in Cybersecurity Policy
[redacted]@crs.loc.gov , 7-....