

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

IN RE ORDER REQUIRING APPLE INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT

Docket Nos. 14 Cr. 387 (MKB)  
15 Misc. 1902 (JO)

**APPLE INC.'S MEMORANDUM OF LAW IN RESPONSE TO THE GOVERNMENT'S  
BRIEF IN SUPPORT OF ITS APPLICATION FOR AN ORDER COMPELLING  
APPLE INC. TO ASSIST LAW ENFORCEMENT AGENTS IN THE  
EXECUTION OF A SEARCH WARRANT**

Marc J. Zwillinger\*  
marc@zwillgen.com  
Jeffrey G. Landis\*  
jeff@zwillgen.com  
ZWILLGEN PLLC  
1900 M Street N.W., Suite 250  
Washington, D.C. 20036  
Telephone: 202.706.5202  
Facsimile: 202.706.5298

\*Admitted *Pro Hac Vice*

Theodore J. Boutrous Jr.\*  
tboutrous@gibsondunn.com  
GIBSON, DUNN & CRUTCHER LLP  
333 South Grand Avenue  
Los Angeles, CA 90071-3197  
Telephone: 213.229.7000  
Facsimile: 213.229.7520

Alexander H. Southwell  
asouthwell@gibsondunn.com  
Mylan L. Denerstein  
mdenerstein@gibsondunn.com  
GIBSON, DUNN & CRUTCHER LLP  
200 Park Avenue  
New York, NY 10166-0193  
Telephone: 212.351.4000  
Facsimile: 212.351.4035

*Attorneys for Apple Inc.*

**TABLE OF CONTENTS**

	<u>Page</u>
I. PRELIMINARY STATEMENT .....	1
II. FACTUAL BACKGROUND.....	4
A. Apple’s Device Security And Prior Extraction Orders.....	4
B. The Drug Trafficking Case Against Jun Feng.....	5
C. The Government Seeks To Enlist Apple To Extract Data From Feng’s iPhone.....	6
D. Following Mr. Feng’s Guilty Plea, The Government Continues Its Efforts To Compel Apple To Extract Data From His iPhone.....	10
E. Judge Orenstein’s Opinion.....	11
F. The Government’s Application To This Court.....	12
III. ARGUMENT .....	13
A. Judge Orenstein’s Order Should Be Reviewed Under The “Clearly Erroneous or Contrary to Law” Standard. ....	13
B. The All Writs Act Does Not Authorize The Order The Government Seeks Here. ....	15
C. The Government’s Request Is Inconsistent With CALEA And The Comprehensive Statutory Framework Of Which It Is A Part.....	21
1. CALEA Specifically Exempts Information Service Providers From Having To Create Or Maintain Systems To Facilitate Government Access. ....	22
2. Congress’s Comprehensive Statutory Scheme Addressing Third Party Assistance In Accessing Communications Delineates The Exclusive Means By Which Courts May Compel Such Assistance. ....	24
3. Use Of The All Writs Act Would Usurp Congressional Authority.....	29
D. The Government’s Request Is Not Authorized By <i>New York Telephone</i> .....	32
1. The Government Has Utterly Failed To Demonstrate Necessity. ....	33

**TABLE OF CONTENTS**  
(continued)

	<u>Page</u>
2. The Remaining Discretionary Factors Under <i>New York Telephone</i> Militate Against Compelling Apple’s Assistance.....	37
IV. CONCLUSION.....	45

**TABLE OF AUTHORITIES**

<b>Cases</b>	<u>Page(s)</u>
<i>ACLU v. Clapper</i> , 785 F.3d 787 (2d Cir. 2015).....	31
<i>In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc’ns over Tel. Facilities</i> , 616 F.2d 1122 (9th Cir. 1980) .....	20, 33, 41, 43
<i>In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information</i> , 809 F. Supp. 2d 113 (E.D.N.Y. 2011) .....	15
<i>In re Application of U.S. for an Order Directing X to Provide Access to Videotapes</i> , 2003 WL 22053105 (D. Md. Aug. 22, 2003) .....	20, 41, 42, 43
<i>In re Application of the U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Tel.</i> , 460 F. Supp. 2d 448 (S.D.N.Y. 2006).....	15
<i>In re Application of the U.S. for an Order of Nondisclosure</i> , 41 F. Supp. 3d 1 (D.D.C. 2014) .....	15
<i>In re Application of U.S. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder</i> , 610 F.2d 1148 (3d Cir. 1979).....	20
<i>Arizona v. United States</i> , 132 S. Ct. 2492 (2012).....	28
<i>Bank of U.S. v. Halstead</i> , 23 U.S. (10 Wheat.) 51 (1825).....	17, 18, 19
<i>Bayway Ref. Co. v. Oxygenated Mktg. &amp; Trading A.G.</i> , 215 F.3d 219 (2d Cir. 2000).....	36
<i>Beers v. Haughton</i> , 34 U.S. (9 Pet.) 329 (1835).....	19
<i>Bernstein v. Vill. of Piermont</i> , 2013 WL 5718450 (S.D.N.Y. Oct. 21, 2013).....	35
<i>Block v. Cmty. Nutrition Inst.</i> , 467 U.S. 340 (1984).....	28

**TABLE OF AUTHORITIES**

(continued)

	<u>Page(s)</u>
<i>Bob Jones Univ. v. United States</i> , 461 U.S. 574 (1983).....	30, 32
<i>Bowsher v. Synar</i> , 478 U.S. 714 (1986).....	31
<i>Clinton v. Goldsmith</i> , 526 U.S. 529 (1999).....	17
<i>District of Columbia v. Heller</i> , 554 U.S. 570 (2008).....	38
<i>FTC v. Dean Foods Co.</i> , 384 U.S. 597 (1966).....	31
<i>FDA v. Brown &amp; Williamson Tobacco Corp.</i> , 529 U.S. 120 (2000).....	24
<i>Gonzalez v. Raich</i> , 545 U.S. 1 (2005).....	28
<i>Greater New Orleans Broad. Ass’n v. United States</i> , 527 U.S. 173 (1999).....	32
<i>Harris v. Nelson</i> , 394 U.S. 286 (1969).....	17
<i>INS v. Chadha</i> , 462 U.S. 919 (1983).....	31
<i>Ivey v. Harney</i> , 47 F.3d 181 (7th Cir. 1995) .....	17, 19
<i>Knipe v. Skinner</i> , 999 F.2d 708 (2d Cir. 1993).....	36
<i>Lowery v. McCaughtry</i> , 954 F.2d 422 (7th Cir. 1992) .....	16
<i>Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.</i> , 13 F. Supp. 3d 157 (D.D.C. 2014).....	14
<i>Michigan Bell Tel. Co. v. United States</i> , 565 F.2d 385 (6th Cir. 1977) .....	33, 34, 38, 41

**TABLE OF AUTHORITIES**

(continued)

	<u>Page(s)</u>
<i>New York v. Mountain Tobacco Co.</i> , 953 F. Supp. 2d 385 (E.D.N.Y. 2013) .....	15
<i>In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant by Unlocking a Cellphone</i> , 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014).....	21
<i>P.R. Dep’t of Consumer Affairs v. Isla Petrol. Corp.</i> , 485 U.S. 495 (1988).....	30, 32
<i>Pa. Bureau of Corr. v. U.S. Marshals Serv.</i> , 474 U.S. 34 (1985).....	19, 27, 28
<i>Plum Creek Lumber Co. v. Hutton</i> , 608 F.2d 1283 (9th Cir. 1979) .....	17, 33, 35, 45
<i>Revise Clothing, Inc. v. Joe’s Jeans Subsidiary, Inc.</i> , 687 F. Supp. 2d 381 (S.D.N.Y. 2010).....	36
<i>Trenkler v. United States</i> , 536 F.3d 85 (1st Cir. 2008).....	17, 24, 28
<i>In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.</i> , 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) .....	15
<i>United States v. Barret</i> , 178 F.3d 34 (1st Cir. 1999).....	28
<i>United States v. Blake</i> , No. 13-CR-80054 (S.D. Fl. July 14, 2014).....	21
<i>United States v. Burr</i> , 25 F. Cas. 30 (C.C., D. Va. 1807).....	20
<i>United States v. Catoggio</i> , 698 F.3d 64 (2d Cir. 2012).....	38
<i>United States v. Cellular Tel. Devices Seized On Or About June 11, 2014 From Premises Located At 41-21 149th Street, First Floor, In Queens, NY</i> , 15-MJ-610 (VVP) (E.D.N.Y. 2015) .....	6
<i>United States v. Craft</i> , 535 U.S. 274 (2002).....	31
<i>United States v. Djibo</i> , 2015 WL 9274916 (E.D.N.Y. Dec. 16, 2015).....	9, 34

**TABLE OF AUTHORITIES**

(continued)

	<u>Page(s)</u>
<i>United States v. Doe</i> , 537 F. Supp. 838 (E.D.N.Y. 1982) .....	20
<i>United States v. Estate of Romani</i> , 523 U.S. 517 (1998).....	31
<i>United States v. Fricosu</i> , 841 F. Supp. 2d 1232 (D. Colo. 2012).....	38
<i>United States v. Hall</i> , 583 F. Supp. 717 (E.D. Va. 1984) .....	20, 41, 42, 43
<i>United States v. Hayman</i> , 342 U.S. 205 (1952).....	16, 29
<i>United States v. N.Y. Tel. Co.</i> , 434 U.S. 159 (1977).....	2, 15, 17, 28, 29, 32, 33, 37, 38, 39, 41, 42, 43, 44
<i>United States v. The Premises Known and Described as 41-21 149th Street, 1st Floor, Queens, NY</i> , No. 14-MJ-530 (E.D.N.Y. 2014).....	5
<i>United States v. Premises Known as 281 Syosset Woodbury Rd.</i> , 862 F. Supp. 847 (E.D.N.Y. 1994) .....	14
<i>United States v. Warshay</i> , 1998 WL 767138 (E.D.N.Y. Aug. 4, 1998).....	14, 15
<i>United States v. X</i> , 601 F. Supp. 1039 (D. Md. 1984).....	20
<i>United States v. Yang</i> , 14-CR-387 (MKB).....	6, 10, 14
<i>Virginian Ry. Co. v. Sys. Fed’n No. 40</i> , 300 U.S. 515 (1937).....	19
<i>Wayman v. Southard</i> , 23 U.S. 1 (1825).....	18
<i>Youngstown Sheet &amp; Tube Co. v. Sawyer</i> , 343 U.S. 579 (1952).....	31
<i>Zino Davidoff SA v. CVS Corp.</i> , 571 F.3d 238 (2d Cir. 2009).....	31

**TABLE OF AUTHORITIES**

(continued)

	<u>Page(s)</u>
<b>Statutes</b>	
18 U.S.C. § 2510.....	26
18 U.S.C. § 2511.....	25, 28
18 U.S.C. § 2518(4).....	25
18 U.S.C. § 2703.....	10, 25, 26, 28, 36
18 U.S.C. § 3123.....	25, 27
28 U.S.C. § 636.....	14, 15
28 U.S.C. § 1651.....	7, 16
47 U.S.C. § 153.....	41
47 U.S.C. § 1001.....	21, 22, 24, 26
47 U.S.C. § 1002.....	22, 25, 26
Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1849 (1986).....	28
Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978).....	4, 27, 28
Pen/Trap Statute, Pub. L. No. 99-508, 100 Stat. 1848 (1986).....	27
Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).....	28
USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 274 (2009).....	28
<b>Other Authorities</b>	
An Act to Establish the Judicial Courts of the United States, § 14, 1 Stat. 81 (1789).....	16
Edward Jenks, <i>The Prerogative Writs in English Law</i> , 32 Yale L. J. 523 (1923).....	16
End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015).....	4
F.W. Maitland, <i>The History of the Register of Original Writs</i> , 3 Harv. L. Rev. 97 (1889).....	16
H.R. Rep. No. 103-827(I) (1994).....	22



**TABLE OF AUTHORITIES**

*(continued)*

	<u>Page(s)</u>
Restatement (Second) of Contracts § 367.....	19
Secure Data Act of 2015, H.R. 726, 114th Cong. (2015).....	4
Secure Data Act of 2015, S.135, 114th Cong. (2015) .....	4

**Rules**

E.D.N.Y. Loc. Crim. R. 59.1 .....	15
E.D.N.Y. Loc. Civ. R. 72.1.....	15
Fed. R. Crim. P. 59 .....	14

## I. PRELIMINARY STATEMENT

The government seeks to compel Apple to take possession of an iPhone and breach its security features absent any showing of the need for Apple’s assistance, and under a sweeping interpretation of the All Writs Act that has been soundly rejected by Magistrate Judge Orenstein—an inconvenient fact the government attempts to obscure by styling its present application as a renewed application subject to *de novo* review. The government requests this extraordinary relief notwithstanding: the likely minimal evidentiary value of any data on the phone (given that all defendants have pled guilty and the phone was seized and last used nearly two years ago); that Congress has never authorized the power to compel private parties that the government seeks here; and that the record is devoid of evidence that Apple’s assistance is necessary—and remains so even after a similar claim of necessity was proven untrue in a recent proceeding in California. Indeed, in its original application to Judge Orenstein, the government acknowledged that it sought Apple’s help to spare *the government* from having to expend “significant resources.” DE 1 at 2-3.<sup>1</sup> Moreover, the government has lodged this application even as members of Congress are debating the legality of these kinds of requests, and after FBI Director James Comey expressly observed that litigation is ill-suited for resolution of complex policy debates such as this. *See* Ex. A<sup>2</sup> [James Comey, *The Expectations of Privacy: Balancing Liberty, Security, and Public Safety*, Kenyon College (Apr. 6, 2016) (observing that “litigation is a terrible place to have any kind of discussion about a complicated policy issue, especially one that touches on our values, on the things we care about most, on technology, on tradeoffs and

---

<sup>1</sup> Unless otherwise noted, all references to docket entries (“DE”) are to the docket in Case No. 15-mc-1902.

<sup>2</sup> All referenced exhibits are attached to the Declaration of Alexander H. Southwell, dated April 15, 2016, and filed concurrently herewith.

balance”)]. For all of these reasons, Judge Orenstein’s opinion should be affirmed, and the government’s application should be denied.

As a preliminary matter, the government has utterly failed to satisfy its burden to demonstrate that Apple’s assistance in this case is necessary—a prerequisite to compelling third party assistance under the All Writs Act. *See United States v. N.Y. Tel. Co.* (“*New York Telephone*”), 434 U.S. 159, 175 (1977). The government has made no showing that it has exhausted alternative means for extracting data from the iPhone at issue here, either by making a serious attempt to obtain the passcode from the individual defendant who set it in the first place—nor to obtain passcode hints or other helpful information from the defendant—or by consulting other government agencies and third parties known to the government. Indeed, the government has gone so far as to claim that it has no obligation to do so, *see* DE 21 at 8, notwithstanding media reports that suggest that companies already offer commercial solutions capable of accessing data from phones running iOS 7, which is nearly three years old. *See* Ex. B [Kim Zetter, *How the Feds Could Get into iPhones Without Apple’s Help*, *Wired* (Mar. 2, 2016) (discussing technology that might be used to break into phones running iOS 7)]. Further undermining the government’s argument that Apple’s assistance is necessary in these proceedings is the fact that only two and a half weeks ago, in a case in which the government first insisted that it needed Apple to write new software to enable the government to bypass security features on an iPhone running iOS 9, the government ultimately abandoned its request after claiming that a third party could bypass those features *without Apple’s assistance*. *See* Ex. C [*In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate #5KGD203* (“*In the Matter of the Search of an Apple iPhone*” or the “San Bernardino Matter”), No. 16-cm-10, DE 209 (C.D. Cal. Mar. 28,

2016)]. In response to those developments, the government filed a perfunctory letter in this case stating only that it would not modify its application. DE 39. The letter does not state that the government attempted the method that worked on the iPhone running iOS 9, consulted the third party that assisted with that phone, or consulted other third parties before baldly asserting that Apple's assistance remains necessary in these proceedings. *See id.* The government's failure to substantiate the need for Apple's assistance, alone, provides more than sufficient grounds to deny the government's application.

Apart from this fundamental deficiency, the government's request is predicated on a distortion of the All Writs Act. The government would have this Court believe that the All Writs Act, first enacted in 1789, is a boundless grant of authority that permits courts to enter any order the government seeks—including orders conscripting private third parties into providing whatever assistance law enforcement deems appropriate—as long as Congress has not expressly prohibited its issuance. DE 30 at 18. But that characterization of the All Writs Act turns our system of limited government on its head. It simply is not the case that federal courts can issue any order the executive branch dreams up unless and until Congress expressly prohibits it. That construction of the All Writs Act has it exactly backwards. If the government's view is correct, Congress would never need to pass permissive legislation in the law enforcement context because everything would be on the table until explicitly prohibited. That may be what the government prefers, but it is not the legal system in which it operates.

Moreover, the government's request contravenes congressional intent. Neither the Communications Assistance for Law Enforcement Act ("CALEA") nor the comprehensive legislative scheme of which it is a part authorizes the order the government seeks here; to the contrary, they collectively confirm that Congress never intended that such authority be available.

While Apple strongly supports, and will continue to support, the efforts of law enforcement in pursuing criminals, the government’s sweeping interpretation of the All Writs Act is plainly incorrect and provides no limit to the orders the government could obtain in the future. And that is precisely what the government seeks here: to obtain an order that it can use as precedent to lodge future, more onerous requests for Apple’s assistance, *see* DE 29 at 41 (noting that the government “clearly intends to continue seeking assistance that is similarly burdensome – if not more so – for the foreseeable future”); *see also* Ex. D [Spencer Ackerman & Sam Thielman, *FBI Director Admits Apple Encryption Case Could Set Legal Precedent*, *Guardian* (Feb. 25, 2016)], notwithstanding that the scope of the government’s authority to compel third party assistance and the legality of these requests is currently the subject of ongoing political and public debate.<sup>3</sup> This Court should reject the government’s overreaching and unsupported interpretation of the All Writs Act, and deny the government’s application.

## II. FACTUAL BACKGROUND

### A. Apple’s Device Security And Prior Extraction Orders.

Apple consistently strives to increase the security of its devices to protect the safety and privacy of its customers against threats known and unknown. Apple implemented strong

---

<sup>3</sup> *See, e.g.*, Ex. E [Hearing on Encryption Security and Privacy Before the H. Judiciary Comm. (Mar. 1, 2016) (“*Encryption Hr’g*”)]; Ex. F [Hearing on World Wide Threats Before the H. Select Intelligence Comm. (Feb. 25, 2016)]. In addition, members of Congress have lodged several legislative proposals, some of which would require companies to assist the government, while others would prohibit compulsory assistance. *See* Ex. G [Sean Sposito & Carolyn Lochhead, *As Apple, FBI Spar, Feinstein Pushes Bill to Require Decryption*, *SF Gate* (Apr. 8, 2016) (describing draft legislation by Senators Dianne Feinstein and Richard Burr that would compel technology companies to assist government agencies in gaining access to encrypted technology)]; *see also* Secure Data Act of 2015, S.135, 114th Cong. (2015) (proposal to prohibit federal agencies from requiring hardware or software manufacturers to design or alter security functions in their products to allow surveillance, and exempting products used pursuant to CALEA); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015) (same); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015) (same, amending the Foreign Intelligence Surveillance Act of 1978).

encryption as far back as iOS 3, which was released in 2009, and with each update, has added new security features to better protect users' information from hackers and cyber criminals. In iOS 7, which is the operating system on the iPhone 5s at issue here, Apple, among other things, added Touch ID, introduced FaceTime audio encryption, and upgraded its "Find My iPhone" program to allow users to track, lock, and remotely wipe their lost or stolen phone. *See* Ex. H [Apple Inc., *iOS Security: iOS 9.0 or later* (Sept. 2015)]; *see also* Ex. I [Max Eddy, *iOS 7 Makes the iPhone More Secure than Ever*, PCMag.com (Sept. 13, 2013)]. Beginning with iOS 8, Apple introduced a feature that prevents anyone without the passcode from accessing the device's encrypted data, including Apple. *See generally* Ex. H [Apple Inc., *iOS Security: iOS 9.0 or later* (Sept. 2015)].

Apple does have the technical ability to extract unencrypted user data from a locked device running iOS 7 or earlier. *See* DE 11 at 3. Whether the extraction can be performed depends on the device, and whether it is in good working order. *Id.* As a general matter, certain user-generated active files on an iOS device that are contained in Apple's native apps can be extracted. *Id.* Apple cannot, however, extract email, calendar entries, or any other third-party app data. *Id.* Apple has in the past extracted unencrypted data from locked devices running iOS 7 or earlier and provided such data to the government in response to court orders. DE 16 at 3. In those cases, however, the government had obtained the order in *ex parte* proceedings in which Apple did not participate. *Id.*

**B. The Drug Trafficking Case Against Jun Feng.**

On June 6, 2014, in conjunction with an ongoing drug-trafficking investigation, the government obtained a warrant to search the residence of Jun Feng ("Feng"). *See United States v. The Premises Known and Described as 41-21 149th Street, 1st Floor, Queens, NY*, No. 14-MJ-530 (MDG), DE 2. During that search, the government seized an iPhone 5s running iOS 7

(“Feng’s iPhone”), the then-current operating system for iPhones. Law enforcement arrested Feng on June 11, 2014, and a grand jury indicted him on July 9, 2014, for conspiracy to traffic in methamphetamine. *See United States v. Yang*, No. 14-CR-387 (MKB), DE 25 (minute entry); DE 47 (indictment).

Not until more than a year after seizing Feng’s iPhone did the government seek to search it. A search warrant application was granted on July 6, 2015. *See United States v. Cellular Tel. Devices Seized on or About June 11, 2014 from Premises Located at 41-21 149th Street, First Floor, in Queens, NY*, 15-MJ-610 (VVP), DE 1 (application for warrant). The government claims that the U.S. Drug Enforcement Agency (“DEA”) attempted to execute the warrant but was unable to access the device because it was protected by a passcode that the DEA could not bypass. *See* DE 19 (transcript of hearing dated Oct. 26, 2015) (“Tr.”) at 6-7. The government asserts that the DEA consulted with the FBI, which also claimed it was unable to bypass the passcode.<sup>4</sup> *See id.* There is no evidence in the record that the government consulted with any other governmental entities or third parties. *See infra* III.D.1. In fact, the government refused to make the representation that it had engaged in such consultations when asked by Judge Orenstein on the record, and later claimed it had no obligation to do so. *See* Tr. 34-35; DE 21 at 8.

**C. The Government Seeks To Enlist Apple To Extract Data From Feng’s iPhone.**

Not until October 2015, nearly three months after the warrant issued and on the eve of Feng’s trial, did the government approach Apple regarding execution of the warrant to search Feng’s iPhone. In response to that inquiry, Apple informed the government that the contents of the phone were not backed up to Apple’s iCloud storage service and that the phone had a remote

---

<sup>4</sup> The record does not establish whether the government attempted to access certain types of data (*i.e.*, a log of recent telephone calls) that, depending on user settings, may be accessible without entering the passcode. DE 29 at 4 n.4.

wipe request pending. *See* DE 15 at 8. Apple later informed the government that the remote wipe request would not function on Feng's iPhone. *See* Tr. 32-33.

On October 8, 2015, the government applied to Judge Orenstein, serving as duty magistrate, for an *ex parte* order compelling Apple to bypass the security passcode on Feng's iPhone. DE 1 (the "Initial Application"). The Initial Application cited the All Writs Act, 28 U.S.C. § 1651, as the basis for the Court's authority to issue such an order. DE 1 at 2. The government submitted with its Initial Application a proposed order. *See id.*; DE 1-1. The proposed order included certain language from Apple's law enforcement compliance manual outlining how Apple would obtain the data it was being ordered to produce. Apple included this language in its manual in response to the government's prior reliance on orders that failed to specify the scope of Apple's obligations and did not correspond to the procedures that Apple had available to perform extractions and deliver data to law enforcement. To make clear what Apple could and could not do, Apple opted to include in its law enforcement manual proposed language specifying what it would do when ordered to perform extractions. Nowhere in that manual, however, does Apple concede that the All Writs Act is a proper basis to compel Apple to perform data extractions.<sup>5</sup>

On October 9, 2015, Judge Orenstein issued a memorandum and order deferring decision on the government's Initial Application and observing that whether the All Writs Act was properly invoked depended on "whether the government seeks to fill in a statutory gap that

---

<sup>5</sup> The government asserts in its application to this Court that "Apple has developed guidance for law enforcement agents for obtaining lawful court orders to request such a bypass." DE 30 at 5. As Judge Orenstein observed in response to the same representation, this "could be read to suggest that Apple somehow proposed or approved the government's reliance on the AWA as authority for the request." DE 29 at 4 n.4. That is not the case. As Judge Orenstein noted in rejecting such a suggestion, "it is only the [Initial] Application itself that cites the AWA; the proposed order submitted with it does not, but instead contains the technical language specifically describing the assistance the government wants Apple to provide." *Id.*



Congress has failed to consider, or instead seeks to have the court give it authority that Congress chose not to confer.” DE 2 at 2. Analyzing the All Writs Act, relevant case law, and pertinent legislative enactments, Judge Orenstein “conclude[d] that the authorities on which the government relies do not support the conclusion that the All Writs Act permits the relief the government seeks.” *Id.* at 10. Judge Orenstein nevertheless directed Apple to submit its views on whether compliance with the government’s application would be technically feasible, and if so, whether compliance would be unduly burdensome. *Id.* at 1.

On October 19, 2015, Apple responded to the Court’s memorandum and order, providing relevant technical information regarding the security features of iOS devices and explaining that for the dwindling number of Apple devices running iOS 7, Apple has the technical ability to extract certain categories of unencrypted data from a passcode-locked device. DE 11 at 2-3. Apple also identified the burdens that complying with the government’s application would impose on Apple. *Id.* at 3-4. The government replied to Apple’s opposition on October 22, 2015, DE 15, and at the Court’s direction, Apple submitted a supplemental brief a day later, addressing the applicability of the All Writs Act to the order the government sought, DE 16.

On October 26, 2015, the Court heard oral argument. DE 18. At the outset, Judge Orenstein brought to the parties’ attention certain materials from *United States v. Djibo*, No. 15-CR-88 (SJ) (E.D.N.Y.), an unrelated criminal matter. *See* Tr. 3. In particular, Judge Orenstein provided the parties with a letter submitted by the Department of Justice in *Djibo*, in which it represented that Homeland Security Investigations (“HSI”) “is in possession of technology that would allow its forensic technicians to override the passcode security feature on the Subject

iPhone and obtain the data contained therein.”<sup>6</sup> *See* Ex. J [*Djibo*, No. 15-CR-88 (SJ), DE 27 (E.D.N.Y. July 9, 2015)]. Judge Orenstein also provided the parties with a transcript from a hearing held on the defendant’s motion to suppress in *Djibo* that contained testimony from an FBI Special Agent asserting that he had personally bypassed an iPhone running a version of iOS 7, the same operating system at issue here. *See* Ex. K [*Djibo*, No. 15-CR-88 (SJ), DE 65, 9/3/15 Hearing Transcript, at 17; 29-31 (E.D.N.Y. Oct. 16, 2015)].

Judge Orenstein also asked the government at the hearing whether it could represent that it sought assistance from other government agencies outside the FBI and DEA, including the intelligence community, to bypass the passcode of the device. *See* Tr. 34. The government would only represent that “the FBI and DEA do not have a reasonable [sic] available tool.” *Id.* at 34-35. Nor did the government make the requested representation in its post-hearing submission, arguing instead that criminal prosecutors are not “required to consult with intelligence agencies or with other components that are not part of the prosecution team before applying for relief under the All Writs Act.” DE 21 at 8. All told, the government offered no evidence that it had consulted with any other agencies or third parties to determine that Apple’s assistance was actually necessary, or that it had exhausted other potential repositories of the information it seeks to extract from Feng’s iPhone, such as Feng himself, cell-phone service providers, email providers or social media services.

Nor did the government exhaust traditional investigative tools that were suggested to the government by Apple. In fact, the government issued Apple a single subpoena in this case,

---

<sup>6</sup> In *Djibo*, the defendant argued that evidence seized from his iPhone should be suppressed because he was asked for, and he provided, the passcode to the phone without being advised of his Miranda rights. *United States v. Djibo*, 2015 WL 9274916, at \*2 (E.D.N.Y. Dec. 16, 2015). One of the bases on which the government opposed defendant’s motion was that the records he sought to suppress would have been discovered using the passcode bypass technology that HSI possessed. *Id.* at \*5.

seeking device connection and Internet Protocol address logs for Feng's iPhone, which Apple provided. The government never sought orders to obtain a log of the remote wipe request on Feng's iPhone or to obtain other potentially useful information pursuant to 18 U.S.C. § 2703(d).

**D. Following Mr. Feng's Guilty Plea, The Government Continues Its Efforts To Compel Apple To Extract Data From His iPhone.**

On October 29, 2015, without the government or Apple having extracted any information from Feng's iPhone, Feng pled guilty to conspiracy to distribute and possess with intent to distribute methamphetamine. *Yang*, 14-CR-387 (MKB), DE 119.

A day later, in response to a notification from the government that the defendant had pled guilty, Judge Orenstein ordered the government to explain why its application was not mooted by Feng's plea. *See* DE 25. The government responded the same day, asserting for the first time that investigation into the drug-trafficking conspiracy involving Feng was ongoing. *Id.* The government's letter also noted that Feng's case remains open until his sentencing, *see id.*, although it did not explain how any information potentially stored on his iPhone might alter the advisory sentencing guidelines range that would apply to him. *See* DE 29 at 6.

The government took no further action on its application for over three months.<sup>7</sup>

---

<sup>7</sup> In the interim, Apple continued to receive additional demands from the government to extract unencrypted data from a variety of iOS devices in different jurisdictions, all of which invoked the All Writs Act as the basis for courts' authority to issue such orders. *See* DE 27 at 2. Apple objected to performing extraction services on those devices. DE 27 at 2-3. In the recent San Bernardino Matter, the government claimed that the All Writs Act provided authority for the government to compel Apple to create a new operating system to disable security measures on an iOS 9 device. *See* Ex. L [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 1 at 14 (C.D. Cal. Feb. 19, 2016)]. The government subsequently abandoned that demand. While Apple agrees with the government that the San Bernardino Matter is factually distinct, its belated admission that Apple's assistance was not necessary to unlock the iPhone there, at the very least, calls into question the credibility of its contention—wholly unsupported by any evidence in the record—that Apple's assistance is necessary in this case. *See* Ex. C [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 209 (C.D. Cal. Mar. 28, 2016)]; *see also infra* III.D.1.

**E. Judge Orenstein's Opinion.**

On February 29, 2016, in a 50-page order, Judge Orenstein recognized that the All Writs Act cannot be used to compel Apple to perform expert forensic services for the government and denied the government's Initial Application. DE 29.

First, Judge Orenstein concluded that, although the relief sought by the government would be in aid of the Court's jurisdiction, *see* DE 29 at 12-13, and "necessary or appropriate" in light of both the Act's language and relevant case law construing it, *see id.* at 13, the government failed to satisfy the All Writs Act's requirement that the requested relief be "agreeable to the usages and principles of law." *See id.* at 14-30. Adhering to a longstanding canon of statutory construction, Judge Orenstein gave meaning to each word of the clause "agreeable to the usages and principles of law," and concluded that an order issued under the authority of the All Writs Act must comport with other relevant statutes and prior congressional action. *Id.* at 21-24. In doing so, he rejected the government's contention, repeated here, that the phrase "agreeable to the usages and principles of law" empowers the judiciary to issue any order not explicitly prohibited by another Congressional statute. *Id.*

Second, Judge Orenstein analyzed the effect of CALEA on the Court's power to compel Apple, as the creator of Feng's iPhone and iOS 7, to assist the government in bypassing its security features and extracting its encrypted data. DE 29 at 16-21. CALEA imposes certain obligations on "telecommunications carriers" to ensure that their equipment and services permit the government to intercept a subscriber's communications pursuant to a court order. *Id.* at 20. But for entities that are "information services" providers, as defined under CALEA, or that fall outside of CALEA's ambit, Judge Orenstein concluded that the absence of statutory requirements to aid law enforcement reflects a deliberate omission by Congress. *Id.* at 19-20. Judge Orenstein rejected as a violation of separation of powers the government's interpretation

that Congress, by specifically protecting “telecommunications carriers” from a requirement to build an encryption backdoor into their products, otherwise declared open season under the All Writs Act on any entity that did not qualify as a telecommunications carrier. *Id.* at 25-26.

Accordingly, he held that the executive branch could not use the All Writs Act to expand the government’s ability to compel third party assistance with electronic surveillance further than Congress had authorized. *Id.* at 16-20.

Third, Judge Orenstein concluded that even if the All Writs Act permitted the government’s request, that request was nonetheless unlawful under the Supreme Court’s decision in *New York Telephone*. *See* DE 29 at 31. In particular, Judge Orenstein analyzed Apple’s connection to the underlying criminal investigation and concluded that Apple did not facilitate or participate in Mr. Feng’s criminal activity by selling him an iPhone, *id.* at 31-33, had done nothing to thwart the government’s investigation, *id.* at 35, and was not closely related to the investigation as a result of its practice of licensing its iOS operating system to its users, *id.* at 32. Judge Orenstein further concluded that the government’s request would pose an undue burden on Apple, *id.* at 43-44, and that the government had failed to establish that Apple’s assistance was necessary because different government entities had made conflicting statements in this and other proceedings that cast doubt on whether the government actually required Apple’s assistance to access Feng’s iPhone. *Id.* at 45-48.

**F. The Government’s Application To This Court.**

On March 7, 2016, the government filed a brief before this Court, styled as a resubmission of its application, seeking to replace Judge Orenstein’s order. DE 30. The government’s application to this Court seeks the same relief that Judge Orenstein denied under the All Writs Act. DE 30-1 (the “March 7 Application”). As support for the March 7 Application, the government reattached the July 6, 2015 Affidavit of Special Agent Benjamin X.

Yu in Support of Application for a Search Warrant, in which Special Agent Yu identified the information he hoped to obtain from Feng’s iPhone, including “records of communications such as call logs, chats, and text messages” and “things that have been viewed via the Internet.” DE 30-3 ¶¶ 24-25. On April 8, 2016—notwithstanding that the government withdrew its application in the San Bernardino Matter because, contrary to the government’s prior assertions, Apple’s assistance was unnecessary in that case—the government submitted a letter to this Court stating that it would not modify its application. DE 39.

### III. ARGUMENT

#### A. Judge Orenstein’s Order Should Be Reviewed Under The “Clearly Erroneous or Contrary to Law” Standard.

In its papers, the government takes great pains to characterize its brief as a *renewed* application rather than an appeal from Judge Orenstein’s order, presumably to bolster its contention that Judge Orenstein’s order should be reviewed *de novo*. See DE 30 at 12.<sup>8</sup> In doing so, the government attempts to obscure the fact that this matter was extensively briefed, a hearing was held, supplemental briefing was provided, and Judge Orenstein issued a 50-page order. Moreover, the government’s insistence that it is entitled to a do-over is belied by Federal Rule of Criminal Procedure 59 and Section 636 of the Federal Magistrates Act.

Federal Rule of Criminal Procedure 59 prescribes the standards of review to be applied by a district court when considering a challenge to a magistrate judge’s order. Rule 59 distinguishes between “dispositive” orders, which include a “motion to dismiss or quash an indictment or information, a motion to suppress evidence, or any matter that may dispose of a charge or defense,” and “non-dispositive” orders, which encompass “any matter that does not

---

<sup>8</sup> On the docket for the proceedings before Judge Orenstein, however, the government described its application as an “Appeal of Magistrate Judge Decision to [the] District Court.” DE 30.

dispose of a charge or defense,” Fed. R. Crim. P. 59(a)-(b).<sup>9</sup> While *de novo* review is reserved for objections to dispositive orders, nondispositive orders must be reviewed under the “contrary to law or clearly erroneous” standard. Compare Fed. R. Crim. P. 59(b)(3), with Fed. R. Crim. P. 59(a). These standards apply regardless whether the magistrate judge is acting pursuant to § 636(b)(1) of the Federal Magistrates Act or § 636(b)(3), as the government suggests here. See *United States v. Warshay*, 1998 WL 767138, at \*3 (E.D.N.Y. Aug. 4, 1998) (“[Alt]hough § 636(b)(3) prescribes no review procedures, courts have borrowed both the dispositive-nondispositive distinction and the review procedures of subsection (b)(1).”); see also *United States v. Premises Known as 281 Syosset Woodbury Rd.*, 862 F. Supp. 847, 851 (E.D.N.Y. 1994), *aff’d*, 71 F.3d 1067 (2d Cir. 1995).

The government’s search warrant for the devices recovered from Feng’s residence and its subsequent application to compel Apple to bypass the security features on his phone were brought in furtherance of an ongoing criminal case against him, DE 30 at 12, and thus did not dispose of any “charge or defense” in that proceeding. In fact, no charges were disposed of until October 2015 when Mr. Feng pled guilty, while the government’s application was pending. See *Yang*, 14-CR-387 (MKB), DE 119. Because the application and Judge Orenstein’s order did not dispose of any charge or defense, the order’s factual determinations must be reviewed for clear error. See, e.g., *Matter the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157, 162 (D.D.C. 2014) (reviewing for

---

<sup>9</sup> Section 636(b)(1) of the Federal Magistrates Act also distinguishes between dispositive matters (“a motion for injunctive relief, for judgment on the pleadings, for summary judgment, to dismiss or quash an indictment or information . . . to dismiss for failure to state a claim upon which relief can be granted, and to involuntarily dismiss an action,” 28 U.S.C. § 636(b)(1)(A) and nondispositive “pretrial matter[s],” *id.* § 636(b)(1). Consistent with Rule 59, nondispositive pretrial matters may be reconsidered only “where it has been shown that the magistrate judge’s order is clearly erroneous or contrary to law.” *Id.* § 636(b)(1)(A).

clear error); *In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 2006 WL 2871743, at \*1 (E.D. Wis. Oct. 6, 2006) (same); *see also New York v. Mountain Tobacco Co.*, 953 F. Supp. 2d 385, 389 (E.D.N.Y. 2013); E.D.N.Y. Loc. Crim. R. 59.1(c) (applying E.D.N.Y. Local Civil Rule 72.1 in criminal proceedings).<sup>10</sup>

**B. The All Writs Act Does Not Authorize The Order The Government Seeks Here.**

The government contends that the All Writs Act should be broadly construed to “permi[t] a court, in its ‘sound judgment,’ to issue orders necessary ‘to achieve the rational ends of law’ and ‘the ends of justice entrusted to it.’” DE 30 at 14 (quoting *N.Y. Tel.*, 434 U.S. at 172-73). One struggles to find any limiting principle in that account of the Act’s scope. But the government goes even further, urging the Court to wield this power “flexibly.” *Id.* Applying its boundless construction of the All Writs Act to this case, the government asserts that courts have authority to issue ancillary orders to third parties to facilitate the execution of search warrants, subject only to two limitations: (1) that the order does not impose an “unreasonable burden” (*id.*

---

<sup>10</sup> Two of the cases cited by the government for the proposition that *de novo* review applies contain no analysis of the proper standard of review and do not cite to Rule 59 or § 636. *See In re Application of the U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Tel.* (“*Certain Cellular Telephone*”), 460 F. Supp. 2d 448, 454 (S.D.N.Y. 2006); *see also In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information* (“*Historical Cell Information*”), 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011). And while the third case states that cases decided under § 636(b)(3) are subject to *de novo* review, it does so without acknowledging the distinction between dispositive and nondispositive matters, and wholly ignores authority holding that this distinction applies even when a case is brought under § 636(b)(3). *See In re Application of the U.S. for an Order of Nondisclosure* (“*Order of Nondisclosure*”), 41 F. Supp. 3d 1, 3 (D.D.C. 2014); *cf. Warshay*, 1998 WL 767138, at \*3. Moreover, each of these cases involved requests for a warrant *prior to the charging of any criminal defendant*. Accordingly, unlike this case, there was no underlying criminal case subject to the ongoing supervision and control of a district judge, *cf.* DE 30 at 12 (“This Court retains . . . ‘supervision and control’ of matters delegated to magistrate judges in connection with the Feng investigation.”), meaning that the magistrate judge’s opinion was the final disposition of the legal action concerning the investigation, *see Order of Nondisclosure*, 41 F. Supp. at 3 (concerning grand jury subpoena); *Historical Cell Information*, 809 F. Supp. 2d at 114 (concerning cell-site location records); *Certain Cellular Telephone*, 460 F. Supp. 2d at 448 (seeking prospective cell-site location data).



at 15), and (2) that Congress has not “express[ly] or implied[ly] prohibit[ed] the requested relief” (*id.* at 26). In the government’s account, however, these are no limitations at all. Congress simply cannot be expected to preemptively prohibit every overreaching order the government might dream up in furtherance of a valid warrant. The Court should reject the government’s interpretation of the Act as inconsistent with the statute’s text, history, and relevant precedent. By its terms, the All Writs Act authorizes federal courts to issue “all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a). The Act’s reference to “writs” “agreeable to the usages and principles of law” is understood to refer to “traditional writs that have not been altered or abolished by some other statute.” *Lowery v. McCaughtry*, 954 F.2d 422, 423 (7th Cir. 1992). Underscoring the Act’s close connection to the common law, the Act specifically referenced two of the most well-known common law writs, *habeas corpus* and *scire facias*. See An Act to Establish the Judicial Courts of the United States, § 14, 1 Stat. 81 (1789). The Act thus grants federal courts power to issue the established common law writs in use at the time of the American Founding, such as, *inter alia*, *certiorari*, *mandamus*, *quo warranto*, and *capias*. See Edward Jenks, *The Prerogative Writs in English Law*, 32 Yale L.J. 523, 527-34 (1923); F.W. Maitland, *The History of the Register of Original Writs*, 3 Harv. L. Rev. 97 (1889) (describing the “*Registran Brevium*—the register of writs current in the English Chancery”). Accordingly, “[i]n determining what auxiliary writs are ‘agreeable to the usages and principles of law,’ [the Court] look[s] first to the common law.” *United States v. Hayman*, 342 U.S. 205, 221 n.35 (1952). Indeed, the government concedes the phrase “agreeable to the usages and principles of law” “refers to the collection of historical writs that formed the basis of English and early

American legal systems.” DE 30 at 29 (citing *Bank of U.S. v. Halstead*, 23 U.S. (10 Wheat.) 51 (1825)).

Because the Act is grounded in the common law, it cannot be construed as a “grant of plenary power to the federal courts” or to “give the district court a roving commission” to order private parties to assist the government. *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). Rather, as Judge Orenstein recognized, it “function[s] as a ‘gap filler,’” DE 29 at 14, that “suppl[ies] the courts with the instruments needed to perform their duty,” *Harris v. Nelson*, 394 U.S. 286, 300 (1969); *see also Trenkler v. United States*, 536 F.3d 85, 97 (1st Cir. 2008). For example, Congress has authorized courts to issue “the writ of *habeas corpus ad testificandum*,” such that a “court may direct the custodian to produce the prisoner in court as a witness.” *Ivey v. Harney*, 47 F.3d 181, 183 (7th Cir. 1995). But “[w]at happens if the testimony takes two days? Where does the prisoner stay overnight? . . . The statute does not say; neither, however, does it subtract from the court’s common law powers to control such details.” *Id.* In this instance, the All Writs Act would fill the gap as a “residual source of authority” empowering the court “to issue writs that are not otherwise covered by [the] statute.” *Clinton v. Goldsmith*, 526 U.S. 529, 537 (1999) (internal quotation marks omitted).

The order the government seeks here, which would require Apple to take possession of and use its own technology to extract data from a device over which it has no custody or control, is neither grounded in the common law nor authorized by statute. *See infra* III.C. The government suggests that Apple conceded before Judge Orenstein that the order sought here has “a close enough antecedent in the common law,” DE 30 at 30 (quoting DE 29 at 14 n.10), but Apple made no such concession. On the contrary, Apple consistently argued that the All Writs Act does not authorize the requested order. DE 16 at 4-8. The government is thus incorrect

when it insists that there is “no dispute between the parties that the writ sought herein” is “agreeable to the usages and principles of law . . . .” DE 30 at 30.

The government is also incorrect when it contends that *Halstead* “fatally undermines” Judge Orenstein’s interpretation of the All Writs Act. DE 30 at 31. The “principal inquiry” in that case was “whether the laws of the United States authorize the Courts . . . to alter the form of the process of execution, which was in use in the Supreme Courts of the several States in the year 1789, [so] as to uphold the *venditioni exponas* issued in this cause.” *Halstead*, 23 U.S. (10 Wheat.) at 54-55.<sup>11</sup> The question arose because the Process Act of 1792 provided that “the forms of writs and executions, and modes of process, in the Circuit and District Courts, in suits at common law, shall be the same in each State respectively, as are *now* used or allowed in the Supreme Courts of the same,” *id.* at 57, *and* that this limitation was “subject . . . to such alterations and additions, as the said Courts respectively shall, in their discretion, deem expedient” *id.* at 58. Interpreting these provisions, the Court explained that federal courts “have authority . . . from time to time to alter the process, in such manner as they shall deem expedient, and likewise to make *additions* thereto, which necessarily implies a power to enlarge the effect and operation of the process.” *Id.* at 60. The Court rejected the argument that modifying the forms of the writ and the modes of process was an improper “exercise of legislative power,” because the limited “power given to the Courts over their process is no more than authorizing them to regulate and direct the conduct of the Marshal, in the execution of the process.” *Id.* at 61. The narrow holding of *Halstead* was thus that the “operation of an execution” was not

---

<sup>11</sup> A writ of execution is a common law writ that a court issues directing a law enforcement officer to sell property in satisfaction of a judgment. *See Halstead*, 23 U.S. (10 Wheat.) at 55 (“That executions are among the writs hereby authorized to be issued, cannot admit of a doubt . . . .”); *Wayman v. Southard*, 23 U.S. 1, 22 (1825) (“An execution is a writ, which is certainly ‘agreeable to the principles and usages of law.’”).

limited “to that which it would have had in the year 1789[.]” *Id.* at 62; *cf. Beers v. Haughton*, 34 U.S. (9 Pet.) 329, 360 (1835) (explaining that the practical result in *Halstead* was that a writ of execution “may reach property not liable, in 1789, by the state laws to be taken in execution, or may exempt property, which was not then exempted, but has been exempted by subsequent state laws”).

The authority to alter the *forms* and *process* of traditional common law writs is not authority to invent new writs with no common law analogue. But that is precisely what the government is asking the Court to do here—to issue an order with no common law analogue, directing an unrelated third party to use its own technological know-how to extract data from a device in the government’s possession. *Cf. Ivey*, 47 F.3d at 185 (reversing order issued under the All Writs Act because “[n]othing in the common law supports an order directing a third party to provide free services that facilitate litigation”).<sup>12</sup> The Court should reject the government’s “call[] for ‘creative’ use of federal judicial power” lacking any foundation in the common law. *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 40 (1985); *cf. Ivey*, 47 F.3d at 185 (considering “hypothetical parallel[s]” showing that petitioner’s reading of the All Writs Act would allow the court to issue all sorts of orders not allowed at common law).

The government’s legal authorities are not to the contrary, as they overwhelmingly involve All Writs Act orders addressed to third parties whose facilities were being used to

---

<sup>12</sup> In fact, the requested order is akin to an injunction directing specific performance of a personal services contract, a remedy the common law specifically disfavored. *See* Restatement (Second) of Contracts § 367 (“A promise to render personal service will not be specifically enforced”); *Virginian Ry. Co. v. Sys. Fed’n No. 40*, 300 U.S. 515, 550 (1937) (“Equity will not . . . compel one to enter into performance of a contract of personal service which it cannot adequately control.”).

facilitate suspected ongoing criminal activity,<sup>13</sup> and where the information being sought was in the third parties' possession.<sup>14</sup> DE 30 at 16; *see infra* III.D.2. Unlike the order requested here, these writs fit squarely within the common law tradition. As the government notes, courts may issue orders to third parties outside of the law enforcement context where the plaintiff demonstrates that the defendant is using the third party's facilities to violate the plaintiff's rights. DE 30 at 16 n.3 (discussing All Writs Act orders to third parties to support injunctive relief). And there is nothing novel about requiring a third party to produce documents or records in its possession for use in a criminal case. *See, e.g., United States v. Burr*, 25 F. Cas. 30, 30-37 (C.C.D. Va. 1807) (holding that subpoena *duces tecum* could be issued to President Jefferson directing him to produce, *inter alia*, a letter he received from General Wilkinson with potential relevance to Burr's criminal case). What courts have *not* historically had the authority to do is order a third party to use its proprietary technological know-how to help the government access information that is already in *the government's possession*.

To be sure, courts have previously issued *ex parte* orders directing Apple to "assist in extracting data from an Apple device through bypassing the passcode in order to execute a

---

<sup>13</sup> *See In re Application of U.S. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder*, 610 F.2d 1148, 1155 (3d Cir. 1979) (suspects using company's phone lines in furtherance of criminal enterprise); *In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1123-24 (9th Cir. 1980) ("*Mountain Bell*") (same).

<sup>14</sup> *See United States v. Doe*, 537 F. Supp. 838, 839 (E.D.N.Y. 1982) (ordering phone company to produce toll records because they could "reveal the present whereabouts of the subscriber's daughter"); *United States v. X*, 601 F. Supp. 1039, 1040 (D. Md. 1984) (ordering production of toll records believed to be "of critical importance in locating defendant X"); *United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (ordering credit card company to produce records of customer believed to be harboring a fugitive); *In re Application of U.S. for an Order Directing X to Provide Access to Videotapes* ("*Videotapes*"), 2003 WL 22053105, at \*1, \*3 (D. Md. Aug. 22, 2003) (ordering third party "merely to provide access to surveillance tapes already in existence, rather than any substantive assistance" so that the government could "locate defendant Y and . . . execute a warrant for [his/her] arrest").

search warrant.” DE 30 at 17 (citing cases). But the government’s cited orders were issued *ex parte*, without Apple’s participation, without the benefit of adversarial briefing on the scope of the All Writs Act, and with no supporting analysis. Apple also was not a party in *United States v. Blake*, No. 13-CR-80054 (S.D. Fl. July 14, 2014), in which the court denied the defendant’s motion to suppress evidence gathered from an iPhone that Apple helped unlock. Accordingly, such cases are not even persuasive authority on the scope of the All Writs Act, let alone precedential; certainly such *ex parte* orders issued with little analysis should carry less weight than Judge Orenstein’s lengthy and reasoned opinion.<sup>15</sup>

Because the order the government seeks goes well beyond the common-law powers authorized by the All Writs Act, and the All Writs Act confers interstitial rather than plenary authority, the Court can only grant the government’s requested relief if some other statute provides it with such authority. There is no such statute here. To the contrary, the relief the government seeks is inconsistent with existing statutory authority.

**C. The Government’s Request Is Inconsistent With CALEA And The Comprehensive Statutory Framework Of Which It Is A Part.**

In attempting to expand the limited scope of the All Writs Act, the government seeks authority that Congress has expressly and impliedly rejected through CALEA, 47 U.S.C. § 1001 *et seq.*, and the comprehensive legislative scheme of which CALEA is a part.

---

<sup>15</sup> The only court that did assess the scope of the All Writs Act in connection with a request to order a third party to unlock a cellular phone misread New York Telephone as standing for the proposition that a third party’s assistance can be compelled whenever it has the ability to unlock a phone because its decision not to do so would “frustrate” the government’s search efforts. See *In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant by Unlocking a Cellphone*, 2014 WL 5510865, at \*2 (S.D.N.Y. Oct. 31, 2014) (quoting *N.Y. Tel.*, 434 U.S. at 174). But if that were the rule, the government could conscript any third party with the ability to assist a search in any way on the ground on the ground that refusing to assist would “frustrate” law enforcement’s efforts. That is not the law.

**1. CALEA Specifically Exempts Information Service Providers From Having To Create Or Maintain Systems To Facilitate Government Access.**

CALEA specifies the types of private companies that can be compelled to assist the government in accessing communications, the circumstances in which such assistance can be compelled, and the form that compulsory assistance may take—and it expressly excludes Apple, which serves as an “information services” provider, from being conscripted by law enforcement to provide it with access to stored communications. *See* 47 U.S.C. § 1001 *et seq.*

In drafting and enacting CALEA, Congress sought to ensure that “government surveillance authority is *clearly defined and appropriately limited*,” H.R. Rep. No. 103-827(I), at 17 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3497 (emphasis added), and to “balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies,” *id.* at 13, 1994 U.S.C.C.A.N. at 3493.

In keeping with these principles, CALEA requires “telecommunications carriers” to ensure that their “equipment, facilities, or services” enable the government to intercept communications pursuant to a court order or other lawful authorization. 47 U.S.C. § 1002. Expressly excluded from CALEA’s definition of “telecommunications carrier” are persons or entities providing “information services,” *id.* § 1001(8), a term CALEA defines to include “electronic messaging services” and services that “permit[] a customer to retrieve stored information from, or file information for storage in, information storage facilities,” *id.* § 1001(6)(B)(i), (iii). CALEA thus reflects Congress’s deliberate decision to exclude services that facilitate “information storage” from being forced to assist in government surveillance or accessing electronic information.

As relevant to the government's request in this case, Apple is an information services provider. In particular, FaceTime, iMessage, and Mail are all features of iOS 7 that serve as electronic messaging services that permit users to communicate and store passcode-protected electronic communications. *See* DE 29 at 20 (Judge Orenstein observing that "information services" provider is broadly defined in CALEA and "easily encompasses Apple"). The government attempts to avoid this reality by insisting that Apple should not be considered an "information services" provider for purposes of this case because Apple's only relevant role is as the "manufacturer of a consumer device." DE 30 at 19-21. But the government's position is inconsistent with its own admission that the requested order is intended to facilitate "access to [the device's] *contents*," *id.* at 4 (emphasis added), which the government expressly describes as "records of communications such as call logs, chats and text messages" and "things that have been viewed via the Internet," DE 30-3 ¶¶ 24-25; *see also* DE 30 at 34 (asserting the defendant facilitated drug deals by using his phone to make calls, send text messages, and chat). In other words, what is at issue in this case is access to communications that were exchanged using messaging services and information storage that Apple provides to its users in its capacity as an information services provider.

Finally, while insisting that Apple is merely a "manufacturer" for purposes of its CALEA analysis, *see* DE 30 at 20, the government relies on the very features that make Apple an information services provider to argue that Apple is not "too far removed" from this case in its *New York Telephone* analysis, *id.* at 34-35. The government cannot have it both ways. Because the assistance the government requests here implicates Apple's role as an information services provider, CALEA controls. Thus, Apple cannot be required to facilitate law enforcement access



to its information services—in real-time or after such communications are stored on a user’s passcode-protected device. *See* 47 U.S.C. § 1001(6)(B)(i).

**2. Congress’s Comprehensive Statutory Scheme Addressing Third Party Assistance In Accessing Communications Delineates The Exclusive Means By Which Courts May Compel Such Assistance.**

The government concedes that Congress can either “explicitly or implicitly” bar certain All Writs Act orders, DE 30 at 18, but nevertheless insists that its request in this case is permissible because there is no statute that *specifically* provides “procedures for requiring any device manufacturer, such as Apple, to extract data from a passcode-locked phone,” *id.* at 19. It is difficult to reconcile the government’s concession that Congress can “implicitly” bar certain All Writs Act orders with its insistence that Congress must speak with such specificity. Moreover, the government’s demand for congressional precision in this case is at odds with the longstanding principle that statutes within a legislative scheme must be interpreted as part of “a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into [a] harmonious whole.” *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) (citations and internal quotation marks omitted).

Here, the “comprehensive legislative scheme” of which CALEA is a part specifically “prescribe[s] the extent to which law enforcement may secure access to a wide array of data—both ‘in motion’ and ‘at rest’—[and imposes] obligations [on] some private entities but not others to provide affirmative assistance” to law enforcement. DE 29 at 20. In delineating the acceptability of certain government requests relating to surveillance and access to data, that scheme is “so comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the statute does not affirmatively prescribe.” *Id.* at 15-16; *cf. Trenkler*, 536 F.3d at 97 (“[W]hen a statute . . . specifically addresses a particular *class of claims or issues*, it is that statute, not the All Writs Act, that takes precedence.”) (emphasis added).

Thus, even if CALEA did not expressly bar the government from demanding Apple's assistance (and it does), the court is *impliedly* prohibited from compelling such assistance by the absence of any legal authorization in the comprehensive statutory scheme of which CALEA is a part.

The legislative scheme governing third party technical assistance for government surveillance and data collection efforts was developed over the course of decades and includes several congressional enactments, each of which identifies certain kinds of entities whose assistance can be compelled, the circumstances in which such assistance can be demanded, and the kind of assistance that can be required. *See* CALEA, 47 U.S.C. § 1002; Pen/Trap Statute, 18 U.S.C. § 3123(b)(2) (permitting the government to compel a third party to furnish “information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device”); Wiretap Act, 18 U.S.C. § 2518(4) (permitting the government to compel a third party to furnish “all information, facilities, and technical assistance necessary to accomplish the interception” of a “wire, oral, or electronic communication”); Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2511(2)(a)(ii) (amending the Wiretap Act to authorize “providers of wire or electronic communication service” “to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance”); Stored Communications Act (“SCA”), 18 U.S.C. § 2703(a) (providing that the government “may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant”).<sup>16</sup>

---

<sup>16</sup> The parties agree that the ECPA, the SCA, the Wiretap Act, and the Pen/Trap Statute do not expressly cover the government's specific request in this case. *See* DE 30 at 22-23.

In addition to conferring certain, specific powers on law enforcement, these statutes include express limitations on compulsory third party assistance, thereby demonstrating Congress's deliberate effort to limit the scope of lawful third party conscription. CALEA, for example, explicitly *excludes* "information services" providers from its ambit, *see supra* III.C.1, while limiting what law enforcement can demand of both "telecommunications carriers" and "electronic communication service" providers.<sup>17</sup> Specifically, law enforcement cannot require "electronic communication service" providers to adopt "any specific design of equipment, facilities, services, features, or system configurations" to facilitate government access. 47 U.S.C. § 1002(b)(1)(A). Moreover, the SCA details when governmental entities can require providers of electronic communications and remote computing services to *produce* stored content to the government, but it does not obligate them to provide technical assistance. 18 U.S.C. § 2703(a), (b). Importantly, the SCA is limited to information held or maintained (in electronic storage, or otherwise) on the providers' systems and does not impose obligations on providers to assist the government in retrieving information stored on private computers or other devices. *Id.*

When viewed collectively, the requirements and limitations included in these statutes comprehensively specify the third parties from which the government can seek technical assistance and the kinds of assistance it can require. This framework is not, as the government contends, an "incomplete patchwork of statutes," DE 30 at 24; rather, as Judge Orenstein recognized, it is a highly complex legislative scheme in which both express provisions and omissions reflect Congress's reasoned compromise between the competing interests of third parties and law enforcement, DE 29 at 20. These deliberate policy choices, and the careful

---

<sup>17</sup> The term "electronic communication service" is broadly defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 47 U.S.C. § 1001(1); 18 U.S.C. § 2510(15).

balance struck by Congress, cannot be swept aside simply because the government finds it more convenient. *Cf. Pa. Bureau of Corr.*, 474 U.S. at 43 (the All Writs Act does not empower federal courts “to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate”).

The government fails to grasp the scope and import of this statutory framework, insisting that CALEA is merely “tangential,” DE 30 at 25, and likening the legislative scheme at issue here to the one in *New York Telephone*, in which the Supreme Court compelled a public telephone company to assist in setting up a pen register to intercept communications prior to Congress’s enactment of the Pen Register statute, *id.* at 25-26. There, the Court reasoned that because the Wiretap Act required third party assistance in intercepting wire communications, “it would be remarkable if Congress thought it beyond the power of the federal court to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy.” *N.Y. Tel.*, 434 U.S. at 176-77. Because the order was “consistent with the intent of Congress,” the Court did not need to wait for Congress to “fill in” a gap when requiring third parties to assist in setting up lawful pen traps. *Id.* at 172. Here, by contrast, the government is not asking the Court to “fill in” a statutory gap through an order that is less invasive than those explicitly authorized; it is asking the Court to circumvent CALEA’s express limitations and go beyond any statutory authorization currently on the books. Thus, unlike the order in *New York Telephone*, the government’s demand here is demonstrably *inconsistent* “with the intent of Congress.” *Id.*<sup>18</sup>

---

<sup>18</sup> Moreover, to the extent this area of law may have been a “patchwork” of statutes at the time *New York Telephone* was decided, it has since been expanded into a comprehensive scheme, and Congress continues to legislate actively in this area. *See* Pen/Trap Statute, Pub. L. No. 99-508, 100 Stat. 1848, 1869-70 (1986) (enacting 18 U.S.C. § 3123(b)(2)); Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783, 1796-97 (1978) (adding third party

The government nonetheless insists that the statutory scheme in this case is not sufficiently comprehensive, but its only support for this assertion is a collection of inapposite preemption cases. DE 30 at 25 (citing *Gonzalez v. Raich*, 545 U.S. 1, 10, 15 (2005) (describing the detailed federal scheme regulating marijuana in the context of assessing Congress’s Commerce Clause powers); *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 351 (1984) (concluding that because Congress’s intent to preclude judicial review of agency action was “fairly discernible” from the detail of a legislative scheme, it overcame a contrary presumption); *Arizona v. United States*, 132 S. Ct. 2492, 2500-01 (2012) (explaining that, under the Supremacy Clause and federalism principles, the field preemption doctrine applies to “a field in which Congress has left no room for States to regulate”).

The government characterizes the limits on courts’ authority to issue orders under the All Writs Act—including orders directing a third party to unlock a phone in the government’s possession—as exceedingly narrow, contending that any order is permissible so long as “that specific relief” has not been “explicitly or implicitly prohibited by law.” DE 30 at 18. But the cases the government cites—*Pennsylvania Bureau of Correction, New York Telephone*, and *United States v. Barret*, 178 F.3d 34 (1st Cir. 1999), *id.*, say no such thing. Rather, those cases stand only for the unremarkable proposition that an otherwise lawful writ may not be issued where Congress has affirmatively prohibited it. *Cf. Trenkler*, 536 F.3d at 97 “[W]hen a statute . . . specifically addresses a particular class of claims or issues, it is that statute, not the All Writs Act, that takes precedence.”). None of the government’s cases (or any other case) holds that the All Writs Act gives courts *carte blanche* to issue any order the government might request when

---

language to 18 U.S.C. § 2511(2)(a)(ii)); ECPA, Pub. L. No. 99-508, 100 Stat. at 1849-51 (amending same); SCA, Pub. L. No. 99-508, 100 Stat. at 1861 (enacting 18 U.S.C. § 2703); USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 274, 283 (2009) (amending same).

Congress has remained silent (which, in any event, is not the case here). On the contrary, in the face of congressional silence, the court must “look . . . to the common law” to determine whether a writ is “agreeable to the principles and usages of law.” *Hayman*, 342 U.S. at 221 n.35. As previously discussed, *see supra* III.B, the type of writ the government seeks here is wholly foreign to the common law and is therefore unavailable under the All Writs Act.

### **3. Use Of The All Writs Act Would Usurp Congressional Authority.**

Congress has continued to consider the scope of permissible government impositions on third parties, and the Court should not allow the All Writs Act to be used to invade the province of the legislature. The Supreme Court in *New York Telephone* recognized the role of congressional intent in its All Writs Act analysis, relying on the fact that its order was “consistent with the intent of Congress” and with “recent congressional actions.” 434 U.S. at 172, 176. Here, Congress has considered but declined to enact legislation to provide the government the very authority it seeks in these proceedings. This silence, when viewed in the context of the existing statutory scheme regarding electronic surveillance and third party assistance to law enforcement in accessing communications, is not meaningless or indicative of a “gap” to be filled by the All Writs Act. Rather, it reflects a deliberate legislative decision reflecting Congress’s carefully calibrated balance of third party and law enforcement interests.

The government wrongly asserts that legislative intent can never be discerned from an absence of affirmative legislation. *See* DE 30 at 26-27. While silence can be a weak indicator of congressional intent in some circumstances, it is a different story altogether when Congress actively considers legislation to address a major policy issue but deliberately declines to enact it.

Here, Congress opted to require certain third party assistance through several different enactments designed to aid law enforcement in gathering electronic evidence (although none as expansive as what the government seeks here), but it has declined to include similar provisions in

other statutes, despite vigorous lobbying by law enforcement and notwithstanding its “prolonged and acute awareness of so important an issue” as the one presented here. *Bob Jones Univ. v. United States*, 461 U.S. 574, 601 (1983). Accordingly, the lack of statutory authorization in CALEA or any of the complementary statutes in the “comprehensive federal scheme” of surveillance and telecommunications law speaks volumes. *P.R. Dep’t of Consumer Affairs v. Isla Petrol. Corp.*, 485 U.S. 495, 503 (1988) (“Where a comprehensive federal scheme intentionally leaves a portion of the regulated field without controls, *then* the preemptive inference can be drawn—not from federal inaction alone, but from inaction joined with action.”).

That the Executive Branch recently abandoned plans to seek legislation expanding CALEA’s reach provides additional confirmation that Congress has not acceded to the government’s wishes, and belies the government’s view that courts have possessed authority to issue these types of orders under the All Writs Act since 1789.<sup>19</sup> Although the Administration is free to keep its powder dry for future lobbying efforts, it cannot use the courts to rewrite federal legislation or circumvent legislative intent. As explained above, CALEA prohibits compelling Apple to assist the government in the manner it seeks here, and this Court should decline the government’s invitation to violate the separation of powers by usurping Congress’s

---

<sup>19</sup> Federal officials familiar with that failed lobbying effort confirmed that the FBI had in fact developed a “draft proposal” containing a web of detailed provisions, including specific fines and compliance timelines, and had floated that proposal with the White House. *See* Ex. M [Ellen Nakashima, *Proposal Seeks To Fine Tech Companies for Noncompliance with Wiretap Orders*, Wash. Post (Apr. 28, 2013)]. As *The Washington Post* reported, advocates of the proposal within the government dropped the effort, because they determined they could not get what they wanted from Congress at that time: “Although ‘the legislative environment is very hostile today,’ the intelligence community’s top lawyer, Robert S. Litt, said to colleagues in an August [2015] e-mail, which was obtained by The Post, ‘it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement.’ There is value, he said, in ‘keeping our options open for such a situation.’” Ex. N [Ellen Nakashima & Andrea Peterson, *Obama Faces Growing Momentum to Support Widespread Encryption*, Wash. Post (Sept. 16, 2015)].

“exclusive constitutional authority to make laws.” *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 588-89 (1952); *see* DE 29 at 12.<sup>20</sup>

The government’s reliance on *FTC v. Dean Foods Co.*, 384 U.S. 597 (1966), DE 30 at 28-29, is misguided, as that case concerned the powers of the Federal Trade Commission, not the powers of courts under the All Writs Act, 384 U.S. at 609. Similarly inapposite are *United States v. Craft*, 535 U.S. 274 (2002), and *Zino Davidoff SA v. CVS Corp.* 571 F.3d 238 (2d Cir. 2009), which the government invokes for the unremarkable proposition that, oftentimes, several different equally tenable conclusions can be drawn from failed legislation, including that Congress thought existing legislation already encompassed the proposed enactment.<sup>21</sup> *See Craft*, 535 U.S. at 287; *Zino*, 571 F.3d at 243 (explaining that a failed attempt to amend the Lanham Act “to state a proposition with unmistakable clarity tells nothing about whether the preexisting [trademark] law already covered the point, albeit less clearly”). Such an inference is not tenable here, where Congress has faced sustained lobbying efforts, opted to provide and withhold authorizations in a “comprehensive federal scheme” of surveillance and telecommunications

---

<sup>20</sup> The government relies on several inapposite cases to argue that failed legislation universally lacks significance. *See* DE 30 at 27-28 (citing *INS v. Chadha*, 462 U.S. 919 (1983) (stating the uncontroversial proposition that laws cannot be passed without bicameralism and presentment, without discussing the import of legislative silence for interpreting congressional intent); *United States v. Estate of Romani*, 523 U.S. 517, 535 (1998) (Scalia, J., concurring) (criticizing the majority for analyzing the impact of rejected legislation); *Bowsher v. Synar*, 478 U.S. 714, 733-34 (1986) (holding that when Congress reserved to itself the ability to act without passing additional legislation, it unconstitutionally impinged on the role of the executive)).

<sup>21</sup> The same is true of *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), which the government cites to highlight the difficulty of discerning congressional intent from anything other than enacted law. DE 30 at 27-28. *Clapper* involved a failed amendment that would have expressly provided for judicial review, but the fact that the amendment failed to pass was not probative because the amendment “encompassed more than the issue of judicial review” and did not contemplate the particular circumstances in which judicial review was sought in that case. 785 F.3d at 807.



statutes, *Isla Petroleum*, 485 U.S. at 503, actively debated granting the requested powers, and made an affirmative decision not to do so, *see Bob Jones*, 461 U.S. at 601.

**D. The Government’s Request Is Not Authorized By *New York Telephone*.**

As Judge Orenstein observed, the government’s request for assistance is based on a construction of the All Writs Act that would “open[d] the separation of powers,” DE 29 at 26, and “cast doubt on the [Act]’s constitutionality if adopted.” *Id.* at 12. The Court can avoid that constitutional thicket by deciding this case on narrower grounds. *See, e.g., Greater New Orleans Broad. Ass’n v. United States*, 527 U.S. 173, 184 (1999). Indeed, even assuming that the All Writs Act can be invoked here (and it cannot as a matter of law, *see supra* III.B & III.C), the relief the government seeks is foreclosed by *New York Telephone*.

In that case, the district court had issued an order requiring the telephone company to provide the government with use of an otherwise unused telephone line so that the government could install a pen register on two lines that “had been, were currently being, and would continue to be used” in connection with an ongoing gambling enterprise. *N.Y. Tel.*, 434 U.S. at 162. The Supreme Court found the order authorized by the All Writs Act and “consistent with the intent of Congress.” *Id.* at 172; *see also id.* at 176-77 (Congress “clearly intended” to provide for third party assistance with respect to pen registers, given statute providing for assistance with respect to Title III wiretaps).<sup>22</sup> Although the Court cautioned that “the power of federal courts to impose duties upon third parties is not without limits,” *id.*, it upheld the district court’s exercise of discretion for three reasons. *First*, the company’s assistance was necessary, as without it “there [was] no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished.” *Id.* at 175. *Second*, it observed that it “d[id] not think that the

---

<sup>22</sup> In contrast, as described *supra* III.B & III.C, the relevant statute, legislative history, and legislative scheme evince Congress’s intent that the requested order *not* be available.

Company was a third party so far removed from the underlying controversy that its assistance could not be permissibly compelled,” especially given that “the Company’s facilities were being employed to facilitate a criminal enterprise on a continuing basis.” *Id.* at 174. *Third*, the Court ruled that the “order [was not] in any way burdensome” because the assistance sought was “meager” and the company was “a highly regulated public utility” for whom the use of pen registers was “by no means offensive to it.” *Id.* at 174-75. In all of these respects, *New York Telephone* forecloses the government’s request in this case.

**1. The Government Has Utterly Failed To Demonstrate Necessity.**

It is well established that a third party cannot be compelled to assist the government unless it demonstrates that the third party’s participation is essential. *See N.Y. Tel.*, 434 U.S. at 164 n.5; *see also Plum Creek*, 608 F.2d at 1289-90 (denying All Writs Act application because “there has been no showing that the object to be achieved could not have been accomplished by using non-company employees”). In *New York Telephone*, the Court issued the order authorizing installation of a pen register only after observing that the FBI had conducted “an exhaustive search” and “was unable to find a location where it could install its own pen registers without tipping off the targets of the investigation.” 434 U.S. at 175. Accordingly, the telephone company’s participation was “essential to the fulfillment of the purpose” of the warrant—“there [was] *no conceivable way*” to install the pen register in an undetectable location without the company’s assistance. *Id.* (emphasis added); *see also Mountain Bell*, 616 F.2d at 1129 (compelling third party to assist with tracing was necessary to carry out a wiretap—otherwise the tracing operation would be “completely frustrated”); *Mich. Bell Tel. Co. v. United States*, 565 F.2d 385, 389 (6th Cir. 1977) (telephone company was “the only entity that c[ould] effectuate the order . . . to prevent company-owned facilities from being used in violation of both state and federal laws”).

Here, the government has failed to demonstrate that it has conducted an “exhaustive search” for alternative options to obtain the data from Feng’s iPhone by any means other than compelling Apple to extract the data.<sup>23</sup> *First*, the government has not made any showing that it sought or received technical assistance from federal agencies with expertise in digital forensics. *See* Tr. 34-35. In fact, the government has failed to make any showing that it consulted non-intelligence agencies, and all but conceded to Judge Orenstein that it has not attempted to obtain such assistance from intelligence agencies, opting instead to insist that “federal prosecutors don’t have an obligation to consult the intelligence community in order to investigate crime.” Tr. 36.

*Second*, despite submitting a declaration in the San Bernardino Matter acknowledging that certain third parties have the ability to circumvent passcodes and other security mechanisms in different iPhone operating systems, *see* Ex. O [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 149-3, Decl. of Stacey Perino ¶ 28(a)-(e) (C.D. Cal. Mar. 10, 2016)], the government has made no showing that it has consulted any such third parties (or others) *in this case* and determined that Apple is the “only entity” that could “effectuate” the search warrant here. *See Mich. Bell*, 565 F.2d at 389. In its brief, the government asserts that it “has explored the possibility of using third party technologies but has determined that using such technology . . . presents the [] risk of triggering the auto-erase feature.” DE 30 at 41. But it only describes communications with one government agent—who was brought to the government’s attention by Judge Orenstein, Tr. 33—about one potential third party solution, *see* DE 30 at 43; *United States v. Djibo*, 2015 WL 9274916, at \*6 (E.D.N.Y. Dec. 16, 2015) (discussing a tool that successfully

---

<sup>23</sup> While the government has argued in its briefing that it needs Apple’s help, *see, e.g.*, DE 1 at 1; DE 15 at 20-21; DE 30 at 10, those statements are not evidence. And, to date, no one from the DEA, let alone a forensic agent, has corroborated those assertions via an affidavit, in stark contrast to the San Bernardino Matter, in which FBI agents submitted several declarations attesting to the need for Apple’s assistance, even though those claims were later proven untrue.

bypassed the passcode on several iPhones). This is plainly inadequate—an exchange with a single third party is not an exhaustive search, and while the government may believe that compelling Apple to access Feng’s iPhone is likely to be the most *efficient* or *cheapest* method of accessing the data, *see* DE 30 at 42, the All Writs Act “does not authorize a court to order a party . . . to aid the government in conducting a more efficient investigation, when other forms are available.” *Plum Creek*, 608 F.2d at 1289-90 & n.5; *see also Bernstein v. Vill. of Piermont*, 2013 WL 5718450, at \*4 (S.D.N.Y. Oct. 21, 2013) (denying All Writs Act relief because an “insurer’s refusal to fund [a Village employee’s defense] would not ‘frustrate the implementation’ of this Court’s Order; it would merely mean that the Village must bear the cost directly”). Indeed, paying a third party other than Apple for the services the government wants Apple to perform is certainly a “conceivable way” to extract the data from Feng’s iPhone without compelling Apple’s involvement, as the government conceded by requesting vacatur of the order in the San Bernardino Matter.

*Third*, the government’s claim of necessity is belied by its eleventh hour request to vacate its application in the San Bernardino Matter. *See* Ex. C [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 209 (C.D. Cal. Mar. 28, 2016)]; *see also supra* at 2. That the government submitted declarations in the San Bernardino Matter that it unequivocally needed Apple’s assistance to access the iPhone in question—only to have those declarations later disproven when it acquired technology from a third party—shows that the government’s knowledge of its own capabilities and those available in the marketplace was lacking, and thus its unsupported claims of necessity here are not credible. While the government has suggested publicly that the technology used in the San Bernardino Matter will not work on Feng’s iPhone, it has made no showing that it has exhausted *other* methods in use by third parties that may be

able to access an iPhone 5s running iOS 7. *See, e.g.*, Ex. B [Kim Zetter, *How the Feds Could Get into iPhones Without Apple's Help*, Wired (Mar. 2, 2016)].<sup>24</sup> At the very least, in light of the successful assistance by a third party in the San Bernardino Matter, the government should have a heightened duty to make similar inquiries here before a last minute intervention results in further waste of judicial resources.

*Fourth*, the government has failed to show that it has exhausted other potential repositories of the information it wants from Feng's iPhone. The government says that it seeks to learn Feng's customers and sources from the data on his iPhone, DE 30 at 8, but it has not shown, for example, whether it attempted to get this information by subpoenaing relevant records from Feng's cell-phone service provider, or by obtaining a warrant under the SCA, 18 U.S.C. § 2703, for the contents of any accounts Feng owns, such as an Internet-based email service or a social-media service, or for text messages sent to and from his phone. Nor did the government seek an SCA order to obtain other potentially useful information from Apple. These records or others may obviate the purported need for Apple's assistance to bypass Feng's passcode.

*Finally*, as Judge Orenstein noted, the government has failed to make any showing that it has made serious efforts to get the passcode directly from Feng or to have him unlock the phone

---

<sup>24</sup> The government should not be allowed to supplement the record on necessity in its upcoming reply brief. It is axiomatic that a court need not address arguments or evidence introduced for the first time in a reply brief, *see, e.g., Knipe v. Skinner*, 999 F.2d 708, 710-11 (2d Cir. 1993), particularly where the information "was available to the moving party at the time that it filed its motion and [] is necessary in order for that party to meet its burden," *Revise Clothing, Inc. v. Joe's Jeans Subsidiary, Inc.*, 687 F. Supp. 2d 381, 387 (S.D.N.Y. 2010). Should the government be permitted to introduce new evidence, Apple should be allowed, at the very least, to file a sur-reply addressing those new issues, *see, e.g., Bayway Ref. Co. v. Oxygenated Mktg. & Trading A.G.*, 215 F.3d 219, 227 (2d Cir. 2000) (noting that the district court should permit a nonmoving party to respond to new matters raised in a reply brief before deciding a motion (citation omitted)), and potentially test the veracity of the evidence and information introduced.

for lawful inspection. DE 29 at 35. Likewise, the government has offered no evidence that it has attempted to prompt Feng’s memory by showing him a similar phone or having him try to recall the passcode (likely just a 4-digit PIN) by remembering passcodes he commonly uses on other devices.

In conclusion, the government has utterly failed to demonstrate that the requested order is necessary to effectuate the search warrant, including that it exhausted all other avenues for recovering the information it seeks. Before the government demands that Apple do the work of law enforcement, the government must offer evidence that it has performed an “exhaustive search” and that it remains unable to obtain the data it seeks without Apple’s assistance. The government has failed to make that showing here and thus its application must be denied.

**2. The Remaining Discretionary Factors Under *New York Telephone* Militate Against Compelling Apple’s Assistance.**

“**Closely Related.**” As Judge Orenstein rightly held, Apple’s “assistance “c[an]not be permissibly compelled” because Apple is too “far removed” from the underlying criminal conduct. *N.Y. Tel.*, 434 U.S. at 174. This is because Apple, unlike the public utility in *New York Telephone*, is a private company that does not own or possess the phone at issue, has no connection to the data that may or may not exist on the phone, and is not related to the events giving rise to the investigation. A critical predicate to the application of the All Writs Act in *New York Telephone* and its progeny—but absent here—is the fact that the government was investigating an ongoing crime that was being perpetrated *using the third party’s property*.<sup>25</sup> In

---

<sup>25</sup> The government contends that although Feng has pled guilty, DE 30 at 3, it is still “seeking evidence in an ongoing investigation” of a drug conspiracy, and the contents of the iPhone could be relevant to uncovering the details of this conspiracy, *id.* at 32. But the government’s explanation is belied by its actions—waiting more than a year after seizing the iPhone to seek permission to search its contents, and when it finally did so, citing its evidentiary value only in Feng’s prosecution. DE 15 at 3; DE 29 at 6. Tellingly, the government did not emphasize the utility of evidence of a conspiracy until after Feng pled guilty, in response to

fact, the government has not cited a single binding case in which the All Writs Act has been invoked to compel a third party to aid in the investigation of a crime to which all defendants have pled and where that third party's property was not being used as an instrumentality in ongoing criminal activity.<sup>26</sup> *See, e.g., id.* at 162 (noting that the subject telephones “had been, were currently being, and would continue to be used in connection” with the suspected offenses); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012) (requiring *defendant* to provide unencrypted copy of hard drive); *United States v. Catoggio*, 698 F.3d 64, 68-69 (2d Cir. 2012) (per curiam) (affirming order restraining *defendant's* disposition of assets); *Mich. Bell*, 565 F.2d at 386 (authorizing a trap-and-trace of telephones used in ongoing illegal gambling operations in which “gambling operators had established procedures thwarting the effectiveness of . . . wiretaps and pen registers”).

The government nevertheless contends that Apple's proximity to the crime—which, again, has already been completed and for which the perpetrator has already pleaded guilty—is established because (1) its facilities were used in the commission of the crime, and (2) its software threatens to obstruct the government's investigation. DE 30 at 32. But this is both incorrect and a distortion of *New York Telephone* and its progeny. To extend that case law to find Apple “closely related” to Feng's criminal conduct in this case would expand the All Writs

---

Judge Orenstein's order that the parties explain why this case was not moot. *See supra* II.D. In addition, all of Feng's co-defendants have already entered guilty pleas. And, in any event, it is wholly speculative that evidence of a conspiracy is only on Feng's iPhone; whatever evidence may have existed when the phone was seized, the likelihood that there is evidence of a present and ongoing conspiracy on a phone that has not been used in nearly two years is vanishingly low.

<sup>26</sup> That is not to say that no order has ever issued compelling third parties to assist the government in such circumstances. But those orders were issued by lower courts in an *ex parte* posture. *See supra* III.B. Lower court orders are, of course, non-binding, and their weight should be further discounted when not the product of adversarial testing. *See District of Columbia v. Heller*, 554 U.S. 570, 623 (2008) (“It is particularly wrongheaded to read [an earlier case] for more than what it said . . . [when] [t]he defendants made no appearance in the case, neither filing a brief or appearing at oral argument . . .”).

Act beyond recognition, to the point at which there would truly be no limit to the government's power to conscript private entities into the service of law enforcement.

The government asserts that Apple's "facilities" were "used" by Feng in committing his crime, yet it fails to explain what facilities it has in mind. Presumably the government is suggesting that because Feng likely used the iPhone *itself*—which "Apple designed, manufactured, and sold," DE 30 at 33—in some manner during the course of his criminal conduct, Apple is closely related to Feng's drug conspiracy. But once the iPhone was sold, Apple never owned or possessed the phone again. And the fact that Apple designed and sold a product that allowed its subsequent owner to communicate about drug transactions hardly renders Apple closely related to that conduct. At bottom, the government's argument that Apple satisfies *New York Telephone*'s proximity requirement is based on Apple's mere insertion of a product into the stream of commerce. *Cf.* DE 29 at 37-38. But as Judge Orenstein rightly observed, interpreting *New York Telephone* to demand nothing more than personal jurisdiction would render the proximity assessment a nullity and violate the oft-expressed admonition that the All Writs Act grants only residual power. *See id.*; *see also supra* III.B.

For this reason, the government relies less on the fact that Feng may have used a device that Apple designed and sold in connection with the commission of his crime than the unsupported contention that Apple is "actively impeding" an investigation by, it would seem, creating software that enables iPhone users to protect their most sensitive personal information and which updates periodically to make devices more secure. DE 30 at 33. Of course, there is nothing active on Apple's part about the security features on the iPhone, as these features require



the owner to activate them. *See id.* at 33.<sup>27</sup> And as for software updates, as with many modern devices, from cars to phones to refrigerators to thermostats, customers buy a combination of hardware and licensed software that updates at regular intervals with the customer’s approval. Merely releasing periodic software updates to iPhone users—updates that can be accepted or declined—cannot possibly render Apple on par with telecommunications carriers that have ongoing misconduct occurring on their networks, yet that is precisely what the government seeks to do here. Finally, there is nothing inherently nefarious or obstructionist about building iOS with robust security features. To the contrary, the government has encouraged stronger device encryption in order to protect against the increasing sophistication of cyber criminals, and in the overwhelming majority of cases, such encryption is used for benign purposes. *See Ex. P* [Mike McConnell, Michael Chertoff, & William Lynn, *Why the Fear over Ubiquitous Data Encryption Is Overblown*, Opinion, Wash. Post (July 28, 2015)] (“We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level . . . .”). In none of these respects has Apple “actively impeded” the government’s investigation. DE 30 at 33.

Ultimately, it is unnecessary to decipher how exactly the government believes that Apple is closely related to Feng’s drug conspiracy because binding case law supports a finding of proximity only where the third party is mediating or hosting the illegal conduct.<sup>28</sup> In *New York Telephone*, for example, a criminal enterprise leveraged the company’s telephone network to coordinate and conduct an illegal gambling operation. *See* 434 U.S. at 162. And the Court

---

<sup>27</sup> In addition, to the extent the government suggests that the existence of a remote wipe feature on Feng’s iPhone amounts to Apple actively impeding its investigation, DE 30 at 33, Apple has already informed the government that the remote wipe request will not work on Feng’s iPhone, Tr. 32-33.

<sup>28</sup> As noted above, Apple acknowledges the existence of nonbinding *ex parte* orders that have departed from these principles. *See supra* at 20-21.

emphasized that the company was a public utility—not, as the government would have it, to explain the company’s duty to assist in law enforcement (which the government contends is shared by private entities)—but because under federal law the company owned and bore a responsibility for maintaining the channels through which the crime was being perpetrated, and did so under the special regulatory oversight applicable to common carriers, 47 U.S.C. § 153. *Id.* at 174; *see also Mountain Bell*, 616 F.2d at 1129; *Mich. Bell*, 565 F.2d at 389.

The same characteristic is present in those rare cases in which an All Writs Act order has issued against a private entity. For instance, in *Hall*, the district court ordered a credit card company to disclose records of transactions that were believed to be used to support a fugitive. 583 F. Supp. at 722. Although the court conceded that the credit card issuer was “not as closely connected with [defendant’s] efforts to avoid capture as *New York Telephone* was with the gambling investigation,” it nevertheless found the issuer sufficiently close given that it was actively extending credit that was being used to benefit the fugitive. *Id.* at 720; *see also Videotapes*, 2003 WL 22053105, at \*3 (ordering apartment complex to provide security videotapes because government had reason to believe fugitive was taking refuge there). Notably, the assistance ordered in these cases was limited to the provision of information already in the third party’s possession.

Here, of course, Feng’s crime was carried out through the telecommunications networks that connected him to his co-defendants—networks distinct from anything Apple owns or controls. To the extent any incidental use of the iPhone can be deemed relevant, there is no sense in which Apple was hosting or mediating the wrongdoing—indeed, it could not be because, unlike in *New York Telephone*, *Mountain Bell*, *Hall*, or *Videotapes*, Apple does not own

or control the iPhone.<sup>29</sup>

Because Apple is not closely related to the underlying crime, it cannot be compelled to assist in its investigation under the All Writs Act. Indeed, Apple is no more closely related to the underlying crime in this case than it is to music piracy, insurance fraud, or adultery in which an iPhone might play an incidental role; proximity is not established by the happenstance that the offending individual used an Apple device in some way to facilitate his or her conduct—to communicate about drug transactions, to download a song, to send an email to a claims adjustor, or to arrange a rendezvous. At bottom, the government seeks a power that knows no bounds, and that neither the All Writs Act nor *New York Telephone* countenances.

**Unreasonable Burden.** The Court in *New York Telephone* also made clear that “unreasonable burdens may not be imposed” under the All Writs Act. 434 U.S. at 172. Because the government’s request placed no affirmative duty on the telephone company and only required passive assistance—permitting the government to access an unused telephone line to install a pen register—the Court considered it a “meager” burden easily within the ambit of the All Writs Act. *Id.* at 174. Here, however, Apple is being asked to provide affirmative assistance by taking possession of and extracting data from a passcode-protected iPhone. Moreover, unlike the telephone company in *New York Telephone*, Apple has never “offered the government the information needed to bypass an iPhone’s passcode security,” DE 29 at 40, or performed the type

---

<sup>29</sup> The government argues that, because Apple “licenses” iOS rather than sells it, the iOS on Feng’s iPhone is Apple’s property, thus placing this case on all fours with *New York Telephone*. DE 30 at 33 n.7. As Judge Orenstein correctly observed, however, nothing in the record “support[s] an inference that Feng in any way used the licensed software itself—as opposed to the data it allowed Feng to store on the hardware Apple no longer owns—to facilitate his crimes.” DE 29 at 32. Moreover, as Judge Orenstein also noted, “[i]n a world in which so many devices, not just smartphones, will be connected to the Internet of Things, the government’s theory that a licensing agreement allows it to compel the manufacturers of such products to help it surveil the products’ users will result in a virtually limitless expansion of the government’s legal authority to surreptitiously intrude on personal privacy.” *Id.* at 32 n.26.

of extractions being requested here for its own commercial purposes, *id.* at 39-40 (contrasting this case with *New York Telephone*, in which the company used pen registers for its own business purposes). The few cases that have upheld orders requiring an entity to engage in affirmative conduct involved instances in which the entity already routinely performed the requested task or retained the requested information *outside the context of a court order* (albeit for different purposes). *See, e.g., Mountain Bell*, 616 F.2d at 1126-27 (public utility could be compelled to assist with tracing calls where such traces were “identical to operations routinely undertaken by the company without court order in a variety of circumstances”); *Hall*, 583 F. Supp. at 721 (no undue burden to compel credit card issuer to disclose transaction information that it already maintained); *Videotapes*, 2003 WL 22053105, at \*3 (apartment complex had to provide security tapes “already in existence” and in its possession). Here, Apple is being asked to provide affirmative assistance to access data that it does not have in its possession and that is outside the scope of its regular business practices.

In addition, while Apple has said that assisting the government with Feng’s iPhone “would not likely place a substantial financial or resource burden on Apple by itself,” it has also cautioned that it would “divert[] man hours and hardware and software from Apple’s normal business operations,” DE 29 at 41; DE 11 at 3, may result in testimonial obligations in order that the evidence obtained from Feng’s iPhone may be admissible, DE 11 at 3-4, and will open the floodgates to a deluge of additional requests from the government, *see* DE 29 at 41. Indeed, if this case were only about *a single* iPhone—as the government repeatedly argued in the San Bernardino Matter, but which law enforcement officials have since conceded is not the case—then the burden on Apple would be minor. But law enforcement officials from the Attorney General to the FBI Director and the New York District Attorney have made clear that cases like

the San Bernardino Matter and this case are intended to set a precedent, one that will support an avalanche of similar data access requests from across the country. *See, e.g.*, Ex. Q [Emily Chang, *Interview with Loretta Lynch at RSA Conference* (Mar. 1, 2016) (Lynch explaining that “the fact that there are other phones just shows that in fact this issue is going to grow”)]; Ex. E at 15-16 [Comey, *Encryption Hr’g*, Part I (confirming he would “of course” use the All Writs Act to “return to the courts in future cases to demand that Apple and other private companies assist . . . in unlocking secure devices.”)]; Ex. R at 10 [New York District Attorney Cyrus Vance, *Encryption Hr’g*, Part II (asserting that there are “thousands of phones” taken as evidence each year and that his office currently has hundreds of devices it cannot access)]. The government’s arguments in this case—much like the arguments advanced and then abandoned in the San Bernardino Matter, which involved a different iPhone model and a different operating system—confirm that the burden to Apple must be assessed not through the lens of a single phone or a specific operating system, but in light of the government’s unambiguous intent to obtain a precedential ruling that can and will be used to support subsequent orders involving other iPhones running different operating systems and with a variety of security features.

Judge Ornstein rightly recognized that the burden analysis contemplated by *New York Telephone* extends beyond an assessment of the material and labor expenses that would be imposed on Apple if it is ordered to comply with the government’s demand. *See* DE 29 at 41 (observing that “the government continues to seek orders compelling Apple’s assistance in bypassing the passcode security of more recent models and operating systems, notwithstanding the fact that such requests are more burdensome than the one pending here”). Similarly, here, the Court must consider the practical implications for Apple if the All Writs Act is held to support the boundless power claimed by the government in this case. *See, e.g., Plum Creek*, 608

F.2d at 1289 (considering the cost of future potential injuries). This cumulative burden weighs heavily against granting the government's application.

#### IV. CONCLUSION

For the foregoing reasons, this Court should affirm Magistrate Judge Orenstein's opinion and deny the government's application for an order compelling Apple's assistance.

Dated: April 15, 2016

Marc J. Zwillinger\*  
marc@zwillgen.com  
Jeffrey G. Landis\*  
jeff@zwillgen.com  
ZWILLGEN PLLC  
1900 M Street N.W., Suite 250  
Washington, D.C. 20036  
Telephone: 202.706.5202  
Facsimile: 202.706.5298

\*Admitted *Pro Hac Vice*

Respectfully submitted,

/s/ Theodore J. Boutrous Jr.

Theodore J. Boutrous Jr.\*  
tboutrous@gibsondunn.com  
GIBSON, DUNN & CRUTCHER LLP  
333 South Grand Avenue  
Los Angeles, CA 90071-3197  
Telephone: 213.229.7000  
Facsimile: 213.229.7520

Alexander H. Southwell  
asouthwell@gibsondunn.com  
Mylan L. Denerstein  
mdenerstein@gibsondunn.com  
GIBSON, DUNN & CRUTCHER LLP  
200 Park Avenue  
New York, NY 10166-0193  
Telephone: 212.351.4000  
Facsimile: 212.351.4035

*Attorneys for Apple Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 15th day of April, 2016, I caused the foregoing document to be filed with the Clerk of the Court for the U.S. District Court for the Eastern District of New York via the Court's CM/ECF system. I further certify that electronic service was accomplished on the following parties:

Robert L. Capers  
Saritha Komatireddy  
Lauren Howard Elbert  
Ameet Kabrawla  
U.S. Attorney's Office for the Eastern District of New York  
Eastern District of New York  
271 Cadman Plaza East  
Brooklyn, NY 11201  
Telephone: 718.254.7577

/s/ Theodore J. Boutrous Jr.

Theodore J. Boutrous Jr.

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

IN RE ORDER REQUIRING APPLE INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT

Docket Nos. 14 Cr. 387 (MKB)  
15 Misc. 1902 (JO)

**DECLARATION OF ALEXANDER H. SOUTHWELL IN SUPPORT OF APPLE INC.'S  
RESPONSE TO THE GOVERNMENT'S BRIEF IN SUPPORT OF ITS APPLICATION  
FOR AN ORDER COMPELLING APPLE INC. TO ASSIST LAW ENFORCEMENT  
AGENTS IN THE EXECUTION OF A SEARCH WARRANT**

I, Alexander H. Southwell, declare as follows:

1. I am an attorney licensed to practice law before this Court. I am a partner in the law firm of Gibson, Dunn & Crutcher LLP, and represent Apple Inc. in the above-captioned matter. I submit this declaration in support of Apple Inc.'s Response to the Government's Brief in Support of its Application for an Order Compelling Apple Inc. to Assist Law Enforcement Agents in the Execution of a Search Warrant. The following facts are true to the best of my knowledge and belief and, if called and sworn as a witness, I could and would testify competently to them.

2. Attached hereto as **Exhibit A** is a true and correct copy of a speech given by FBI Director James Comey at Kenyon College on April 6, 2016, titled *Expectations of Privacy: Balancing Liberty, Security, and Public Safety*, available at <https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety>. The speech was printed on April 15, 2016.



3. Attached hereto as **Exhibit B** is a true and correct copy of the Wired article, *How the Feds Could Get into iPhones Without Apple's Help*, by Kim Zetter, originally published on March 2, 2016, available at <http://www.wired.com/2016/03/feds-might-get-iphones-without-apples-help/>. The article was printed on April 15, 2016.

4. Attached hereto as **Exhibit C** is a true and correct copy of the Government's Status Report filed on March 28, 2016, in the case *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #5KGD203*, Case No. 16-cm-00010-SP-1 (C.D. Cal.), filed at Docket Entry No. 209.

5. Attached hereto as **Exhibit D** is a true and correct copy of the Guardian article, *FBI Director Admits Apple Encryption Case Could Set Legal Precedent*, by Spencer Ackerman and Sam Thielman, originally published on February 25, 2016, available at <https://www.theguardian.com/technology/2016/feb/25/fbi-director-james-comey-apple-encryption-case-legal-precedent>. The article was printed on April 14, 2016.

6. Attached hereto as **Exhibit E** is a true and correct copy of the transcript of Testimony at the House Judiciary Committee Hearing on Encryption Security and Privacy, Panel 1, *Encryption Tightrope: Balancing Americans' Security and Privacy*, on March 1, 2016. The transcript was printed from Congressional Quarterly on March 2, 2016.

7. Attached hereto as **Exhibit F** is a true and correct copy of the transcript of Testimony at the House Select Committee on Intelligence Hearing on World Wide Threats on February 25, 2016. The transcript was printed from Congressional Quarterly on February 29, 2016.

8. Attached hereto as **Exhibit G** is a true and correct copy of the SF Gate article, *As Apple, FBI Spar, Feinstein Pushes Bill to Require Decryption*, by Sean Sposito and Carolyn Lochhead, originally published on April 8, 2016, available at <http://www.sfgate.com/business/article/As-Apple-FBI-spar-Feinstein-pushes-bill-to-7237590.php>. The article was printed on April 14, 2016.

9. Attached hereto as **Exhibit H** is a true and correct copy of the Apple Inc. document, *iOS Security: iOS 9.0 or later*, originally published in September 2015, available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf).

10. Attached hereto as **Exhibit I** is a true and correct copy of the PCMag article, *iOS 7 Makes the iPhone More Secure than Ever*, by Max Eddy, originally published on September 13, 2013, available at <http://www.pcmag.com/article2/0,2817,2424408,00.asp>.

11. Attached hereto as **Exhibit J** is a true and correct copy of the letter from Assistant United States Attorney Karen Koniuszy to the Honorable Sterling Johnson, Jr., dated July 9, 2015, regarding the case *United States v. Djibo*, Case No. 15-CR-00088-SJ-1 (E.D.N.Y.), filed at Docket Entry No. 27.

12. Attached hereto as **Exhibit K** is a true and correct copy of the transcript of a hearing held on September 3, 2015, before the Honorable Sterling Johnson, Jr., on the defendant's motion to suppress in the case *United States v. Djibo*, Case No. 15-CR-00088-SJ-1 (E.D.N.Y.), filed at Docket Entry No. 65 on October 16, 2015.

13. Attached hereto as **Exhibit L** is a true and correct copy of the Government's Motion to Compel Apple Inc. to Comply with the Court's February 16, 2016 Order Compelling Assistance in Search filed on February 19, 2016 in the case *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*,

*California License Plate #5KGD203*, Case No. 16-cm-00010-SP (C.D. Cal.), filed at Docket Entry No. 1.

14. Attached hereto as **Exhibit M** is a true and correct copy of the Washington Post article, *Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, by Ellen Nakashima, originally published on April 28, 2013, available at [https://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71\\_story.html](https://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html). The article was printed on February 23, 2016.

15. Attached hereto as **Exhibit N** is a true and correct copy of the Washington Post article, *Obama Faces Growing Momentum to Support Widespread Encryption*, by Ellen Nakashima and Andrea Peterson, originally published on September 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](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).

16. Attached hereto as **Exhibit O** is a true and correct copy of the Declaration of Stacey Perino, Electronics Engineer, FBI. The Declaration was filed by the Government on March 10, 2016, in the case *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #5KGD203*, Case No. 16-cm-00010-SP (C.D. Cal.), filed at Docket Entry No. 149-3.


17. Attached hereto as **Exhibit P** is a true and correct copy of the Washington Post opinion article, *Why The Fear Over Ubiquitous Data Encryption Is Overblown*, by Mike McConnell, Michael Chertoff, and William Lynn, originally published on July 28, 2015,

available at [https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4\\_story.html](https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html).

18. Attached hereto as **Exhibit Q** is a true and correct copy of a transcript of Emily Chang's interview with Attorney General Loretta Lynch at the RSA Conference on March 1, 2016. The transcript was printed from LexisNexis.

19. Attached hereto as **Exhibit R** is a true and correct copy of the transcript of Testimony at the House Judiciary Committee Hearing on Encryption Security and Privacy, Panel 2, *Encryption Tightrope: Balancing Americans' Security and Privacy*, on March 1, 2016. The transcript was printed from Congressional Quarterly.

I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 15<sup>th</sup> day of April, 2016 at New York, New York.

  
\_\_\_\_\_  
Alexander H. Southwell

# **Exhibit A**

# Expectations of Privacy: Balancing Liberty, Security, and Public Safety

- - ✉
  - James B. Comey
  - Director
  - Federal Bureau of Investigation
  - Center for the Study of American Democracy Biennial Conference, Kenyon College
  - Gambier, OH
  - April 06, 2016

## *Remarks as delivered.*

Thank you so much President Decatur. I wish I could explain to my parents as well as you just explained it why they were paying for an education in chemistry and religion. They thought it was about alchemy or something.

Thank you all for being here. I very much appreciate your taking the time on a rainy weeknight. There's only one of you who is required to be here and that is my son. The rest of you could have actually been enjoying a little free time before finals. As the weather has finally improved, I am very grateful that you've taken the time to stay and to listen to me and I hope to talk with me, because I want to share some thoughts and I'd like to have a conversation with you that focuses on the things you'd like to know about, and the things you'd like to test me on, and push me on. That you're here means you care about these issues which I do very much, and this is a great thing that Kenyon is sponsoring this conference.

Tonight I want to talk to you about privacy as the keynote speaker. I also want to talk to you about how we might have better conversations about privacy, how we deal with the issues of privacy, how we think about the costs associated with the tough decisions will affect your lives—I'm talking to the students now—most of all and longest. I think we need to find a way to make smart balanced decisions. Ones that will serve us well over the long run, and to make good decisions we have to find a way to have good conversations about things that matter, and that can often separate people of goodwill. Let me start with something you heard earlier, expectations of privacy.

What does privacy mean to you? What are your expectations, and what should they be? Right now I suspect your privacy revolves mostly around social media, and your personal lives. You don't want your mom to see the text you're exchanging with somebody in bio class. You don't want your next employer to know that you're a big fan of taking fish gape selfies with your friends. I understand the fish gape has replaced the duck face in selfie world. I am much cooler than I appear to be.

You want to keep your nosey relatives from reading your Facebook posts, your tweets, visiting your Instagram account, looking at your texts. You really don't like the idea of the government, law enforcement in particular, seeing any of it, not pictures, not texts, not tweets, who your friends are, where you've been online. I get that, I really do. I don't want anybody looking at my stuff either. I don't want anyone poking through my Instagram account, which has seven followers. They're all my children, my spouse, and I've let one son-in-law in so far.

As much as I get that, I also think there are other perspectives in play, other issues to consider. Imagine this, what if law enforcement had a phone owned by somebody who abducted your sister? A phone used by a suicide bomber who blew up the train station in your hometown? The phone of somebody who hurt a little kid in your neighborhood? Would that cause you to think about it differently? I think it should, or at least it should change the way that we have a conversation about it, and I'll tell you why.

In this great country, we often have a reasonable expectation of privacy in our houses, in our cars, in telephone booths, in our devices, that makes good sense. That has long meant that the government could not invade our privacy without good reason reviewable in court. It also meant that with good reason, law enforcement could enter private spaces. Since the founding of our country, if law enforcement had probable cause to believe that there was evidence of a crime in some space, whether that's a house, or a vehicle, or a device, some space that you controlled, law enforcement could go to a judge and get a warrant, go to that private space look through your stuff.

They could search wherever the judge said they could, in your car, in your closets, in your computer, in your phone. They could take whatever the judge said they could take. There are vital constraints on law enforcement, and we must never ever forget them, but the general principle is one we've always accepted in this country. There is no such thing as absolute privacy in America. There is no place outside the reach of judicial authority. That's a bargain that we made with ourselves 240 years ago to achieve two things we all treasure, liberty and security.

And that bargain—"No invasion of private spaces without good reason and appropriate oversight"—has made America a country rooted deeply in the rule of law. It has also meant that there are no absolutes in American life. All kinds of interactions that are incredibly important to everybody here, and to me, incredibly personal and private, none of them are absolutely so under the law.

Private conversations that matter most to us often at the most difficult moments in our lives, conversations with our doctors, with our attorneys, with our therapists, with our lawyers, with our spouses, with reporters, with all kinds of people that we have to have important conversations with, those are all protected by law, but none of them absolutely so.

All of those zones of privacy can be pierced if a court finds compelling reasons to do so, and have long been physical spaces in our lives that are intensely personal, and private to all of us, but none of them absolutely so. Safe-deposit boxes, storage units, car trunks, our diaries, even if we have one of those

little locks on them, all of those things, all of those things can be opened if the interests favoring opening them are compelling. As strange as it sounds even our memories are not absolutely private.

Anyone of us could be compelled by a judge to testify about what we saw, what we heard, what we remember. We can be compelled to say what's in the content of our minds even if it would hurt us, even if it was incriminating to us so long as we were protected from the government's use of that information by an immunity order. In America we've always balanced privacy and security. It can be messy, it can be painful, but we've always worked through the three branches of government to achieve that balance in a sensible way.

The country's effort to achieve that balance for over 200 years was not complicated by technology, because there was no widely available space in American life that couldn't be entered if there was a court order. No car, no trunk, no closet, no safe-deposit box, no safe that couldn't be opened if a judge said it should be open. Here's what changed, the advent of widely available strong encryption has changed the entire thing. It's really happened in a huge way just in the last three years.

I say it that way because encryption has always been around at least for decades, always available to the sophisticated user, both for data at rest sitting on a device, and data in motion being transmitted over a line. What's changed in the last few years is that it has now become the default covering wide swaths of our lives, and covering wide swaths of law enforcement's responsibilities. For mobile devices for instance, Apple and Google made the move to encrypt the devices only in late 2014.

It seems like a lifetime ago, WhatsApp announced that encryption moved on all of their services yesterday. A billion people now communicating in ways that can't be intercepted even with a judge's order. Today those of us in law enforcement are confronted with boxes that can't be opened. We face devices that we can't open, we face data that even if we're able to collect it with a court order, we can't read it. It's gobbledygook to us, so encryption brings us to a place or to quote a portion of the Fourth Amendment, all of our papers and effects can be entirely private to a place where nobody can listen to our conversations, read our texts, look at our documents, see our pictures, know what's in our e-mails, unless we give them permission, unless we say so.

There is a lot to love about this. I love strong encryption. It protects us in so many ways from bad people. It helps the FBI with our mission, which centers on protecting privacy and fighting hackers. In many ways I think all of us like the idea of a storage space in our lives that no one can get into, a safe box that's only mine, but it takes us to a place of absolute privacy that we have not been to before where the balance we have long struck is fundamentally challenged, and changed.

That's why we have to talk about it, that's why we have to have an adult conversation about the balance that means so much to all of us, because no matter how you feel about it, you have to acknowledge there are costs to this new world. You may decide the costs are outweighed by the benefits, or you may decide that there's nothing we can do about it technologically, but you simply have to as part of the



conversation stare at the cost in a fair way. The reason for that is we are not the only ones who love strong encryption.

Child predators love it, organized criminals love it, terrorists love it, and it's part of their tradecraft. Hackers love it in all of their work. All of those people understand the power of strong encryption. ISIL, the so-called Islamic State, uses mobile messaging apps that are encrypted end-to-end to reach its followers, motivate them, and then direct them. We work very, very hard in the FBI to track those who might be moving to violence on ISIL's behalf, but sometimes it's like searching for a needle in a haystack. When that needle moves to a mobile messaging app that's end-to-end encrypted, that needle disappears.

The great fear that dominates our lives is that that needle's going to reappear at a train station wearing a suicide vest. As I said before, we can get a court order, but what we collect is unreadable. Last spring to give one example, a group of terrorists tried to attack, and did attack a "Draw Mohammed" contest in Garland, Texas. Before that attack, one of those people in Texas exchanged 100 messages with an overseas terrorist. We today have no idea what they said to each other, because they used a mobile messaging app that was end-to-end encrypted.

We can look at that, it's gobbledygook to us. This isn't a problem just in national security cases. Last spring an eight-month pregnant woman opened her front door in Baton Rouge, Louisiana, to somebody she apparently knew, and that person killed her. The case is cold already, her mom says she kept a detailed diary on her phone. The phone was there with her body, and the phone is locked, and we can't open it. We don't know what was going on in her life that she confided to her diary, and that case remains unsolved.

These are powerful and painful examples, but I think everybody has to agree that whether you work in technology, or law enforcement, or you simply own a phone, which I think is all of us, the logic of strong encryption means that all of our lives, including law enforcement's life will soon be affected by strong encryption. We live our lives on these mobile devices, and when those are off-limits despite court orders, our world changes.

My first point is simply we have a problem.

Maybe there is nothing that can be done about it, maybe there is, but we should weigh things differently. I hope we will start with the common ground, that ubiquitous strong encryption is bringing significant change to the way we think about liberty and security. We should try to have a thoughtful conversation about what we do about it as a people. Let's turn to what I hope, what I dream that conversation can be like.

I have discovered that it is incredibly difficult to have a good conversation about the impact of encryption on law enforcement and national security.

There is for reasons I don't fully understand, an intensity of emotion around the issue on all sides that makes even really bright people struggle to find balance and empathy that they might otherwise bring readily to hard topics. A group of technology companies last year sent the letter to President Obama where they urged him to promise never to seek legislation to address the intersection of encryption and public safety. That's certainly an understandable position, and these were serious people from serious companies.

When I read the letter at the time, I said something that maybe one of those things that's in your head, you said, "Did I say that out loud?" I did say it out loud, and I meant it so I'm going to repeat it, I said, "I think the letter is depressing." The reason I said that is, the letter did a great job of talking about awesome things that encryption offers all of us, and I agree with all that. The letter made no mention of the impact on public safety, and to my mind that meant either that these folks writing the letter didn't understand the potential costs, or that they weren't being fair-minded about it.

Either way that was a depressing thing, because to me it said either we have to spend a ton more time trying to have people understand why we're talking about this, or a ton more time trying to get people to be open and fair with us in the conversation. I've got to tell you I found a whole lot of the rhetoric of that we have engaged in this country in connection with the recent litigation involving the government and Apple, I found a whole lot of it similarly disheartening.

First let me make sure though that we're all on the same page when it comes to that case. In December, two terrorists attacked an office gathering in San Bernardino, and they killed 14 people and wounded 22 others. They left behind three phones. Two were cheapo phones that they smashed, and we could not recover anything from them. The third was an iPhone 5C running IOS 9, and that matters. It was a phone owned by one of the killer's employers, the County of San Bernardino.

For the FBI to competently investigate a mass murder in the United States, we believe we had to use all lawful tools to find out whether there was evidence on that phone that either shed more light on what these two killers had done, or shed light on who else might be involved and still out there. We got a search warrant, and we got consent from the phone's owner—the county—and we tried to open the 5C. We checked with everybody inside the U.S. government, and we checked with a whole lot of people outside of the U.S. government to see if anybody had a solution that will allow us with the court order to open a 5C running IOS 9.

The danger is if we try to guess the passcode beyond the 10th guess, the phone may well auto encrypt permanently, essentially erase itself. Even if that feature goes away, guessing would take us decades, because the phone is designed to have each guess require a longer period of time as you wait to make the next guess, and to make the number of guesses you'd have to crack the code it would take us many, many years. We went to court, the court from which we'd gotten the search warrant, and the government's lawyers from the Department of Justice required a court order that would direct Apple to do a couple of things, two things:

Shut off that auto encrypt feature on the phone, and shut off the feature that delays successively longer periods after each unsuccessful guess. With those two features disabled, then the government would be able to try to guess the code, and our people are confident that they could guess it without those features, with electronic pulses in about 26 minutes. Under the judge's order, Apple would be required to write code for that phone to turn off those features. The phone could stay in Apple's possession, the software that they wrote would stay in Apple's possession.

Apple resisted the order, which is their right, and their main argument was that the court didn't have the authority to order them to take the step of creating software for that particular device, that it went beyond the court's authority to direct Americans to assist with the execution of court orders. That's a good-faith reasonable argument about a federal court's authority, and it's an interesting question. Obviously the government has a different view of the law there, because we believe that the court's authority does extend to such assistance, but it was Apple's right to make that argument.

If I were their lawyer, I would have made the same argument. I believe it was a reasonable argument even if I have a different view of the law, but beyond the reasonable arguments, the controversy over the Apple case, over the challenge of encryption more broadly, has been chock-full of slippery slope arguments, and absolutist arguments. If we do this for example, and you can supply your own "this," but if we open this phone, if we make this accommodation, then horrible things will inevitably happen.

It's the first step down a slippery slope, or a whole lot of folks have said things like, "We must protect privacy absolutely. Phones contain our lives, and they must be off-limits to the government." Now I know you've already learned this from your philosophy classes here at Kenyon, but every time you hear somebody making a slippery slope argument, an alarm should go off in your head. There is a reason your professors call this "slippery slope fallacy." It could be that if you take one step you'll inevitably fall down a slick slope, it could be.

It depends a lot on what kind of shoes you're wearing, whether the slope is a stairs slope, and whether there's a railing. It is a fallacy, because it is deceptively misleading. Sometimes one step leads inevitably to others, sometimes not; it depends upon a whole lot that a good conversation is needed to figure out. The notion that privacy should be absolute, or that the government should keep their hands off our phones, to me just makes no sense given our history and our values—something that President Obama said two weeks ago in Texas.

You may still end up disagreeing with the government, but starting from the position that privacy should be absolute is just not a fair-minded place to be in my estimation. What I find so frustrating about the emotion around encryption, is that very, very smart people who would otherwise be deeply skeptical of slippery slope, and absolute arguments in the context of other issues like guns, seemed less skeptical of those rhetorical techniques in this context for reasons that I honestly don't understand.

It is simply not the case that if Apple wrote software for the killer's phone it would inevitably be at

catastrophic risk, anymore than we are at catastrophic risk now that the government has purchased a tool that allows court-authorized access to the phone. As I mentioned, until late 2014, neither Apple nor Google made phones that law enforcement couldn't open, and with court orders they routinely opened those phones. Today, the iCloud is encrypted, Apple decrypts it in response to court orders, and produces the contents in law enforcement investigations.

In my view, privacy and security didn't end in 2014, and we are not ending it today. There are risks, there are benefits, there are steps that make us more secure, there are steps that make us less secure. It requires detailed facts, and balancing to assess how do those risks, how do those benefits change with each step? I believe the stakes are high enough that thoughtful people should work very hard to resist fallacies, and talk to each other in a fair-minded way. It's also not the case I believe that any infringement on privacy is to be feared.

The question we must all ask is this: So what's the nature of the infringement, and under what circumstances, and with what oversight, and what are the benefits of the costs associated with that incremental infringement? We have to find thoughtful, productive ways to talk about issues of privacy and security, and here's the thing, by thoughtful I don't mean that I'm right, and you're wrong. I could be wrong about the way I assess, the way I perceive, the way I balance, the way I reason, but I think all productive conversations start from a place of humility. I could be wrong.

I hope very much that you recognize that you could be too, and if we start there, that's the basis for a good conversation. On behalf of the grown-ups of the United States, I'd like to apologize that we have not done a good job in this country in recent years at modeling how to have good conversations about hard things. We tend to shout talking points at each other, or as we get cooler, even though we're old we launch tweets at each other without any real interest in questioning our own assumptions, our own perceptions, our own reasoning, and without an openness to be wrong, in whole or in part.

The litigation between the government and Apple over the San Bernardino phone has ended, because the government has purchased from a private party a way to get into that phone 5C running IOS 9. I think that's a very good thing for at least two reasons. First, that litigation really, really was about the government needing to get access to a terrorist's device. As I said at the time, we should be fired if we had a lawful means to get into terrorist's phone and we didn't try to. It was not—repeat not—about trying to send a message, or create a precedent.

We kept trying to find ways into that phone before we brought the litigation. We kept trying to find ways to get into that phone after the litigation, and one of the benefits, one of the maybe few benefits to all the controversy around it, is that a worldwide market of creative people was stimulated that hadn't existed before, where a whole lot of folks tried to see, "Could I break into a 5C running IOS 9?" Everybody and his Uncle Fred called us with ideas. We had people in Congress asking me about ideas during hearings, and I said, "I welcome all comers, this really is about trying to get into that phone."

We have a conversation we have to have about the broader issues. I don't want this to be part of it, I want to find out whether there's something we need to know in a terrorist's phone. Someone outside the government in response to that attention came up with a solution. One that I am confident will be closely protected, and used lawfully and appropriately. That's a very good thing for this terrorist investigation. Second, litigation is a terrible place to have any discussion about a complicated policy issue, especially one that touches on our values, on the things we care about most, on technology, on trade-offs, and balance.

It is a good thing that the litigation is over, but it will be a bad thing if the conversation ended, because we have to have it. It's unbelievably complicated, touching on every issue we care about, it has implications for safety, privacy, innovation, human rights, national security, international relations, and probably a few others that you can think of that I can't think of. It does not fit in a tweet. We must have the conversation because encryption's impact is great, wonderful in a lot of ways, and growing.

At some point it's going to figure in a major tragedy in this country. It is very hard for us as a people to have thoughtful conversations in an emergency, and in the wake of a major tragedy. We have to have this conversation now, and let me now show you what a dreamer I am.

I hope as we have this conversation that we will successfully resist some of the most challenging aspects of our very nature. One of the strongest forces I think in human experience is the confirmation bias.

That extraordinary aspect of our brains that makes us hungry for data, that is consistent with that which we already believe, and often keeps contrary data from reaching my consciousness. From never entering into my mind, because it got filed away before it got there. I don't know about you, but that is terrifying to me. I think it's part of the reason that humans can convince themselves of nearly anything, and then cling to it like a life raft in a storm. It's one of the things that should make all of us in government, out of government, skeptical of power.

John Adams once wrote to Thomas Jefferson, "Power always thinks it has a great soul." People, in my experience are at their most dangerous when they are certain their cause is just, and certain that their facts are right. Oh lordy, they are frequently certain of both. Today, even if you're tempted to doubt, you can be quickly reinforced by an echo chamber that's on your device 24 hours a day. It will buttress that which you already believe, so there's very little risk of you overcoming the confirmation bias that way.

To depress you further, I think humans also have a tendency to travel in packs, and surrender individual judgment to the will of a group, and allow the loudest voices to hijack that group, the lowest common denominator to hijack that group. That side of us is only reinforced today by the technology that's around us. By the world of reflexive likes and retweets. Human nature, and our respect for it, and fear of it, is the reason why all FBI agents in training, and all FBI intelligence analysts in training go to the Holocaust Museum in Washington, so they can see, and hear, and feel what we are capable of.

What people who are believing they are righteous, and lack constraint and oversight can do. When

people surrender their moral authority to the group. It's also the reason why every new analyst and agent at the FBI is required to take a course on this organization's interactions with Dr. Martin Luther King, Jr. It's intended to remind all of them of the dangers of becoming untethered to oversight and accountability without having checks on human nature.

As a further reminder about human nature, I think all of my employees now know this.

I have an old desk that has a glass tabletop. In the right-hand corner of it under the glass is a single piece of paper. It's from October 1963, and it's a memo from J. Edgar Hoover to Robert F. Kennedy, the Attorney General of the United States, asking for permission to bug Martin Luther King Jr. It's five sentences long, it's utterly devoid of factual content, of any consequence. There is no date limitation, there's no geographic limitation, it simply says we need to bug this guy essentially. Hoover signed it, Kennedy signed it, and they were off to the races.

This isn't about me trying to pick on Bobby Kennedy, or J. Edgar Hoover, but here's the thing. I have no doubt that they believed they were doing the right thing. I keep it there to remind me in that spot, because that's the spot where every morning I review the thick stack of applications that the FBI's going to send to federal judges to ask permission to wiretap or bug people in our national security investigations. Those things are thicker than my arm, it's a huge pain in the neck to get those orders, that's a great thing.

It sits there—that order—to remind me and everybody who hears about it, to be very, very careful about being certain that your cause is just and that your facts are right.

I'm hugely grateful to Kenyon for a bunch of reasons. You have afforded my son an incredible education. I'm grateful to all of you for fighting to find the space to have a quality conversation about privacy, and to talk about things that matter. My hope is that tonight when we start talking, and over the next two days you will engage, you will question assumptions, and biases, your own, and those of the people you're talking with.

You'll ask good questions, you'll listen with an open mind, and by that I mean a mind open to being convinced, even if you're not convinced at the end of the day. I also hope we will resist the temptation to demonize anybody in this discussion, whether that's the tech companies, or the government, or anybody else. I haven't seen any demons in this conversation. We are all people trying to do the right thing as we see the right. It is not for the FBI to decide how this country should govern itself.

It's not for the FBI to decide what the right approach is here. Our job is to investigate. Our job is to tell you, the people who pay for us, when the tools you count on us to use aren't working so much anymore, so you can figure out what to do about that. It's also not the job of the technology companies to tell us—to tell you—what to do about this. Their job is to innovate and come up with the next great thing, and they're spectacular at that, which is to be treasured. How we move forward needs to be resolved by the American people, and especially the young who know technology so well, and who care so deeply about

getting the hard things right.

Thank you for caring about it, thank you for getting involved, and I look forward to our conversation.  
Thank you very much.

# **Exhibit B**



# How the Feds Could Get Into iPhones Without Apple's Help

It's a showdown that has the country mesmerized. In court battles brewing across the nation, the FBI is trying to force Apple to help it extract data from iPhones seized in more than a dozen cases.

The government is so intent on forcing Apple's hand that in each case the Justice Department has invoked the 200-year-old law All Writs Act to do it. But application of the Act requires the government to show that it has no other method of extracting data from the phones. And according to experts who spoke with WIRED, that's not necessarily the case. They say there are ways the government can extract data on phones without Apple's help, from using outside contractors to asking its friends at the NSA—ways that it has, in fact, already used in the past. The solutions won't work for every iPhone the government has collected, and the solution offered for extracting data from the phone in San Bernardino involves some speculation about the NSA's capabilities. But they do raise questions about whether the government has done everything it can do to collect the data it says it needs.

Date Received	Jurisdiction	Device Type	iOS Version	Status
10/8/2015	Southern District of New York	iPhone 4S	7.0.4	Apple objected (12/9/2015)
10/30/2015	Southern District of New York	iPhone 5S	7.1	Apple objected (12/9/2015)
11/16/2015	Eastern District of New York	iPhone 6 Plus	8.1.2	Apple objected (12/9/2015)
		iPhone 6	8.1.2	
11/18/2015	Northern District of Illinois	iPhone 5S	7.1.1	Apple objected (12/9/2015)
12/4/2015	Northern District of California	iPhone 6	8.0 (or higher)	Apple objected (12/9/2015)
		iPhone 3	4.2.1	
		iPhone 3	6.1.6	
12/9/2015	Northern District of Illinois	iPhone 5S	7.0.5	Apple requested copy of underlying Motion but has not received it yet (2/1/2016)
1/13/2016	Southern District of California	N/A (device ID not yet provided)	N/A (device ID not yet provided, but the requesting agent advised device is pre-iOS 8)	Apple was advised by the requesting agent that she is seeking a new warrant. Apple has not yet received this warrant.
2/2/2016	Northern District of Illinois	iPad 2 Wifi	7.0.6	Apple objected (2/5/2016)
2/9/2016	District of Massachusetts	iPhone 6 Plus	9.1	Apple objected (2/11/2016)

Chart showing other cases in which the government is using the All Writs Act to compel Apple to assist it in extracting data

from iPhones. Not included in this chart is the San Bernardino case or the one involving the drug case in New York.

## The Commercial Ways In

According to one expert in the forensic industry who spoke with WIRED on condition of anonymity, there are commercial solutions that could possibly help the government extract data from more than half the iPhones in question and possibly more—the phones are running various versions of operating system ranging from 4.2.1 to 9.0. Many of these capabilities involve defeating security mechanisms put in place by Apple and the phone owners, such as encryption and passcodes.

“Forensic companies have been working on ways to extract evidence from mobile phones for years,” says the expert. “They develop proprietary software and hardware to do that. It is well-known that these solutions exploit vulnerabilities on the device that allow them to perform these extractions.”

The FBI in fact has a [sole-source contract](#) with one of them, a mobile forensic firm founded in Israel called Cellebrite. The company offers [data-extraction services and tools](#) for iPhones, Android and Windows phones and Blackberries. And according to its web site, this includes extracting data from locked phones that are using any version of operating system up to 8.4.1, the last version of iOS8 that Apple released.

It’s a service the company only began providing last year for iOS 8, according to a [newsletter it published last August](#). The first version of iOS 8 was released by Apple in September 2014.

“Cellebrite has a unique unlock capability for devices running iOS 8.x that will provide you with unprecedented access to evidence you can stand behind,” the company says [on its web site](#). “This unique capability is the first of its kind—unlock of Apple devices running iOS 8.x in a forensically sound manner and without any hardware intervention or risk of device wipe.”

This could possibly have worked in the case of the phone in New York and in other cases where the FBI is trying to force Apple to help extract data. The New York case, which the judge ruled on [yesterday in Apple’s favor](#), involved a drug suspect whose phone was seized by Drug Enforcement Agency agents. The agents obtained a warrant to search the phone, but during the two-week window covered by the warrant, they were unable to access data stored on it. The government “initiate[d] the execution of the search warrant by attempting to search the device, turning it on and placing it in airplane mode,” the [court ruling reads](#). “The [DEA] agents ... began that search but were unable to complete [it] because” the device required a password to allow access to certain information... The DEA agents then sought the assistance of the Federal Bureau of Investigation (“FBI”), but remained unable to bypass the iPhone’s passcode security.”

The government asserted in that case that “examining the iOS device further without Apple’s assistance, if it is possible at all, would require significant resources and may harm the iOS device.” But Cellebrite uses what’s called a boot-loader extraction method with phones like this. A custom operating system

gets loaded into the device's memory during the boot sequence and makes the user-data partition read-only.

"This guarantees the forensic soundness of the extraction, unlike other methods," the forensic expert says.

Asked to clarify if it actually involves unlocking the phone or simply extracting data from it, he replied, "it's quite similar to what FBI is asking Apple to do [in the San Bernardino case] but Cellebrite is able to create a situation where you can bruteforce the passcode."

In the San Bernardino case, the government has asked a California court to force Apple to write a new version of its operating system that eliminates certain protections against bruteforcing the passcode that exist in the iOS9 software that's running on the phone.

The forensic expert won't describe how the commercial forensic tool for other versions of iOS works in detail. "Apple can close that, so if they realize what forensic investigators are doing, they can fix the vulnerability," he says. In fact, Apple may already have fixed it in iOS 9, since the method no longer works for that version of its operating system.

"The presumption is that they have a vulnerability that's basically a jailbreak for a locked phone," says Nicholas Weaver, a senior researcher at the International Computer Science Institute at UC Berkeley. Generally jailbreaking a phone—which removes software restrictions written into the code by the phone maker—requires the phone to be unlocked; but this would allow jailbreaking, and data extraction, from a phone that is locked. "It's a harder vulnerability to find than most jailbreaking vulnerabilities," Weaver says.

The solution wouldn't work on the San Bernardino phone, since that device uses iOS 9, for which there is currently no commercial solution, the expert says; he notes, however, that forensic analysts are currently working on finding a solution to get into the latest iOS9 phones as well.

The current method *would* work with most versions of iOS 7, though the amount of effort involved varies with different versions, the forensic expert says. It's not clear if it would work with the specific phone in New York, however, since the exact version of iOS 7 on that phone is unknown. Apple did not respond to inquiries asking about the phone. But the government is using the All Writs Act to force Apple's assistance in opening at least five other iPhones that use various versions of iOS 7.

## Paging the NSA

Weaver says there is one possible method the government could use to crack the San Bernardino iPhone without Apple's help. It would involve a vulnerability and exploit for the phone's baseband.

Operating system exploits for the iPhone—that allow investigators to hack a phone that is still being

actively used by a target—can be very powerful but also very expensive. Zero-day exploit seller Zerodium claimed last year that it [paid \\$1 million for an iOS zero-day exploit](#). Such an exploit wouldn't help in the San Bernardino case, since the phone would need to be unlocked.

But a baseband zero-day would.

iPhones don't have just one operating system, but two. A second low-level operating system in the baseband controls the cellular interface, which means if investigators can take over that operating system, they can take over the phone. Since a booted iPhone will connect to a nearby cellular network even before you enter a passcode, investigators could get it to connect to a rogue cell tower that they control—a more powerful version, for example, of a stingray—and use an exploit to take over the phone. But they would need to have an exploit capable of attacking a vulnerability in the baseband operating system.

“Once you have the baseband exploited you're able to bypass all that bruteforce protection and just try all the passwords that you want,” Weaver says. “If you take over the baseband, you have the ability to write to memory, which means you can take over the running operating system. And because the phone is running but locked, you take over that running but locked operating system and now you can do what the FBI wants to do, where you just keep trying PINs against the secure enclave until you get in...So you corrupt the root operating system to say, don't do these protections.”

The FBI may not have access to a \$1 million baseband exploit if one exists, but it likely has friends who do. Apple suggested in its brief last week, that there may be some untapped resources the government has failed to tap to help it get into the San Bernardino phone. The government, Apple wrote, “has not made any showing that it sought or received technical assistance from other federal agencies with expertise in digital forensics, which assistance might obviate the need to conscript Apple to create the back door it now seeks.”

Who might provide the kind of assistance the FBI needs? The obvious answer is the NSA.

“My hunch is that the NSA does have exploits for iPhones—operating system exploits and baseband exploits,” says Weaver. And if that's the case, it would greatly undermine the government's contention that only Apple can help it get into the phone.

But does the NSA have the ability to help the FBI crack the phone?

FBI Director Comey suggested to Congress on Tuesday that it doesn't. He told lawmakers that the FBI has “talked to anybody who will talk to us about [the phone],” when asked if he had spoken to other government agencies.

Nate Cardozo, a lawyer for the Electronic Frontier Foundation, finds this hard to believe.

“The best hackers in the world are employed over at Fort Meade,” where the NSA is located, says Cardozo. “They’re not at Quantico,” the FBI’s home base. “The phone is at Quantico. That, I think, speaks volumes about what’s going on here.”

Either the NSA doesn’t have the ability to open the phone or doesn’t want to risk exposing its methods in a very public case like the San Bernardino one. Or there’s another reason why the FBI might be claiming helplessness when it comes to the phone.

Cardozo and other experts say the fact the FBI has opted for a very public legal battle in the case when other methods for getting the data may be at its disposal suggests that the case is not about getting data but about [setting a legal precedent](#). Specifically, a precedent that could compel Apple and other tech companies to create or alter their software to make it less secure.

“This case was selected very carefully by the FBI in order to develop precedent going forward,” Cardozo says. “They want to be able to order American tech companies to include (or remove) specific features in order to enable surveillance. They’ve never before claimed such a power.”

So while there may be other ways the FBI could get into the cache of iPhones it currently has—and maybe even into the San Bernardino iPhone—that may be beside the point.

*Brian Barrett contributed reporting.*

# **Exhibit C**

1 EILEEN M. DECKER  
United States Attorney  
2 PATRICIA A. DONAHUE  
Assistant United States Attorney  
3 Chief, National Security Division  
TRACY L. WILKISON (California Bar No. 184948)  
4 Chief, Cyber and Intellectual Property Crimes Section  
Assistant United States Attorney  
5 1500 United States Courthouse  
312 North Spring Street  
6 Los Angeles, California 90012  
Telephone: (213) 894-2400  
7 Facsimile: (213) 894-8601  
Email: Tracy.Wilkison@usdoj.gov

8 Attorneys for Applicant  
9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT  
11 FOR THE CENTRAL DISTRICT OF CALIFORNIA

12 IN THE MATTER OF THE SEARCH  
OF AN APPLE IPHONE SEIZED  
13 DURING THE EXECUTION OF A  
SEARCH WARRANT ON A BLACK  
14 LEXUS IS300, CALIFORNIA  
LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)  
GOVERNMENT’S STATUS REPORT

16 Applicant United States of America, by and through its counsel of record, the  
17 United States Attorney for the Central District of California, hereby files this status  
18 report called for by the Court’s order issued on March 21, 2016. (CR 199.)

19 The government has now successfully accessed the data stored on Farook’s  
20 iPhone and therefore no longer requires the assistance from Apple Inc. mandated by  
21 Court’s Order Compelling Apple Inc. to Assist Agents in Search dated February 16,  
22 2016.  
23  
24  
25  
26  
27  
28

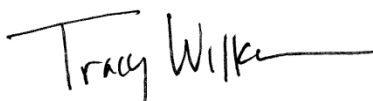
1           Accordingly, the government hereby requests that the Order Compelling Apple  
2 Inc. to Assist Agents in Search dated February 16, 2016 be vacated.

3  
4  
5 Dated: March 28, 2016

Respectfully submitted,

6 EILEEN M. DECKER  
United States Attorney

7 PATRICIA A. DONAHUE  
8 Assistant United States Attorney  
9 Chief, National Security Division

10 

11 TRACY L. WILKISON  
Assistant United States Attorney

12 Attorneys for Applicant  
13 UNITED STATES OF AMERICA  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



# **Exhibit D**

# FBI director admits Apple encryption case could set legal precedent

James Comey tells Congress outcome 'will be instructive for other courts'  
Comey softens insistence on limited scope of case in testimony to Congress

Spencer Ackerman and Sam Thielman in New York

Thursday 25 February 2016 12.45 EST

The director of the FBI has conceded that future judges will look to his battle with Apple as a precedent for law enforcement access to locked or encrypted mobile devices, the first time the government has conceded that the implications of the case stretch beyond an investigation into the San Bernardino terrorist attacks.

The ultimate outcome of the Apple-FBI showdown is likely to “guide how other courts handle similar requests”, James Comey told a congressional intelligence panel on Thursday, a softening of his flat insistence on Sunday that the FBI was not attempting to “set a precedent”.

Comey deferred answering legislators’ questions on the implications of a judge ordering Apple to write code permitting the FBI to guess the passcode of an iPhone 5C used by the San Bernardino killer Syed Farook, something Apple has painted as sufficiently wide-ranging to justify its defiance of a court order.

The director repeatedly said he was “not an expert”, but that technical and legal experts had advised him that “technology [is] the limiting principle”, because the particular combination of the outmoded iPhone 5C and its iOS9 mobile operating system limited the application of the requested court order - a claim Apple rejects.

While Comey continued to argue that the FBI needed to seek access to data on the iPhone for its terrorism investigation of San Bernardino, he acknowledged that police departments and district attorneys around the country were also seeking similar access to locked phones and encrypted conversations in ordinary criminal cases.

Manhattan prosecutor Cyrus Vance has said he has a backlog of 175 locked iPhones awaiting the resolution of the Apple-FBI fight, which is almost certain to be decided in high federal courts.

The outcome “will be instructive for other courts”, Comey told the House intelligence committee.

“I don’t know how lawyers and judges will think about what is the limiting principle on the legal side.”

Apple on Thursday morning challenged Comey’s suggestion that the passcode-breaking tool described in the order could be limited in scope to a single iPhone.

The company referred back to CEO Tim Cook’s statements that the underlying code Apple has been ordered to create is highly transferrable to other phones, to the extent that a similar password-cracking program for another device would be virtually the same.

Technologist and Apple operating system expert Jonathan Zdziarski wrote last week that the basics of the tool Apple has been instructed to build require that it work on multiple phones simply to ensure that it works at all. A senior government official told ABC News on Wednesday that many police departments were anxious to exercise the same privilege.

Cook has also said he is troubled by the precedent set should the high court uphold the order. Comey, testifying on Thursday to the House panel, acknowledged that the outcome of the case would be “instructive to other courts”.

Also for the first time since the 16 February order sent shockwaves around the technology, law enforcement and cybersecurity worlds, Comey softened some of the government’s harsh rhetoric around Apple.

“There are no demons here,” said Comey, striking a more conciliatory tone than that of the Justice Department’s accusation in court last week that Apple was placing “marketing” over security.

Comey’s tone is not shared throughout the US Department of Justice. The attorney general, Loretta Lynch, told the congressional appropriations committees this week that within the department’s \$781m budget request is an initiative devoting \$38m “toward developing the tools we need to lawfully access encrypted data and communications”.

Lynch listed secure communications alongside serious criminal threats, saying that the Justice Department needed “critical measures to address evolving challenges like homegrown extremism, online radicalization and increasingly sophisticated encryption”.

Apple is expected to file its first formal legal response explaining its resistance to the access order by Friday. In advance, both sides have waged a high-profile messaging war.

Cook, in an interview with ABC on Wednesday, said the FBI was asking Apple to write code - which engineers have derisively termed “FBiOS” - that would serve as “the software equivalent of cancer”, opening the door not only for future forced access to data on a phone, but to remote law enforcement hijacking of its functions.

“Maybe it’s an operating system for surveillance, maybe the ability for the law enforcement to turn on the camera. I don’t know where it stops,” Cook told ABC.

Jim Himes, a Connecticut Democrat on the panel, suggested that once Apple writes the

code the FBI desires, the company would become a target of “our sovereign adversaries, of criminal enterprises, of terrorists” attacking the Apple servers on which the company stores the tool - implying that the FBI would in effect mandate the creation of a cybersecurity vulnerability for Apple’s millions of mobile customers.

“There’s a legitimate worry, though, that a decision in favor of the FBI could be the narrow end of a very wide wedge,” Himes said, reframing the debate as “security versus security”.

Comey said he lacked the engineering or legal expertise to address the “reasonable questions” in full, but contradicted software engineers to say the worry of the code getting into other hands was “not a real thing” and praised Apple’s track record on security.

Apple has “done a pretty darn good job of protecting its code”, Comey said.

The House intelligence panel was the first to hear from Comey since the 16 February warrant to Apple, although the committee hearing was not specifically focused on the Apple case. Next week, the House judiciary committee is scheduled to take up the controversy, though it is not yet clear who will testify.

Some Republicans on the panel signalled their early inclination to back the FBI over Apple. Lynn Westmoreland, a Georgia Republican, said the case looked “no different than what you do with a [foreign intelligence] or any other warrant”.

More news

## Topics

Apple FBI San Bernardino shooting

Save for later Article saved

Reuse this content

# **Exhibit E**

CQ CONGRESSIONAL TRANSCRIPTS  
Congressional Hearings  
March 1, 2016 - Final

## House Judiciary Committee Holds Hearing on Encryption Security and Privacy, Panel 1

### LIST OF PANEL MEMBERS AND WITNESSES

GOODLATTE:

We ask all the members of the media that are taking thousands of pictures here, I'm sure they got some excellent ones of the director, but we ask you to please clear aside so we can begin the hearing.

The Judiciary Committee will come to order and without objection the chair is authorized to declare recesses of the committee at any time. We welcome everyone to this afternoon's hearing on, "The Encryption Tightrope: Balancing American Security and Privacy. And I will begin by recognizing myself for an opening statement.

We welcome everyone today to this timely and important hearing on encryption. Encryption is a good thing. It prevents crime. It prevents terrorist attacks. It keeps our most valuable information safe. Yet it is not used as effectively today as is necessary to protect against the ever increasing sophistication of foreign governments, criminal enterprises and just plain hackers.

We see this manifest almost every week in the reports of losses of massive amounts of our most valuable information, from government agencies, retailers, financial institutions and average Americans. From identity theft to the compromising of our infrastructure, to our economic and military security, encryption must play an ever increasing role and the companies that develop it must be encouraged to increase its effectiveness.

Encryption is a topic that may sound arcane or only the province of techies, but in fact, it's a subject whose solutions will have far reaching and lasting consequences. The Judiciary Committee is a particularly appropriate forum for this congressional debate to occur.

As the committee of exclusive jurisdiction over the United States constitution, the Bill of Rights and the federal criminal laws and procedures, we are well versed in the perennial struggle between protecting Americans' privacy and enabling robust public safety.

This committee is accustomed to addressing many of the significant legal questions arising from laws that govern surveillance and government access to communications, particularly the Wiretap Act, the Electronic Communications and Privacy act, the Foreign Intelligence Surveillance Act and the Communications' Assistance to Law Enforcement Act, otherwise known as CALEA.

Today's hearing is a continuation of the committee's work on encryption: work that Congress is best suited to resolve. As the hearing title indicates, society has been walking a tight rope for generations in attempting to balance the security and privacy of Americans' communications with the needs of our law enforcement and intelligence agencies.

In fact, the entire world now faces a similar predicament, particularly as our commerce and communications bleed over international boundaries on a daily basis. Encryption in securing data in motion and in storage is a valuable technological tool that enhances Americans' privacy, protects our personal safety and national security, and ensures the free flow of our nation's commerce.

Nevertheless as encryption has increasingly become a ubiquitous technique to secure communications among consumers, industry and governments, a national debate has arisen concerning the positive and negative implications for public safety and national security.

This growing use of encryption presents new challenges for law enforcement seeking to obtain information during the course of its investigations and even more foundationally, tests the basic framework that our nation has historically used to ensure a fair and impartial evaluation of legal process used to obtain evidence of a crime.

We must answer this question: how do we deploy ever stronger, more effective encryption without unduly preventing lawful access to communications of criminals' and terrorists' intent on doing us harm. This now seems like a perennial question that has challenged us for years.

In fact, over 15 years ago I led congressional efforts to ensure strong encryption technologies and to ensure that the government could not automatically demand a back door key to encryption technologies. This enabled the U.S. encryption market to thrive and produce effective encryption technologies for legitimate actors, rather than see the market head completely overseas to companies that do not have to comply with basic protections.

However, it is true this technology has been a devious tool of malefactors. Here is where our concern lies. Adoption of new communications technologies by those intending harm to the American people is outpacing law enforcement's technological capability to access those communications in legitimate criminal and national security investigations.

Following the December 15 terrorist attack in San Bernardino, California, investigators recovered a cell phone owned by the county government but used by one of the terrorists responsible for the attack.

After the FBI was unable to unlock the phone and recover its contents a federal judge ordered Apple to provide reasonable technical assistance to assist law enforcement agents in obtaining access to the data on the device, citing the All Writs Act as its authority to compel.

Apple has challenged the court order, arguing that its encryption technology is necessary to protect its customers' communications, security and privacy and raising both constitutional and statutory objections to the magistrate's order. This particular case has some very unique factors involved and as such, may not be an ideal case upon which to set precedent.

And it is not the only case in which this issue is being litigated. Just yesterday, a magistrate judge in the eastern district of New York, ruled that the government can not compel Apple to unlock an iPhone pursuant to the All Writs Act.

GOODLATTE:

It is clear that these cases illustrate the competing interests at play in this dynamic policy question, a question that is too complex to be left to the courts and must be answered by Congress.



Americans surely expect that their private communications are protected. Similarly, law enforcement's sworn duty is to ensure that public safety and national security are not jeopardized if possible solutions exist within their control.

This body as well holds its own constitutional prerogatives and duties. Congress has a central role to ensure that technology advances so as to protect our privacy, help keep us safe and prevent crime and terrorist attacks.

Congress must also continue to find new ways to bring to justice criminals and terrorists. We must find a way for physical security not to be at odds with information security.

Law enforcement must be able to fight crime and keep us safe, and this country's innovative companies must at the same time have the opportunity to offer secure services to keep their customers safe.

The question for Americans and lawmakers is not whether or not encryption is essential -- it is -- but instead whether law enforcement should be granted access to encrypted communications when enforcing the law and pursuing their objectives to keep our citizens safe.

I look forward to hearing from our distinguished witnesses today as the committee continues its oversight of this real-life dilemma facing real people all over the globe.

It's now my pleasure to recognize the ranking member of the committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

CONYERS:

Thank you, Chairman Goodlatte.

Members of the committee and our (inaudible) and distinguished guests, I want to associate myself with your comments about our jurisdiction.

It is not an accident that the House Judiciary Committee is the committee of primary jurisdiction with respect to the legal architecture of government surveillance.

In times of heightened tension, some of our colleagues will rush to do something, anything, to get in -- get out in front of an issue. We welcome their voices in the debate, but it is here in this committee room that the House begins to make decisions about the tools and methods available to law enforcement.

I believe that it is important to stay up front, before we get into the details of the Apple case, that strong encryption keeps us safe even as it protects our privacy.

Former National Security Agency Director Michael Hayden said only last week that America is more secure with unbreakable end-to-end encryption. In this room, just last Thursday, Former Secretary of Homeland Security Michael Chertoff testified that, in his experience, strong encryption laws help law enforcement more than it hinders any agency in any given case.

The National Security Council has concluded that the benefits to privacy, civil liberties and cyber security gained from encryption outweigh the broader risk created by weakening encryption.

And Director Comey himself has put it very plainly: universal strong encryption will protect all of us, our innovation, our private thoughts and so many other things of value from thieves of all kinds.

We will all have lockboxes in our lives that only we can open, and in which we can store all that is valuable to us. There are lots of good things about this.

Now, for years, despite what we know about the benefits of encryption, the Department of Justice and the Federal Bureau of Investigation have urged this committee to give them the authority to mandate that companies create backdoors into their secure products.

I've been reluctant to support this idea for a number of reasons. The technical experts have warned us that it is impossible to intentionally introduce flaws into secure products -- often called backdoors -- that only law enforcement can exploit to the exclusion of terrorists and cyber criminals.

The tech companies have warned us that it would cost millions of dollars to implement and would place them at a competitive disadvantage around the world.

The national security experts have warned us that terrorists and other criminals will simply resort to other tools entirely outside the reach of our law enforcement and intelligence agencies. And I accept that reasonable people can disagree with me on each of these points.

But what concerns me, Mr. Chairman, is that, in the middle of an ongoing congressional debate on this subject, the Federal Bureau of Investigation would ask a federal magistrate to give them the special access to secure products that this committee, this Congress and the administration have so far refused to provide.

Why has the government taken this step and forced this issue? I suspect that part of the answer lies in an e-mail obtained by the Washington Post and reported to the public last September.

In it, a senior lawyer in the intelligence community writes that, although the legislative environment towards encryption is very hostile today, it could turn in the event of a terrorist attack or a criminal event where strong encryption can be shown to have hindered law enforcement.

He concluded that there is value in keeping our options open for such a situation. I'm deeply concerned by this cynical mindset, and I would be deeply disappointed if it turns out that the government is found to be exploiting a national tragedy to pursue a change in the law.

I also have doubts about the wisdom of applying the All Writs Act, enacted in 1789, codified in 1911 and last applied to a communications provider by the Supreme Court in 1977, to a profound question about privacy and modern computing in 2016.

I fear that pursuing this serious and complex issue through the awkward use of an inept statute was not and is not the best course of action. And I'm not alone in this view.

Yesterday, in the eastern district of New York, a federal judge denied a motion to order Apple to unlock an iPhone under circumstances similar to those in San Bernardino.

The court found that the All Writs Act, as construed by the government, would confer on the courts an over-broad authority to override individual autonomy.

However, nothing in the government's argument suggests any principal limits on how far a court may go in requiring a person or company to violate the most deeply rooted values.

We could say the same about the FBI's request in California. The government's assertion of power is without limiting principle, and likely to have sweeping consequences whether or not we pretend that the request is limited to just this device or just this one case.

CONYERS:

This committee and not the courts is the appropriate place to consider those consequences, even if the dialogue does not yield the results desired by some in the law enforcement community.

I'm grateful that we are having this conversation today back in the forum in which it belongs -- the House Judiciary Committee.

And so I thank the chairman very much, and I yield back.

GOODLATTE:

Thank you, Mr. Conyers.

And without objection, all other members' opening statements will be made a part of the record.

We welcome our distinguished witness of today's first panel, and if you would please rise, I'll begin by swearing you in.

Do you swear that the testimony that you're about to give shall be the truth, the whole truth and nothing but the truth, so help you God?

COMEY:

I do.

GOODLATTE:

Thank you very much. Please be seated.

I'll now begin by introducing our first distinguished witness today, Director James Comey of the Federal Bureau of Investigation. Director Comey began his career as an assistant United States attorney for both the Southern District of New York and the Eastern District of Virginia. After the 9/11 terrorist attacks, Director Comey returned to New York to become the United States attorney for the Southern District of New York.

In 2003, he was appointed deputy attorney general under the United States Attorney General John Ashcroft. Director Comey is a graduate of the College of William and Mary and the University of Chicago Law School.

Director, welcome. Your entire written statement will be made a part of the record. And I ask that you summarize your testimony in five minutes. And we have the timing light that you're well familiar with on the table.

Again, welcome. We're pleased that you are here, and you may begin your testimony.

COMEY:

Thank you so much, Mr. Chairman and Mr. Conyers. Thank you for hosting this conversation and for helping us all talk about an issue that I believe is the hardest issue I've confronted in government, which is how to balance the privacy we so treasure that comes to us through the technology that we love, and also achieve public safety which we also all very much treasure.

I worry a little bit that we've been talking past each other, both folks in the government and folks in the private sector, when it comes to this question of encryption, which we in the government call "going dark." What I'd like to do is just take three or four minutes and try to frame how I think about it, in a way I hope is fair, fair-minded. And if it's not, I hope you'll poke at me and tell me where you think it's not. But these are the things I believe to be true.

First, that the logic of encryption will bring us in the not too distant future to a place where all of our conversations and all of our papers and effects are entirely private. That is, where no one can listen to our conversations, read out texts, read out e-mails, unless we say so. And

no one can look at our stuff, read out documents, read things we file away without our agreement. That's the first thing I believe, that the logic of encryption is taking us there.

The second thing I believe is, as both you and Mr. Conyers said, there's a lot of good about this, a lot of benefits to this. All of us will be able to keep private and keep protected from thieves of all kinds the things that matter most to us -- our ideas, our innovation, our secret thoughts, our hopes, our dreams. There is a lot to love about this. We will all be able to have storage spaces in our life that nobody else can get into.

The third thing I believe is that there are many costs to this. For the last two centuries, public safety in this country has depended in large measure on the ability of law enforcement agents going to courts and obtaining warrants to look in storage areas or apartments, or to listen with appropriate predication oversight to conversations.

That is the way in which law enforcement brings us public safety. It is very, important and it's been part of the balance in ordered liberty, that sometimes the people's stuff can be looked at, but only with predication and only with oversight and approval by an independent judiciary.

The fourth thing I believe is that these two things are in tension in many contexts, increasingly in our national security work, and in law enforcement work generally across the country. We see it obviously in ISIL's efforts to reach into this country, and using mobile messaging apps that are end-to-end encrypted, task people to kill innocent people in the United States.

That is a huge feature of our national security work and a major impediment to our counterterrorism work because even with a court order, what we get is unreadable. Use a technical term, it's gobbledygook. We cannot de-encrypt that which is covered by strong encryption.

We also see it in criminal work across the country. Very tragically, last year in Baton Rouge, where a pregnant woman eight months pregnant was killed by somebody she opened the door to, and her mom says she kept a diary, but it's on her phone, which is locked. And so the case remains unsolved.

And most recently and most prominently, as both Mr. Conyers and the Chairman mentioned, we see it in San Bernardino -- a case where two terrorists in the name of ISIL killed 14 people and wounded 22 others at an office gathering and left behind three phones, two of which, the cheaper models, they smashed beyond use; and the third was left locked. In any investigation that's done competently, the FBI would try to get access to that phone.

It's important that it's a live ongoing terrorism investigation, but in any criminal investigation, a competent investigator would try and use all lawful tools to get access to that device. And that's what you see happening in San Bernardino.

The San Bernardino case is about that case. It obviously highlights the broader issue and of course it will be looked upon by other judges and other litigants, but it is about the case and trying to do a competent job of understanding: Is there somebody else? And are there clues to what else might have gone on here? That is our job.

The fifth thing I believe is that democracies resolve these kind of really hard questions through robust debate. I think the FBI's job is very very limited. We have two jobs. The first is to investigate cases like San Bernardino and to use tools that are lawful and appropriate. The second thing, it's our job to tell the American people the tools you are counting on us to use to keep you safe are becoming less and less effective.

It is not our job to tell the American people how to resolve that problem. The FBI is not some alien force imposed upon America from Mars. We are owned by the American people. We only use the tools that are given to us under the law. And so our job is simply to tell people there is a problem.

Everybody should care about it. Everybody should want to understand if there are warrant-proof spaces in American life, what does that mean? And what are the costs of that? And how do we think about that?

I don't know what the answer is. It may be the American people through Congress and the courts decide it's too hard to solve, or law enforcement can do its job well enough with strong encryption covering our communications and our papers and effects, or that it's something that we have to find a way to fix to achieve a better balance. I don't know.

My job is to try to offer thoughtful explanations about the tools the FBI has and to bring them to the attention of the American people, and then answer questions about that. So I'm very, very grateful for this forum; very, very grateful for this conversation. There are no demons in this debate. The company is not evil. The government is not evil. You have a whole lot of good people who see the world through different lenses, who care about things. All care about the same things, in my view. The companies care about public safety. The FBI cares about innovation and privacy.

We devote our lives to trying to stop people from stealing our innovation, our secrets, and hacking in to our devices. We care about the same things, which should make this in a way an easier conversation, which I very much look forward to.

Thank you.

GOODLATTE:

Thank you, Director Comey.

We'll now proceed under the five-minute rule with questions for the witness. And I'll begin by recognizing myself.

Director, there has been quite a bit of debate about the government's reliance on the All Writs Act, which most people had never heard of until the last week or so. That is being used in this case to try to compel Apple to bypass the auto-erase functions on the phone. It has been characterized as an antiquated statute dating back to 1789 that was never intended to empower the courts to require a third party to develop new technology.

How do you respond to that characterization? Has the FBI relied on the act in the past to gain access to iPhones or other similar devices? And is the act limited to the circumstances in which Congress has already imposed a statutory duty on a third party to provide assistance?

COMEY:

Thank you, Mr. Chairman.



I smile a little bit when I hear that because old doesn't mean bad, at least I hope it doesn't because I'm rapidly approaching that point. The Constitution is as old or older than the All Writs Act, and I think that's still a pretty useful document.

It's a tool that I use. I think there's some members of the committee who are former federal prosecutors. Every assistant U.S. attorney knows it. I used it when I started as an AUSA in 1987. It is an act that Congress passed when the Constitution was a baby so there was a vehicle for judges to get their orders complied with. And it's been used, many, many, many times and interpreted by the courts many times, including by the Supreme Court.

The cases at hand are simply about, as I understand it, what is the reach of the All Writs Act? It's still good law, but how far does it extend, especially given how technology has changed? And I think the courts are going to sort that out. There was a decision yesterday in New York. There will be decisions in California. There will probably be lots of others because this is a problem law enforcement is seeing all over the country.

GOODLATTE:

Let me ask you about that decision in New York, because in its brief in the California case, Apple argues that a provision of CALEA (ph) another federal statute, actually prohibits the magistrate from ordering it to design a means to override the auto erase functions on the phone.

Just yesterday a magistrate in New York upheld that argument. Can you comment on that?

COMEY:

Not in an intelligent way because I haven't read the decision out of New York. I understand the basic contours of the argument. I don't fully get it honestly because CALEA (ph) is about data in motion, and this is about data at rest. But I also think this is the kind of thing judges do, they take acts of Congress and try and understand so what does it mean especially given changing circumstances.

So I expect it will be bumpy. There will be lots of lawyers paid lots of -- for hours of work, but we will get to a place where we have the courts with an understanding of its reach.

GOODLATTE:

Now, if the FBI is successful in requiring Apple to unlock this phone, that won't really be a one-time request, correct?

COMEY:

Well, the issue of locked phones certainly not because it's become a...

GOODLATTE:

Well, it will set a precedent for other requests from the Federal Bureau of Investigation and all -- and any other law enforcement agency to seek the same assistance in many, many, many other cases.

COMEY:

Sure, potentially, because if any decision of a court about a matter is potentially useful to other courts, which is what a precedent is. I happen to think having talked to experts there are technical limitations to how useful this particular San Bernardino technique will be given how the phones have changed. But sure, other courts, other prosecutors, other lawyers for companies will look to that for guidance or to try and distinguish it.

GOODLATTE:

So that technology once developed, which I presume they could destroy again but then will have to recreate hundreds of times, how confident are you, whichever procedure Apple decided to pursue, how confident are you that what you are requesting -- which is the creation, effectively, of a key, a code -- how confident are you that will -- that will remain secure and allow all the other customers of Apple, and when this is applied to other companies' technology as well, how confident are you that it will not fall into the wrong hands and make everyone's communication devices less secure, not more secure?

COMEY:

First, I've got to -- I've got to quibble a little with the premise of your question. I hear folks talk about keys and back doors. I actually don't see that this way. I mean, there are issues about back door. This is about -- there's already a door on that iPhone, essentially, we're asking Apple take the vicious guard dog away, let us try to pick the lock.

The later phones, as I understand the 6 and after, there aren't doors. So there isn't going to be can you take the guard dog away and let us pick the lock. But look, I have a lot of faith -- and maybe I don't know them well enough -- in the companies' ability to secure their own information. The icloud, for example, is not encrypted, right, but I don't lie awake at night worrying about whether they're able to protect the contents of the icloud. They are very, very good at protecting their information and their innovation.

So one thing is for certain, but I think these folks are pros.

GOODLATTE:

Thank you very much. Chair recognizes the ranking member, Mr. Conyers, for his questions.

CONYERS:

Thank you, Chairman Goodlatte. And welcome again to our forum. You're a very regular visitor to the Judiciary Committee.

Director Comey, it's been suggested that Apple has no interest in helping law enforcement in any criminal case and that the company cares more about marketing than about investigating a terrorist attack. In your view, are companies like Apple generally cooperative when the FBI asks for assistance, accompanied by appropriate legal process? Did Apple assist with this particular investigation?

COMEY:

I think in general, all American companies, and I can't think of an exception sitting here, who want to be helpful especially when it comes to public safety because they have families and children just as we do. So that's the attitude we're met with. And in this particular case, as in many others, Apple was helpful to us.

We had lots of good conversations about what we might be able to do to get this device open, and we got to a place where they said for reasons that I don't question their motive we're not willing to go further. And the government made a decision, we still have an avenue to pursue with the judge, we'll go to the judge. But I don't question their motives.

CONYERS:

All right. Thank you. I sense that you're still reluctant to speak about how your success in this case might set a precedent for future actions. You indicated last week this litigation may guide how other courts handle similar requests. Could you elaborate on that, please?

COMEY:

Sure. There's no -- first of all, let me say this. I've been trying to explain to people this case in San Bernardino is about this case, and the reason I've tried to say that so much publicly is I worry very much about the pain, frankly, to the victims in this case when they see this matter that's so important to them becoming a vehicle for a broader conversation.

So I want to make sure that everybody, especially the FBI remains grounded in the fact this is about that case. My wife has a great expression she uses to help me be a better person which is it's not about you, dear. This case in San Bernardino is not about the FBI, it's not about Apple, it's not about Congress, it's not about anything other than trying to do a competent investigation in an ongoing active case.

That said, of course, any decision by a judge in any form is going to be potentially precedential in some other form, not binding, but guidance, either positive or against. The government lost a case yesterday in Brooklyn, we could lose the case in San Bernardino and it would be used as precedent against the government. That's just the way the law works, which I happen to think is a good thing.

CONYERS:

Thank you. If you succeed in this case, will the FBI return to the courts in future cases to demand that Apple and other private companies assist you in unlocking secure devices?

COMEY:

Potentially, yes. If the All Writs Act is available to us and if the relief under the All Writs Act as explained by the courts fits the powers of the statute, of course.

CONYERS:

And finally, I think we can acknowledge then that this case will set some precedent. And if you succeed, you will have won the authority to access encrypted devices, at least for now. Given that you've asked us to provide you with that authority since taking your position at the Bureau and given that Congress has explicitly denied you that authority so far, can you appreciate our frustration that this case appears to be little more than an end run around this committee?

COMEY:

I really can't, Mr. Conyers. First of all, I don't recall a time when I've asked for a particular legislative fix. In fact, the administration's position has been they're not seeking legislation at this time.

But also we're investigating a horrific terrorist attack in San Bernardino. There's a phone that's unlocked that belonged to one of the killers. The All Writs Act we've used since I was a boy, we think is a reasonable argument to have the court to use the All Writs Act to direct the company to open that phone. That's what this is about. If I didn't do that, I ought to be fired, honestly.

I can also understand your frustration at the broader conversation because it goes way beyond this case. This case will be resolved by the courts, it does not solve the problem we're all here wrestling with.

CONYERS:

I thank the director. And I yield back any unused time. Thank you, Mr. Chairman.

GOODLATTE:

Thank you. And the chair recognizes the gentleman from Ohio, Mr. Chabot, for five minutes.

CHABOT:

Thank you, Mr. Chairman. I have a statement from the Application Developers Alliance here that I'd like to have included in the record.

GOODLATTE:

Without objection, it will be made a part of the record.

CHABOT:

Thank you, Mr. Chairman. And Director Comey, like yourself I happen to be a graduate of the College of William & Mary, so I'm going to start with a tough question. Anything nice you'd like to say about the College of William & Mary?

(LAUGHTER);

COMEY:

I could tell there was a glow coming from your seat. That's explained by your being a member of the Tribe. Best thing that ever happened to me beside -- I actually met my wife there. That's the best thing that happened to me, second best is that I was there.

CHABOT:

Excellent. Yeah, it's a great place to go. There's two members currently -- Ms. Titus of Nevada is also a graduate. Now, this hearing is about electronic data security, or as you...

GOODLATTE:

Chair is happy to extend additional time to the gentleman for recognizing an important Virginia educational institution.

(LAUGHTER)

CHABOT:

I appreciate the chairman. And as already indicated this is about electronic data security or as you described it keeping our stuff online private. So I'd like to ask you this, and it may seem a little off topic, but I don't think it is. A few weeks back, the FBI's general counsel James

Baker acknowledged that the FBI is, quote, "working on matters related to Former Secretary of State Hillary Clinton's use of a private e-mail server," unquote.

And then the White House Press Secretary Josh Earnest stated that, quote, "some officials over there" -- referring to the FBI -- "had said that Hillary Clinton is not a target of this investigation and that it's not trending in that direction," unquote. And the president then weighed in, even though he apparently had never been briefed on the matter, commenting that he didn't see any national security implications in Hillary's e-mails. And obviously this is a matter of considerable import.

Is there anything that you can tell us as to when this matter might be wrapped up one way or the other?

COMEY:

I can't. Congressman, as you know, we don't talk about our investigations. What I can assure you is that I am very close personally to that investigation to ensure that we have the resources we need, including people and technology, and that it's done the way the FBI tries to do all of its work: independently, competently and promptly. That's our goal. And I'm confident it's being done that way. But I can't give you any more details beyond that.

CHABOT:

I certainly understand and I appreciate it. I thought you might say that, but you can't blame me for trying. Let me move on. If Apple chose to comply with the government's demand, maybe it does have the technical expertise and time and finances to create such a vulnerability so we can get in and get that information.

But let me ask you, what about a small business? I happen to be the chairman of the House Small Business Committee. Wouldn't such a mandate to say a small company, a start-up, say with four or five, six employees, wouldn't that be a huge burden on a small business to have to comply with this sort of thing?

COMEY:

It might be. And that's one of the factors as I understand it, courts consider in passing on an All Writs Act request, the burden to the private actor, how much would it cost them and how much time and effort.

And I think Apple's argument in this case is it would take a ton of effort, time and money to do it and so that's one of the reasons we shouldn't be compelled to do it. So it's a consideration built into the judicial interpretations of the act.

CHABOT:

Thank you. As chair of the committee, we'd ask you certainly to consider how this could affect -- you know, seven out of ten new jobs created in the economy are small business folks, half of the people employed in this country in the private sector are small businesses. And I think we should always consider that.

Let me move onto something else. In this testimony from our December 2015 hearing about HR-699, the E-mail Privacy Act, Richard Littlehale, the assistant special agent in charge of Criminal Investigation Division of the Tennessee Bureau of Investigations, voiced a frustration with the increasing technological capabilities of both criminals and noncriminals.

Rather than trying to arguably infringe on the fourth amendment rights of all Americans, would it be possible to better train our law enforcement officers and equip them to keep up with this changing world that we're discussing today?

COMEY:

Well, there's no doubt that we have to continue to invest in training so that all of our folks are digitally literate and able to investigate in that way. The problem we face here is all of our lives are on these devices, which is why it's so important that they be private.

That also means all of criminals' and pedophiles' and terrorists' lives are on these devices. And if they can't -- if they're warrant proof, even if a judge can't order access to a device, that is a big problem. I don't care how good the cop is. I don't care how good the agent is, that is a big problem. So that we can't quite train our way around.



CHABOT:

Thank you very much. I'm almost out of time, so let me conclude with, go tribe, thank you.

GOODLATTE:

Chair thanks the gentleman, recognize the gentleman from New York, Mr. Nadler.

NADLER:

Thank you. Since we've gone a little far afield here, let me do so again very briefly to point out that among others, Thomas Jefferson, who among his minor accomplishments was the founder of the Democratic Party, he was also a graduate of William & Mary.

Mr. Comey -- Director Comey, the -- we're all certainly very condemning of the terrorist attack in San Bernardino. And we all -- our hearts go out to the families of the victims and I commend the FBI for everything you've done to investigate this matter.

Now, the two terrorists are dead and another co-conspirator, the neighbor, is in jail. You've used the USA Freedom Act to track their phone calls and investigate -- which this committee wrote last year -- to track their phone calls and investigate everyone they ever spoke to on that phone.

The FBI has done a great job already. Now let me ask you a few questions. It's my understanding that we have found that the attack in San Bernardino was not in any way planned or coordinated by ISIS, is that correct? It may have been inspired by it but not directed or planned by it.

COMEY:

Right. So far as we know, correct.

NADLER:

And you have -- have you eliminated any connection between the two suspects and any overseas terrorist organization?

COMEY:

Eliminated any?

NADLER:

Have you seen any evidence of any? That's a better way of putting it.

COMEY:

We have not seen any evidence of that.

NADLER:

OK. Now, given those facts, there's no evidence of coordination with anybody else, it's the two home grown, self-motivated, perhaps inspired by ISIS, terrorists. Now, the investigators seize the iPhone in question on December 3rd.

The FBI reached out to Apple for assistance on December 5th. Apple started providing the FBI with information -- I would gather from the information I gathered, the same day. But then the next day, on December 6th, at the instruction of the FBI, San Bernardino County changed the password to the iCloud account associated with that device.

They did so without consulting Apple at the instruction or suggestion of the FBI. And changing that password foreclosed the possibility of an automatic backup that would have allowed Apple to provide you with this information without bypassing its own security and thus necessitating in the first place, the application to the court that you made that we're discussing today.

In other words, if the FBI hadn't instructed San Bernardino County to change the password to the iCloud account, all this wouldn't have been unnecessary and you would have had that information. So my question, is why did the FBI do that?

COMEY:

I have to -- first of all, I want to choose my words very, very carefully. I said there is no evidence of direction from overseas terrorist organizations. This is a live investigation and I can't say much more beyond that. This investigation is not over. And I worry that embedded in your question was that you understood me to be saying that.

Second, I do think, as I understand from the experts, there was a mistake made in the -- in that 24 hours after the attack, where the county at the FBI's request, took steps that made it hard -- impossible later to cause the phone to backup again to the iCloud.

The experts have told me I'd still be sitting here -- I was going to say unfortunately -- fortunately, I'm glad I'm here. But we would still be in litigation because the experts tell me there's no way we would have gotten everything off the phone from a backup. I have to take them at their word, but you're -- either -- that part or premise to your question is accurate.

NADLER:

OK. So second part of my question -- excuse me. The second part of my question is, it wasn't until almost 50 days later, on January 22nd, when you served the warrant. Given the allegedly critical nature of this information, why did it take the FBI 50 days to go to court?

COMEY:

I think there were a whole lot of conversations going on in that interim with companies, with other parts of the government, with other resources to figure out if there was a way to do it short of having to go to court.

NADLER:

OK. Thank you. Now, getting off this specific case because I do think we all understand that it's not just a specific case. It will have widespread implications in law and however the courts resolve this, which is essentially a statutory interpretation case, the buck is going to stop here at some point.

We're going to be asked to change the law. So, encryption software is free, open-source and widely available. If Congress were to pass the law forcing U.S. companies to provide law enforcement with access to encrypt its systems, would that law stop bad actors from using their own encryption?

COMEY:

It would not.

NADLER:

It would not. So the bad actors would just get around it.

COMEY:

Sure. Encryption's always been available to bad actors -- nations...

NADLER:

So if we were to pass a law saying that Apple and whoever else had to put back doors or whatever you want to call them into their systems, the bad actors -- and with all the appropriate -- with all the -- not appropriate, all the concomitant surrenders of privacy, et cetera, the bad actors could easily get around that by making their own encryption systems?

COMEY:

The reason I'm hesitating is I think we're mixing together two things, data in motion and data at rest. The bad guys couldn't make their own phones, but the bad guys could always try and find a device that was strongly encrypted. The big change happened in the fall of 2014 when the companies flipped from available encryption to default. And that's the shadow going dark in an apartment.

NADLER:

Yes, but couldn't foreign companies and bad actors generally do that? Whatever we said?

COMEY:

Sure, potentially people could say I love this American device but because I worry about a judge ordering access to it, I'm going to buy this phone from a Nordic country that's different in some way. That could happen. I have a hard time seeing it happen a lot, but it could happen.

NADLER:

Thank you. My time has expired. Thank you.

ISSA:

Chairman, what I would like to ask for your unanimous consent, some documents be placed in the record at this time. I'd like to ask for unanimous consent that patent number 02407302, patent...

GOODLATTE:

Without objection.

ISSA:

Thank you. Additionally 27353, another patent. Additionally, a copy of the USA Today, entitled, "Ex-NSA Chief Backs Apple on iPhone". Additionally, from science and technology, an article that says "Department of Homeland Security awards \$2.2 million to Malibu, California company for mobile security research and in other words, an encryption-proof, unbreakable phone.

Additionally and lastly, the article in Politico today on the New York judge's ruling in favor of Apple.

GOODLATTE:

Without objection they will all be made a part of the record.

ISSA:

Thank you, Mr. Chairman.

GOODLATTE:

Gentleman is recognized for five minutes.

ISSA:

Thank you Mr. Chairman. Justice Scalia said it's best -- said best what I'm going to quote almost 30 years ago in *Arizona v. Hicks*, in which he said, "there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of all of us." I think that stands as a viewpoint that I want to balance when asking you questions.

As I understand the case, and there's a lot of very brilliant lawyers and experienced people that know about All Writs Act, but what I understand is that you, in the case of Apple in California, are demanding through a court order that Apple invent something.

Fair to say that they have to create something. And if that's true, then my first question to you is, the FBI is the premier law enforcement organization, with laboratories that are second to none in the world.

Are you testifying today that you and/or contractors that you employ could not achieve this without demanding an unwilling partner do it?

COMEY:

Correct.

ISSA:

And you do so because you have researched this extensively?

COMEY:

Yes. We've worked very, very hard on this. We're never going to give up, but we've worked...

ISSA:

Did you receive the source code from Apple? Did you demand the source code?

COMEY:

Did we ask Apple for their source code? I don't -- not that I'm aware of.

ISSA:

OK. So you couldn't actually figure -- hand a software person the source code and say, "can you modify this to do what we want," if you didn't have the source code.

So who did you go to, if you can tell us, that you consider an expert on writing source code changes that you want Apple to do for you? You want them to invent it, but who did you go to?

COMEY:

I'm not sure I'm following the question.

ISSA:

Well, you know -- I'm going to assume that the burden of Apple is X. But before you get to the burden of Apple doing something it doesn't want to do because it's not in its economic best interests and they've said that they have real ethical beliefs that you're asking them to do something wrong -- so to (ph) their moral fiber, but you are asking them to do something, and there's a burden.

No question at all -- there's a burden. They have to invent it. And I'm asking you, have you -- have you fully viewed the burden to the government? We have. We spend \$4.2 trillion every year. You have a multi-billion-dollar budget.

Is the burden so high on you that you could not defeat this product, either through getting the source code and changing it or some other means? are you testifying that?

COMEY:

I see. I -- we wouldn't be litigating if we could. We have engaged all parts of the U.S. government to see does anybody have a way, short of asking Apple to do it, with a 5c running iOS 9 -- to do this, and we do not.

ISSA:

OK. Well, let's go through the 5c running iOS 9. Is -- does the 5c have a non-volatile memory in which all of the encrypted data and the selection switches for the -- the phone settings are all located in that encrypted data?

COMEY:

I don't know.

ISSA:

Well, it does. And take my word for it for now.

So that means that you can, in fact, remove from the phone all of its memory -- all of its non-volatile memory -- its disk drive, if you will -- and set it over here, and have a true copy of it that you could conduct infinite number of attacks on.

Let's assume that you can make an infinite number of copies once you make one copy, right?

COMEY:

I have no idea.

ISSA:

Well, let's go through what you asked -- and I'm doing this because I came out of the security business, and this befuddles me, that you haven't looked at the source code and you don't really understand the disk drive -- at least to answer my rather -- you know, dumb questions, if you will.

If there's only a memory, and that memory -- that non-volatile memory sits here, and there's a chip, and the chip does have an encryption code that was burned into it, and you can make 10,000 copies of this chip -- this non-volatile memory hard drive -- then you can -- you can perform as many attacks as you want on it.

Now you've asked specifically Apple to defeat the finger code so you can attack it automatically, so you don't have to punch in codes. You've asked them to eliminate the -- the ten and destroy (ph).



But you haven't, as far as I know, asked them, "OK, if we make 1,000 copies or 2,000 copies of this and we put it with the chip and we run five tries -- 00 through 04 -- and then throw that image away and put another one in and do that 2,000 times, won't we have tried -- with a non-changing chip and an encryption code that is duplicated 2,000 times -- won't we have tried all 10,000 possible combinations in a matter of hours?"

If you haven't asked that question, the question is how can you come before this committee, and before a federal judge, and demand that somebody else invent something if you can't answer the questions that your people have tried this?

COMEY:

Firstly, I'm the director of the FBI. If I could answer that question, there'd be something dysfunctional in my leadership.

ISSA:

Now, I only asked if your people had done these things. I didn't ask you if that would work. I don't know if that would work. I asked you who did you go to -- did you get the source code?

Have you asked these questions? Because you're expecting somebody to obey an order to do something they don't want to do, and you haven't even figured out whether you could do it yourself.

You've just told us, "well, we can't do it," but you didn't ask for the source code, and you didn't ask the questions I asked here today, and I'm just a -- I'm just a guy that...

GOODLATTE:

The time of the gentleman has expired, and the director is permitted to answer the question.

COMEY:

I -- I did not ask the questions you're asking me here today, and I'm not sure I fully even understand the questions. I have reasonable confidence -- in fact, I have high confidence that all elements of the U.S. government have focused on this problem, and I've had great conversations with Apple.

Apple has never suggested to us that there's another way to do it other than what they've been asked to do in the All Writs Act. It could be, when the Apple representative testifies, you'll ask him and we'll have some great breakthrough, but I don't think so.

I'm totally open to suggestions. Lots of people have e-mailed ideas. I've heard about mirroring, and maybe this is what you're talking about. We haven't figured it out.

But I'm hoping my folks are watching this, and if you've said something that makes good sense to them, we'll jump on it. We'll let you know.

ISSA:  
Thank you.

GOODLATTE:  
The chair recognizes the gentlewoman from California, Ms. Lofgren, for five minutes.

LOFGREN:  
Thank you, Mr. Chairman. And thank you, Director Comey, for your service to our country and your efforts to keep us safe. It is appreciated by every member of this committee, and along with your entire agency, we do value your service and appreciate it.

I -- I remember, in law school, the phrase, "bad cases make bad law." I'm sure we all have heard that. And I think this might be a prime example of that rule.

We can't think of anything worse than what happened in San Bernardino -- two terrorists murdering innocent people. It's outrageous. It -- it -- it sickens us, and it sickens the country.

But the question really has to be, what is the rule of law here? Where -- where are we going with this? And as I was hearing your opening statement, talking about a world where everything is private, it may be that the alternative is a world where nothing is private.

Because once you have holes in encryption, the rule is it's not a question of if, but when those holes will be exploited, and everything that you thought was protected will be revealed.

Now, the United States law often tends to set international norms, especially when it comes to technology policy. And in fact, China removed provisions that required backdoors when its counterterrorism law passed in December because of the strong international norm against creating cyber weaknesses.

But last night, I heard a report that the ambassadors from America -- the United States, Canada, Germany and Japan sent a joint letter to China, because they're now thinking about putting a hole in encryption in their new policy.

Did you think about the implication for foreign policy, what China might do, when you filed the motion in San Bernardino? Or was that not part of the equation?

COMEY:

Yeah, I don't think -- I don't remember thinking about it in the context of this particular investigation, but I think about it a whole lot broadly, which is one of the things that makes it so hard.

There are undoubtedly international implications -- actually, I think less to the device encryption question, more to the data in motion question. But yeah, I have no doubt that there's international implications.

I don't have good visibility into what the Chinese require from people who sell devices in their country. I know it's an important topic.

LOFGREN:

Before I forget, Mr. Chairman. I'd like to ask unanimous consent to put in the record an op-ed that was printed in the Los Angeles Times today, authored by myself and my colleague Mr. Issa, on this subject.

GOODLATTE:

How could anyone object to that being part of the record?

(LAUGHTER)

LOFGREN:

I just note that, in terms of the -- you mentioned that the code at Apple -- that they've done a pretty good job of protecting their code, and you didn't remember anything getting out loose.

LOFGREN:

But I do think -- you know, if you take a look, for example, at the situation with Juniper Networks, where they had -- they -- their job is cybersecurity, really, and they felt that they had strong encryption, and yet there was a vulnerability. And they were hacked and it put everybody's data, including the data of the U.S., I mean, of the FBI and the State Department and the Department of Justice at risk and we still don't know what was taken by our enemies.

Did you think about the Juniper Networks issue when you filed the All Writs Act report, you know, remedy in San Bernardino?

COMEY:

No, but I think about that and a similar of similar intrusions and hacks all day long because it's the FBI's job to investigate those and stop those.

LOFGREN:

I was struck by your comment that Apple hadn't been hacked, but in fact, icloud accounts have been hacked in the past. I think we all remember in 2014 the female celebrity accounts that were hacked from the cloud, from icloud and CNBC had a report that China likely attacked icloud accounts. And then in 2015, last year, Apple had to release a patch in response to concerns that there had been brute force attacks on icloud accounts. So I'm anticipating, we'll see, that Apple will take further steps to encrypt and protect not only its operating system that it has today but also the protection as well as the icloud accounts.

And I'll just close with this. I have on my iPhone all kinds of messaging apps that are fully encrypted. Some better than others. Some were designed in the United States, a bunch of them were designed in other countries. And I'm not -- I wouldn't do anything wrong on my iPhone, but if I were a terrorist I could use any one of those apps and communicate securely and there wouldn't be anything that the U.S. government -- not the FBI, not the Congress or the president -- could do to prevent that from occurring.

So I see this as, you know, the question of whether my security is going to be protected but the terrorists will continue abate. And I thank you, Mr. Comey, for being here. I yield back, Mr. Chairman.

GOODLATTE:

The chair thanks the gentlewoman. And the chair recognizes the gentleman from Texas, Mr. Poe, for five minutes.

POE:

Thank you, Director. Appreciate you being here. Start with a little -- some basics. The Fourth Amendment protects citizens from government. Citizens have rights, government has power. There is nowhere I see in the Fourth Amendment that there is a "except for terrorist case" exception or fear case that the Fourth Amendment should be waived.

I signed lots of warrants in 22 years from everybody, including the FBI. Four corners of the warrant, what is to be searched, and law enforcement typically would fulfill the duty or ability in that warrant as far as they could, which is a good thing, and return the warrant.

Now we have a situation where the issue is not lawful possession. The FIB is in lawful possession of the San Bernardino phone, lawful possession of the phone in New York. You agree with me on that?

COMNEY:

Yes.

POE:

So we're not talking about whether the phones are in lawful possession, the issue is whether -- the specific issue is whether government can force Apple in this case to give them the golden key to unlock the safe because they can't develop the key. I know that's kind of simplistic, but is that a fair statement or not?

COMEY:

No.

POE:

It's not?

COMEY:

I think it...

POE:

Well, let me ask you this. OK, you say it's not. Apple developed this software and gives it to -- and unlocks the phone, but this is not the only phone in question, is that correct? There are other phones that the FBI has in lawful possession that you can't get into.

COMEY:

Sure. Law enforcement increasingly encounters phones, investigations all over the place that can't be unlocked.

POE:

OK, so...

COMEY:

That's in the Baton Rouge case too.

POE:

All right, there are several. How many of those cases do you have in lawful possession that you want to get into the phone but you can't get into it because you don't have the software to break into it or to get into it?

COMEY:

I don't know -- I don't know the number. A lot.

POE:

A lot.

COMEY:

And they're all different, which is what makes it hard to talk about any one case without being specific about what...

POE:

But you're in lawful possession of all these phones. This is not the issue of whether the FBI lawfully possesses them. You have these phones, you can't get into them. Here's a specific phone, you want iPhone, Apple to develop software to get to this phone.

My question is what would prevent the FBI from then taking that software and going at all those other phones you have and future phones you see?

COMEY:

I see. This seems like a small difference, but I think it's actually kind of a big difference. The ask, the direction from the judge is not to have Apple get us into the phone, it's to have Apple turn off by developing software that will tell the phone to turn off the auto erase and the delay features so that we can try and guess the password.

And so in theory, if you had another 5C running iOS-9, which is what makes this relief possible, I mean it when I say it's obsolete because I understand the 6s, there is no door for us even to try and pick the lock on so it wouldn't work, but if there were phones in the same circumstances, sure. You could ask for the same relief from a court to try and make effective the search warrant.

POE:

So rather than giving you the key, it's really you want Apple to turn the security system off so you -- they can get into the phone or you can get into the phone.

COMEY:

Yeah. My homely was take away the drooling watchdog that's going to attack us if we try and open it. Give us time to pick the lock.

POE:

Or like the Viper system that Mr. Issa developed. Turn off the Viper system so you can get into the phone.

And it boils down to the fact of whether or not government has the ability to demand that occur. We have two court rulings, they're different; I've read the opinions. They different -- a little different cases. Would you agree, or not, Congress has to resolve this problem? We shouldn't leave it up to the judiciary to make this decision, Congress should resolve the problem and determine exactly what the expectation of privacy is in these particular situations of encryption or no encryption, key or no key. Would you agree or not?

COMEY:

I think that the courts are competent -- and this is what we've done for 230 years to resolve the narrow question about the scope of the All Writs Act, but the broader question we're talking about here goes far beyond phones or far beyond any case. This collision between public safety and privacy. the courts cannot resolve that.

POE:

So courts -- and only Congress should then resolve what is the expectation of privacy in this high-tech atmosphere of all this information stored in many different places -- on the cloud, on the phone, wherever it's stored. And would you agree or not? I'm just asking since Congress resolved this issue of expectation of privacy of the American citizens.

COMEY:



I think Congress certainly has a critical role to play. Like I said, since the founding of this country, the courts have interpreted the Fourth Amendment and the Fifth Amendment, so they are competent. That's an independent branch of government, but I think there's a huge role for Congress to play. And we're playing it today, I hope.

POE:

Well I agree with you. I think it's Congress responsibility to determine the expectation of privacy in this high- tech world. And I yield back, Mr. Chairman.

GOODLATTE:

The time of the gentleman has expired. The gentleman from Tennessee is recognized for five minutes. There is 9:45 remaining in this vote. I'll take a chance if the gentleman from Tennessee will.

COHEN:

If you want to go, I'll go or I'll come back.

GOODLATTE:

Well, I'm trying to move it along as...

COHEN:

Thank you.

GOODLATTE:

...and not keep the director any longer than we have to. So go ahead.

COHEN:

Director Comey, are there limitations that you could see in permitting the FBI or government in a court to look into certain records, certain type of cases, certain type of circumstances that you could foresee? Or do you want it open for any case where there could be evidentiary value?

COMEY:

I'm not sure I'm following you. I like the way we have to do our work, which is go to a judge in each specific case and show lawful authority and a factual basis for access to anybody's stuff.

COHEN:

But if -- but if we decided to pass a statute and we thought it should be limited in some way maybe to terrorism or maybe to something where you -- there's a reasonable expectation that a person's life is in jeopardy or that you could apprehend somebody who has taken somebody's life.

Have you thought about any limits because, you know, under what you're saying, you go to a court -- I mean, you can go to a court for cases that are not capital cases. And that's -- I don't think anybody here is --

But the public's fascinated or -- not, say, riveted on it, it's the fact that what happened in San Bernardino was so awful and if we can find some communication or some list of -- in the -- that was in the cloud that these people contacted, you know, Osama bin Laden's cousin and that they get the -- and find out that he had something to do with it, then that's important. But if you're talking about getting into somebody's information to find out who they sold, you know, two kilos or two bags or whatever, it's a whole different issue.

Where would you limit it if you were coming up with a statute that could satisfy both your interest in the most important cases and yet satisfy privacy concerns?

COMEY:

Yeah, I see. I'm sorry. I misunderstood the question. I don't know, and haven't thought about it well enough. And frankly, I don't think that ought to be the FBI making that -- offering that -- those parameters to you. There is precedent for that kind of thing. We can only seek wiretaps, for example, on certain enumerated offenses in the United States. So it has to be really serious stuff before a judge can even be asked, to allow us to listen to someone's communications in the United States. It can't just be any offense.

So there's precedent for that kind of thing, but I haven't thought about it well enough.

COHEN:

Thank you. Because I'm slow in getting up there to vote and the Republicans hit the (inaudible) real quickly, I'm going to yield back the balance of my time and start to walk fast.

GOODLATTE:

The chair thanks the gentleman.

The committee will stand in recess. We have two votes on the floor with seven minutes remaining in the first vote.

Mr. Director, we appreciate your...

(CROSSTALK)

(RECESS)

GOODLATTE:

The committee will reconvene and continue with questions for Director Comey.

And the chair recognizes the gentleman from Utah, Mr. Chaffetz, for five minutes.

CHAFFETZ:

Thank you, Mr. Chairman.

And to the director, thank you so much for being here. As I've mentioned before, my grandfather was a career FBI agent so I have great affinity for the agency and what you do and how you do it. They almost always make us proud.

But the big question for our country is, you know, how much privacy are we going to give up in the name of security. And as you said, there's no easy answer to that.

But when historically, with all the resources and assets of the federal government, all the expertise, all the billions of dollars, when has it been the function of government to compel or force a private citizen or a company to act as an agent of the government to do what the government couldn't do?

COMEY:

I suppose that's a legal question in lots of different circumstances. Private entities have been compelled by court order to assist, again, through the All Writs Act. New York Telephone is the Supreme Court case -- the seminal case on the topic.

CHAFFETZ:

So let's talk for a moment about what you can see and what you can do. With all due respect to the FBI, they did -- they didn't do what Apple had suggested they do in order to retrieve the data, correct? I mean, when they went to change the password, that kind of screwed things up, did it not?

COMEY:

Yeah, I don't know that that's accurate, actually. I -- I wasn't there, don't have complete visibility, but I agreed with the questioner earlier. There was an issue created by the effort by the county, at the FBI's request, to try and reset it to get into it quickly.

CHAFFETZ:

And -- and -- and if they didn't reset it, then they could have gone to a WiFi -- local WiFi -- a known WiFi access and performed that backup so they could go to the Cloud and look at that data, correct?

COMEY:

Right. You could get in the Cloud. Through that mechanism, anything that was backuppable, to make up a word -- the Cloud, but that -- that does not solve your full problem. I think I'd still be sitting here talking about it, otherwise.

CHAFFETZ:

But let's talk about what the government can see, on using a phone.  
And it's not just an iPhone, but you can look at metadata, correct?

COMEY:

Yes.

CHAFFETZ:

The -- the -- the metadata is not -- not encrypted, correct? If I called  
someone else, or that phone had called other people, all of that  
information is available to the FBI, correct?

COMEY:

In most circumstances, right -- metadata...

CHAFFETZ:

In this case -- let's talk about this case. You -- you want to talk about this  
case. You can see the metadata, correct?

COMEY:

My understanding is we can see most of the metadata.

CHAFFETZ:

How would you define metadata?

COMEY:

I was just going to say that. Metadata, as I understand it, is records of  
time of contact, numbers assigned to the particular caller or texter. It's  
everything except content. You can't see what somebody said, but you  
can see that I texted to you, in theory.

My understanding is, with texts in particular, that's tricky, particularly  
texting using iMessage. There's limitations to our ability to see the  
metadata around that. Again, I'm not an expert, but that's my  
understanding.

CHAFFETZ:

And do you believe that geolocation, if you're tracking somebody's actual -- where they are, is that content, or is that metadata?

COMEY:

My understanding is it depends upon whether you're talking historical or real-time, when it comes to geolocation data. But it can very much implicate the warrant requirement, and does, in the FBI's work, a lot.

CHAFFETZ:

So that's what we're trying to -- what I -- what's -- what's frustrating to me, being on judiciary, being the chairman of the Oversight Committee, there is nobody on this panel as -- in a republic representative of the people, that have been able to see what the guidance is post-Jones (ph) in understanding how you interpret and what you're actually doing or not doing with somebody's geolocation.

COMEY:

You've asked that of the FBI and not been able to get it?

CHAFFETZ:

The Department of Justice today (ph) have been asking for this for years. What's frustrating is the Department of Justice is asking for more tools, more compulsion, and we can't even see what you're already doing.

We can't even see to the degree you're using StingRays and how they work. I mean, I think I understand how they work, but what sort of requirements are there? Is it articulable suspicion? Is it -- is there a -- is there a probable cause warrant that's being used or needed?

And it's not just the FBI. I mean, you've got the IRS and Social Security and others using StingRays -- again, other tools that, I would argue, are actually content into the -- to somebody's life and not just the metadata that you are able to see.

So how do we get exposure? How do we -- how do we help you if we can't -- if you routinely refuse -- and I say "you", meaning the Department of Justice -- access and explaining to us what tools you already do have and what you can access? How is -- how do we solve that?

COMEY:

Yeah, I don't -- I don't have a great answer, sitting here. I'll go find out what's been asked for and what's been given. I like the idea of giving as much transparency as possible, because I think people find it reassuring, at least with respect to the FBI, to take cell phone -- cell phone tower simulators -- we always use search warrants.

And so that -- that shouldn't be that hard to get you that information.

CHAFFETZ:

What I worry about -- you may be responsible, but I don't know what the IRS is doing with them, and I have a hard time figuring out when that's -- when that is responsible.

Last comment, Mr. Chairman. To what degree are you able to access and get into -- either in this case or broadly -- are you able to search social media in general? And are you using that as an effective tool to -- investigate and combat what you need to do?

GOODLATTE:

The time of the gentleman has expired. The witness can answer the question.

COMEY:

Social media is a feature of all of our lives, and so it's a feature of a lot of our investigations. Sometimes it gives us useful information, sometimes not. It's hard to answer in the abstract. But it's a big part of our work.

GOODLATTE:

Chair thanks the gentleman, and recognizes the gentleman from Georgia, Mr. Johnson, for five minutes.

JOHNSON:

Thank you, Director Comey.

The framers of our Constitution recognized a right to privacy that Americans would enjoy. Fourth Amendment pretty much implies that right to privacy, does it not?

COMEY:

I'm not a constitutional scholar. I think a scholar, if he were sitting here, might say it's not the Fourth Amendment that's the source of the right to privacy. It's other amendments to the Constitution.

But that's a technical answer. The Fourth Amendment is critically important because it's a restriction on government power. You may not look at the people's stuff -- their houses, their effects -- without a warrant and without independent judiciary.

JOHNSON:

But it also grants, impliedly (ph), to the government, the Fourth Amendment, the authority to search and seize when -- when -- when the search or seizure is reasonable. Is that correct?

COMEY:

Again, to be technical, I think the answer is Congress has given the government that authority through statute. The Fourth Amendment...

JOHNSON:

Well, I mean, the Fourth Amendment...

COMEY:

... is a restriction on that authority.

JOHNSON:



... the Fourth Amendment says that the right of the people to be secure in their place -- in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no warrant shall issue not -- but upon probable cause, supported by oath or affirmation.

And what I'm reading into the Fourth Amendment is that the people do have a right to privacy, have a right to be secure in their persons, houses, papers and effects, but I'm also reading into it an implied responsibility of the government to, on occasion, search and seize.

Is -- would that be your reading of it also?

COMEY:

Yes.

JOHNSON:

And -- of course, upon probable cause. But there are some circumstances where, in the hot pursuit, or at the time of an arrest, there are some exceptions that have been carved out, to where a warrant is not always required to search and seize. Is that correct?

COMEY:

Yes. You mentioned one -- the so-called exigent circumstances doctrine, where if you're in the middle of an emergency and you're looking for a gun that a bad guy might have hid -- you know, in a -- in a car, or something, you don't necessarily have to go get the warrant.

If you have the factual basis, you can do the search, and then have the judge look at it and validate it.

JOHNSON:

Now, even in a situation where exigent circumstances exist, technology has now brought us to the point where law enforcement or government is preempted from being able to search and seize. Is that correct?  
Technology has produced this result.

COMEY:

Yeah, I think technology has allowed us to create zones of complete privacy, which sounds like an awesome thing until you really think about it. But those zones prohibit any government action, under the Fourth Amendment or under our search authority.

JOHNSON:

Well, it's actually a zone of impunity, would it not be? A zone where bad things can happen and the security of Americans can be placed at risk.

COMEY:

Potentially, yes, sir.

JOHNSON:

And that is the situation that we have with end-to-end encryption. Is that not correct?

COMEY:

I think that's a fair description -- where we have communications where, even with a judge's order -- can't be intercepted.

JOHNSON:

Now, you said that you were not a constitutional scholar, and neither am I. But does it seem reasonable that our -- that the framers of the Constitution meant to exempt any domain from its authority to be able to search and seize, if it's based on probable cause, or some exigent circumstance allows for a search and seizure with less than a warrant and a showing of probable cause?

COMEY:

I doubt that they -- obviously, I doubt that they imagined the devices we have today and the ways of communicating. But I also doubt that they imagined there would be any place in American life where law enforcement, with lawful authority, could not go.

And the reason I say that is the First Amendment talks about the people's homes. Is there a more important place to any of us than our homes? So from the founding of this country, it was contemplated that law enforcement could go into your house with appropriate predication and oversight.

So to me, the logic of that tells me they wouldn't have imagine any box or storage area or device that could never be entered.

JOHNSON:

So from that standpoint, to be a strict constructionist about the Constitution and the Fourth Amendment, it's ridiculous that anyone would think that we would not be able to take our present circumstances and shape current law to appreciate the niceties of -- of today's practical realities.

I know I'm rambling a little bit. But did you understand what I just said?

COMEY:

I understand what you said, sir.

JOHNSON:

Would you agree or disagree with me?

GOODLATTE:

Time for the gentleman has expired. The director may answer the question.

COMEY:

I think it's the kind of question that democracies were built to wrestle with and that the Congress of the United States is fully capable of wrestling with in a good way.

JOHNSON:

Well, we have been...

GOODLATTE:

The time for the gentleman has expired.

JOHNSON:

Thank you.

GOODLATTE:

The chair recognizes the gentleman from Pennsylvania, Mr. Marino for five minutes.

MARINO:

Thank you, chairman. Mr. Director, it's always a pleasure.

COMEY:

Same, sir.

MARINO:

I'm going to expand a little bit on one of Judge Pole's (ph) questions. Is the bureau asking Apple to simply turn over the penetration code for the bureau to get into or that you want the penetration code at your disposal? Do you understand what I'm saying?

COMEY:

As I understand the judge's order, the way it could work out here is that the maker of the phone would write the code, keep the phone and the code entirely in their office space and the FBI would send the guesses electronically. So, we wouldn't have the phone. We wouldn't have the code. And that's my understanding of it.

MARINO:

That's a good point to clarify. Because there's some -- been a lot of rumors out there. I'm going to switch to the courts a little bit here. Do you see the federal court resolving the warrant issue that the bureau's presently faced with, whatever way that decision eventually comes down, or should Congress legislate the issue now, if at all?

COMEY:

I don't -- I appreciate the question. I don't think that's for me to say. I do think the courts -- some people have said, so, in the middle of this terrorism investigation, why didn't you come to Congress?

Well, because we're in the middle of a terrorism investigation. And so, I think the courts will sort that out faster than any legislative body could but only that particular case. The broader question, as I said earlier, I don't see how the courts can resolve this tension between privacy and public safety we're all feeling.

MARINO:

Another good point. Given that most of the our social, professional and very personal information is on our desktop computers, our laptops and pads and now more than ever, on these things, what is your position on notching up the level at which members of the federal judiciary can approve a warrant to access critically valuable evidence to solve a horrific felony, particularly when fighting terrorism?

COMEY:

Do you mean making the threshold something above probable cause?

MARINO:

No, not the threshold. The judicial -- the federal judicial individuals making this decision. Right now I understand, it's a magistrate. When I was at the state level, we could do some things at sort of the magistrate level or the District Court, but then we had to go to the Superior Court and working in the federal system with you, we had to go to one or two different levels. What is your position on that?

COMEY:

I see what you're saying. So instead of having the magistrate judges decide these questions, the District Court might?

MARINO:

yes, and no disrespect to Magistrate Courts, I'm very good friends with a lot of those brilliant people who will eventually, I know, go to the bench. But, from a perspective of the public that a more narrowly defined, limited number of people making that decision concerning the electronics that we have?

COMEY:

Honestly, Congressman, I haven't thought about that. I agree with you, I have a number of friends who are magistrate judges and they are awesome and they think well and they rule well. I think they're fully capable of handling these issues. But I haven't thought about it well enough to react other than that.

MARINO:

OK. And just for the record, I've managed a couple of prosecution offices and I've never gone to the experts, whether it's in DNA or whether it's in these electronics that ask them did you complete everything that you should have completed.

GOODLATTE:

Thank you, Mr. Marino.

The chair recognizes the gentlewoman from California Ms. Chu, for five minutes.

CHU:

Director Comey, my district is next to San Bernardino. After the terror attack we mourned the loss of 14 lives and empathized with the 22 wounded. And there is indeed fear and anxiety amongst my constituents. So, our discussion here today is particularly important to the people back home. There are many in our area that want answers, but there are also many that feel conflicted about putting their own privacy at risk.

So, my first question to you is, under federal law we do not require technology companies to maintain a key to unlock encrypted information in the devices they sell to customers.

Some of the witnesses we'll hear from today argue that if such a key or software was developed to help the FBI access a device used by Syed Farook, it would make the millions of other devices in use today vulnerable.

How can we be sure that we're not creating legal or technical backdoors to U.S. technology that will empower other foreign governments in taking advantage of this loophole?

COMEY:

That's a great question. I think what you have to do is just talk to people on all sides of it who are true experts, which I am not, but I've also talked to a lot of experts. And I'm an optimist. I actually don't think we've given this the shot that it deserves. I don't think the most creative and innovative people in our country have had an incentive to try and solve this problem.

But when I look at particular phones -- in the fall of 2014, the makers of these phones could open them and I don't remember people saying the world was ending at that point and that we're all exposed. And so, I do think judgments have been made that are not irreversible, but I think the best way to get at it talk to people about it.

So why do you make the phone this way and what is the possibility?

The world I imagine is a world where people comply with warrants. How they do it is entirely up to them. Lots of phone makers and providers of e-mail and text today provide secure services to their customers and they comply with warrants.

That's just the way they've structured their business and so it gives me a sense of optimism that this is not an impossible problem to solve. Really, really hard and it will involve you all talking to the people who really know this work.

CHU:

Well, I'd like to talk about law enforcement finding technical solutions. I understand there may be other methods or solutions for law enforcement when it comes to recovering data on a smartphone.

Professor Landau argues in her testimony later today that solutions to accessing the data already exist within the forensic analysis community, solutions which may include jailbreaking the phone amongst others.

Or she says other entities within the federal government may have the expertise to crack the code. Has the FBI pursued these other methods or tried to get help from within the federal government such as from agencies like the NSA?

COMEY:

Yes, is the answer. We've talked to anybody who will talk to us about it and I welcome additional suggestions. Again, you have to be very specific; 5c running iOS-9, what are the capabilities against that phone? There are versions of different phone manufacturers and combinations of model and operating system that it is possible to break a phone without having to ask the manufacturer to do it.

We've not found a way to break the 5c running iOS-9. And as I said, in a way, this is kind of yesterday's problem because the 5c, although I'm sure it's a great phone, has been overtaken by the 6 and will be overtaken by others that are different in ways that make this relief yesterday.

CHU:

So, let me ask this, like smartphones, safes can be another form of storage of personal information. Similarly to how technology companies are not required to maintain a key to unlock encryption, safe manufacturers are not required to maintain keys or combinations to locks.

Given this, law enforcement has been able to find a way to get into safes under certain circumstances or obtain critical information through other avenues. So, how does this differ from unlocking a smartphone?

It's clear that technology is outpacing law enforcement's ability to get information from devices like the iPhone even with the proper warrant. But isn't it the FBI or the law enforcement agency who bears the responsibility to figure out the solution to unlock the code?

COMEY:



I'll take the last part, first. Sure, if we can figure it out. The problem with the safe comparison is there's no safe in the world that can't be opened. If our experts can't crack it we'll blow it up, we'll blow the door off. And so, this is different. The awesome, wonderful power of encryption changes that and makes that comparison frankly inept.

And so sure, where law enforcement can appropriately, lawfully figure out how to do it, we will and should. But there will be occasions and it's going to sweep across, again, with the updating of phones and the changing of apps where we communicate end-to-end encrypted, it's going to sweep across all of our work and outstrip our ability to do it on our own.

CHU:

Thank you, I yield back.

GOODLATTE:

The chair thanks the gentlewoman. The gentleman from South Carolina, Mr. Gowdy, is recognized for five minutes.

GOWDY:

Thank you, Mr. Chairman. Mr. Director, thank you for your service to the country. And I do appreciate your acknowledge and that of my colleagues, of the difficulty in reconciling competing, binary constitutional principles like public safety, national security and privacy.

And I confess up front, my bias is towards public safety. Because of this loosely held conviction I have that the right to counsel, the right to free speech, the right to a jury trial just isn't of much use if you're dead.

So, I reconcile those competing principles in favor of public safety. And my concern as I hear you testify, is that I have colleagues and others who are advocating for these evidence-free zones. They're just going to be compartments of life where you are precluded from going to find evidence of anything.

GOWDY:

And I'm trying to -- I'm trying to determine whether or not we as a society are going to accept that; that there are certain, no matter how compelling the government's interest is in accessing that evidence, we are declaring right now this is an evidence-free zone; you can't go here no matter whether it's a terrorist plot -- and I'm not talking about the FENE (ph) case. That's a drug case. The case the magistrate decided yesterday in New York is a drug case.

Those are a dime a dozen. National security? There's nothing that the government has a more compelling interest in than that, and we're going to create evidence-free zones? Am I missing something? Is that -- is that how you see it? You just can't go in these categories unless somebody consents?

COMEY:

That's my worry and why I think it's so important we have this conversation. Because even I on the surface think it sounds great when people say, "Hey, you buy this device; no one will ever be able to look at your stuff." But there are times when law enforcement saves our lives, rescues our children and rescues our neighborhoods by going to a judge and getting permission to look at our stuff.

And so again, I come to the case of the Baton Rouge, eight-month pregnant women, shot when she opens her door. He mom says she keeps a diary on her phone. We can't look at the diary to figure out what might have been going on in her life. Who was she texting with? That's a problem. I love privacy. But all of us also love public safety and it's so easy to talk about buy this amazing device; you'll be private.

But you have to take the time to think: OK, there's that, and what are the costs of that? And that's where this collision is coming in.

GOWDY:

Well, I love privacy, too, but I want my fellow citizens to understand that most of us also in varying degrees also love our bodies and the physical integrity of our body. But since Schmerber (ph), the government has been able to access orders for either blood against the will of the defendant, or in some instances surgical procedures against the will of the defendant.

So, when I hear my colleagues say: Have you ever asked a nongovernment actor to participate in the securing of evidence? Absolutely. That's what the surgeon does. If you have a bullet from an officer who was shot, and a defendant, you can go to a judge and ask the judge to force a nurse or surgeon to anesthetize and remove that bullet.

So if you can penetrate the integrity of the human body in certain categories of cases, how in the hell you can't access a phone, I just find baffling.

But let me ask you this. If Apple were here, and they're going to be here, how would they tell you to do it? If there were a plot on an iPhone to commit an act of violence against, say hypothetically, an Apple facility, and they expected you to prevent it, how would they tell you to access the material on this phone?

COMEY:

I think they would say what they've said, which I believe is in good faith, that we have designed this in response to what we believe to be the demands of our customers to be immune to any government warrant, or our -- the manufacturer's efforts to get in that phone. We think that's what people want.

And that may be so, except I would hope folks would look at this conversation and say: Really? Do I want that? And take a step back and understand that this entire country of ours is based on a balance. It's a hard one to strike, but it's so seductive to talk about privacy as the ultimate value. In a society where we aspired to be safe and have our families safe and our children safe, that can't be true.

We have to find a way to accommodate both.

GOWDY:

So -- so Apple on the one hand wants us to kind of weigh and balance privacy, except they've done it for us. They have said, at least as it relates to this phone, we've already done that weighing and balancing and there is no governmental interest compelling enough for us to allow you to try to guess the password of a dead person's phone that is owned by a city government.

I -- there's no balancing to be done. They've already done it for us. I would just -- I would just tell you, Director, in conclusion, we ask the bureau and others to do a lot of things -- investigate crime after it's taken place; anticipate crimes; stop it before it happens. And all you're asking is to be able to guess the password and not have the phone self-destruct. And you can go into people's bodies and remove bullets, but you can't go into a dead person's iPhone and remove data. I just find it baffling, but I'm out of time.

GOODLATTE:

The gentleman's time has expired.

The chair recognizes the gentleman from Florida, Mr. Deutch, for five minutes.

DEUTCH:

Thank you, Mr. Chairman.

Director Comey, thank you for being here. Thank you for your service and that of the men and women who work for you. We're all grateful for what they do.

And I just wanted to take a moment before I ask you a couple of questions here to let you know that Bob Levinson, who was an agent for over 20 years, 28 years at the Justice Department, continues to be missing. I want to thank you for what you've done. I want to thank you for the Facebook page in Farsi that you've put up. I'd love a report on the effectiveness and what you've heard from that.

And I want to more than anything else, on behalf of Bob's family, I want to thank you for -- for never forgetting this former agent. And I'm grateful for that.

COMEY:

Thank you, sir. He'll never be forgotten.

DEUTCH:

Now, I want to agree with Mr. Gowdy that if this were as easy as public safety or privacy, I think most of us, probably all of us, if we had to make the choice, we're going to opt for public safety for the very reason that Mr. Gowdy spoke of.

But what I'm -- I have some questions. What I'm confused about is this. The tool that you would need to take away the dogs, take away the vicious guard dogs, is a tool that would disable the auto-erase. There's some confusion as to whether there's an additional tool that you're seeking that would allow you to rapidly test possible pass codes. Is there a second tool as well?

COMEY:

Yes, I think there's actually three elements to it. And I've spoken to experts. I hope I get this right. The first is what you said, which is to disable the self-destruct, auto-erase type feature. The second is to disable the feature that between successive guesses, as I understand, the IOS-9 (ph). It spreads out the time. So even if we got the ability to guess, it would take years and years to guess. So do away with that function.

And the third thing is, which is smaller, is set it up so that we can send you electronic guesses, so we don't have to have an FBI agent sit there and punch in 1-2-3-4, 1-2-3, like that.

DEUTCH:

And once they created that, would you expect them -- after this case, would you expect them to preserve that or destroy it?

COMEY:

I don't know. It would depend on what the judge's order said. I think that's for the judge to sort out. That's my recollection.

DEUTCH:

And so, here's the issue. I think that vicious guard dog that you want to take away, so that you can pick the lock, is one thing. But in a world where we do -- I mean, it's true -- there are awful people, terrorists, child predators, molesters who do everything on here. But so -- so do so

many of the rest of us. And we would like a pack of vicious guard dogs to protect our information to keep us safe. Because there's a public safety part of that equation as well.

And the -- the example of surgical procedures, the reason that I don't think applies here is because in that case, we know the only one doing the surgical procedure is the doctor operating on behalf of law enforcement. But when this tool is created, the fear obviously is that it might be used by others; that there are many who will try to get their hands on it, and will then put at risk our information on our devices.

And how -- do you -- how do you balance it? It's -- I don't -- this a really hard one for me. This isn't an either-or. I don't see it as (inaudible) option. So, how do you do that?

COMEY:

I think it's a reasonable question. I also think it's something the judge will sort out. Apple's contention, which again I believe is made in good faith, is that there would be substantial risk around creating this software. On the government side, count us skeptical, although we could be wrong, because I think the government's argument is: That's your business to protect your software, your innovation. This would be usable in one phone.

But again, that's something the judge is going to have to sort out. It's not an easy question.

DEUTCH:

If -- if it's -- it's the case, though, that it's usable in more than one phone, and that it applies beyond there, then the public safety concerns that we may have, that a lot of us have about what would happen if the bad guys got access to our phones and our children's phones, in that case, those are really valid, aren't they?

COMEY:

Sure. The question that I think we're going to have litigation about is how reasonable is that concern. And, you know, slippery slope arguments are always attractive, but I mean, I supposed you could say, well, Apple's engineers have this in their head. What if they're

kidnapped and forced to write software? That's why the judge has to sort this out, between good lawyers on both sides making all reasonable arguments.

DEUTCH:

And I -- just finally, Mr. Chairman, I just worry when we talk about the precedential value, the discussion is taking place wholly within a domestic context. There are countries around the world where we know very well that the governments do their best to monitor what happens in their country, and through people's cell phones are able to squash dissent, are able to take action to throw people in jail and to torture people.

And I think that precedential value is something else that we have to bear in mind as we engage in this really important, really difficult debate. And I yield back, Mr. Chairman.

GOODLATTE:

The chair thanks the gentleman.

GOODLATTE:

And recognizes the gentleman from Florida, Mr. DeSantis for five minutes.

DESANTIS:

Good afternoon, Director Comey. When you're looking at a case like the Apple case and you want to be able to, as you said, remove the guard dogs and then the FBI go in, are you concerned about preserving the evidentiary value that can then we used, or are you more interested in just getting the information for intel purposes so that you can use that for counterterrorism?

COMEY:

Our hope is to do both, but if we have to choose, we want the information first and then we'd like it obviously to be in a form that could be used if there was a court proceeding against somebody someday.

DESANTIS:

But I guess is there -- are there instances in which maybe a company would provide the data but would provide it to you in a way that you would not necessarily be able to authenticate that in court?

COMEY:

Sure, that happens all the time.

DESANTIS:

And that's something that the FBI -- if that's what you get, then you're fine with that?

COMEY:

It depends upon the case, but in general, that's a tool that we use, private cooperation where we may not be able to use the information in court.

DESANTIS:

And in terms of this, the guy in San Bernardino, it wasn't even his phone and then the owner of the phone has consented for the FBI to have the information. Is that correct?

COMEY:

Right. We have a search warrant for the phone. The guy who was possessing it is obviously dead, and the -- and the owner of the phone has consented.

DESANTIS:

What's the best analogous case to what you're trying to do here? Because people will look at it and say, well, you're basically commandeering a company to have to do these things, that's typically not the way it works. So what would you say is the -- outside of the technology context, what would be an analogous case?

COMEY:



Well, everyone in the United States to some degree has an obligation to cooperate with appropriate authority. The question that the court has to resolve under the All Writs Act is what are the limits of that. Apple's argument is that might be OK if it's -- requires us to hand you something we've already made, to open a phone, but if we're going to make something new, that's beyond the scope of the law.

As you know, that's something courts do every day in the United States, trying to understand a law and interpret its scope based on a particular set of facts. So that's what'll be done in San Bernardino, in a different context it's being done in Brooklyn, in the -- in the drug case in Brooklyn. I think it's being done in different stages all over the country because in investigation after investigation law enforcement is encountering these kind of devices.

DESANTIS:

Have you -- in your cases have you gotten an order under the All Writs Act to just have a defendant, if you have a search warrant, produce the code?

COMEY:

I don't know of a -- I don't of a similar case.

DESANTIS:

In terms of -- I know some of the technology companies are concerned about if they're creating ways to I guess penetrate their systems, that's creating, like, a back door. And my -- I guess my concern is terrorists obviously want to operate in a variety of spheres. One of the ways that they get a lot of bang for their buck is cyber attacks. And so if companies were creating more access for law enforcement in some of these situations, would that create more vulnerability for people and be more likely that they were subjected to a potential cyberattack?

COMEY:

Potentially, sure. If there were access tools that got loose in the wild or that could be easily stolen or available to bad people, it's a concern. As I said, a huge part of the Bureau's work is protecting privacy by fighting against those cybercriminals, so it's something we worry about every day.

DESANTIS:

Well how would you, then, provide assurances if you're requesting a company to work with you that this doesn't get out into the wild so to speak?

COMEY:

Well, I think in the particular case, we have confidence, I think it's justified, that Apple is highly professional at protecting its own innovation and its own information. So the idea here is you keep it. You figure out how to store it. You even take the phone and protect it. I think that's something they do pretty well. But, again, that is something the judge will sort out.

Apple's argument I think will be that's not reasonable because there are risks around that. Even though we're good at this, it could still get away from us and the judge will have to figure that out what's reasonable in that circumstance.

DESANTIS:

Great. Thank you. I yield back the balance of my time.

GOODLATTE:

The chair thanks the gentleman and recognizes the gentleman from Illinois, Mr. Gutierrez.

GUTIERREZ:

Thank you, Mr. Chairman. And thank you, Director Comey, for coming in and being here with us this afternoon. I won't take my five minutes so I'll make a couple of comments and -- beginning by saying that I hope all of the members of the committee will take note that the director is actually answering our questions, and that is obviously very refreshing in that we get a lot of witnesses here and if they bring them, we might

not like them, if we bring them, they don't seem to like them. And it's good to get information without passing judgment. And I think that's what you've done very well here today.

You're not passing judgment on Apple and their motivations. And I think in not questioning people's motivation it's easier to get a solution. Because once you do that, everybody kind of says, OK, let's get all our defenses up, and really what we need to be doing is defending the American people and not Apple or any company or the FBI for that matter, but defending the American people. So I want to thank you for that.

And I just want to suggest that we continue these conversations. I buy a house, I have no reasonable expectation that if you get a warrant you're going to go into my -- any drawer in my bedroom. When I buy the house, I don't have any expectation of privacy once you get a warrant to come.

And I do expect you to get one. I come from a time when I wasn't quite sure the Chicago Police and law enforcement was actually getting warrants in the City of Chicago in the 1960s to get that, so we want to be a little careful and make sure.

I'm trusting of you. If you were the FBI agent, I'd say no problem, Director Comey, come on in. But unfortunately, there are human beings at all the different levels of government, and I just want to say that I'm happy you came because I don't -- I don't have that expectation in my car. I don't have that expectation in -- I don't use the computer a lot, I still write, I don't have any expectation.

But the difference is, and I think you've made it and I think this committee should take it into consideration, we do put a lot of information in these contraptions, and the reason we put them there is because we don't want to put them on a notebook, we want to keep them private. But I don't have any expectation -- I really don't have any expectation once I put this if you have a lawful warrant you should be able to get it even from my computer, if you have...

I think that's where you're going. Could you -- is that where you think -- have I heard you right?

COMEY:

I do. I agree with you, except I think the case for privacy's even stronger than you said. You do have a reasonable expectation of privacy in your home, in your car and in your devices. The government under our Constitution is required to overcome that by going to an independent judge, making a showing of probable cause and getting a warrant.

We need to talk about as a country is we're moving to a place where there are warrant-proof places in our life. And yes, these devices are spectacular because they do hold our whole lives. They're different than a briefcase. They're different than a drawer. So it is a source with -- a place with a tremendous reasonable expectation of privacy. But if we're going to move to a place where that is not possible to overcome that, that's a world we've never lived in before in the United States.

That has profound consequences for public safety, and all I'm saying we shouldn't drift there, right? Companies that sell stuff shouldn't tell us how to be, the FBI shouldn't tell us how to be. The American people should say the world is different. How do we want to be and figure that out.

GUTIERREZ:

Yeah, I think that's -- I think we're on the same place, then, because I do have a reasonable expectation of privacy in my home. But if you go to court, you convince the judge and you overcome it, I have never had any expectation that a court order, because I bought something, a court -- I'm going to be able to overcome a court order. So I think we're in the same place.

So thank you so much, Director, for coming in and sharing your time. I hope you can share more time so we can talk some more. Thank you.

GOODLATTE:

The chair recognizes the gentleman from Iowa, Mr. King for five minutes.

KING:

Thank you, Mr. Chairman. Director, thanks for your testimony here and your leadership of the FBI.

I'm curious about this from a -- from a perspective that has to do with our global war against radical Islamic terrorists. And I have laid out a strategy to defeat that ideology. I would take it back to our ability some years past to be able to identify their cell phones and get into their -- get into their cell phones in such a way that we also got into their heads which drove them into the caves and really it diminished a lot of their otherwise robust activity that they might have -- that al Qaeda might have carried out against us. I think that was a successful effort.

Now we have a global cyberoperations going on with I think by your numbers from a previous report I read well over 100,000 ISIS activities on Twitter and other cyberactivity in a single day. And so I'm interested in how the parameters that have been examined thoroughly by a lot of the lawyers on this panel might apply to an all-out cyberwarfare against ISIS and any of their affiliates or subordinates that I think is necessary if we're going to defeat that ideology.

And so I'm thinking in terms of if this Congress might diminish, slow down or shut down access to this phone, it also means access to any other phone that they might be using. They would have a high degree of confidence that they could operate with a level of impunity in the cyberworld out there.

KING:

Do you have any comments you'd like to make on the implications that being locked out of a opportunity to unlock this phone might mean to a global war on terror that could be prosecuted in the next administration, aggressively across the fields of cyber warfare?

I would just add to that for the sake of enumerating them, financial warfare, educational warfare and human intelligence and the network that would be necessary, not just the kinetic activity, to defeat radical Islamic terrorism.

COMEY:

Thank you, Mr. King. This conversation we're having today and I hope will continue is really important for domestic law enforcement, but it has profound implications for among other things, our counterterrorism work.

Because since Mr. Snowden's revelations, terrorist trade craft changed. And they moved immediately to encrypted apps for their communication and trying to find devices that were encrypted, wrap their lives in encryption, because they understand the power of encryption. And so there's no place we see this collision between our love for privacy and the security of encryption and public safety than in fighting terrorism, especially ISIL.

Because for the FBI's responsibility which is here in the United States, every day we're looking for needles in a haystack and increasingly the most dangerous needles go invisible to us because that's when ISIL moves them to an encrypted app that's end-to-end encrypted and a judge's order is irrelevant there.

That's why this is such an urgent feature of our work. It has huge implications for law enforcement overwhelmingly, but it has profound implications in the fight against terrorism.

KING:

Do you get any signals that the American public or the United States Congress is contemplating some of the things that you've discussed here to the depth that it would be a component in the decision making?

COMEY:

I don't know. I know everybody's interested in this and everybody, all thoughtful people, see both sides of this and are trying to figure out how to resolve it, how to resolve it practically, how to resolve it technically and the other challenge is not to make it harder.

There is no it. There isn't a single it. There's all different kinds of manifestations of this problem we call going dark. So what I see is, people of goodwill who care about privacy and safety, wrestling with this. Court cases are important but they are not going to solve this problem for us.

KING:

Let me suggest that -- I'll just say I think it's a known and a given that ISIS or ISIL is seeking a nuclear device. And pretty much said that publicly. If we had a high degree of confidence that they had -- that they

were on the cusp of achieving such capability and perhaps a capability of delivering it, if that became part of the American consciousness, do you think that would change this debate that we're having here today?

COMEY:

I do worry that it's hard to have nuanced, complicated conversations like this in an emergency and in the wake of a disaster, which is why I think it's so important we have this conversation now. Because in the wake of something awful happening, it will be hard to talk about this in a thoughtful, nuanced way. And so I think that's why I so welcome the chairman having this hearing and having further conversations about it.

KING:

I thank you, director. And I will just state that my view is that I want to protect the constitutional rights of the American people, and I'd like to be able to have this framed in law that reflects our constitutional rights.

But I would like to have us consider how we might keep a nation safe in the face of this and how we might prosecute a global war against radical Islam, even in the aftermath of a decision that might be made by either a judge or the United States Congress.

I thank you, Mr. Chairman, and I yield back the balance of my time.

GOODLATTE:

Chairman thanks the gentleman. The gentlewoman from California, Ms. Bass, is recognized for five minutes.

BASS:

Thank you, Mr. Chair, and thank you, Director Comey, for your time and your patience with us today. I had a town hall meeting in my district on Sunday and actually a couple hundred people showed up. And it was a general town hall meeting talking about issues that Congress is dealing with.

And much to my surprise, this was a burning issue. And many of my constituents came to ask me questions and I told them that they could suggest some questions and I would ask you. And maybe you could speak to some of my constituents today so I can send them a clip of your testimony.

Basically, in general, they had a hard time believing -- I mean, they were not supportive. They don't want, you know, Apple to comply. But they had a hard time believing that the FBI couldn't already do this and so a couple of the questions were, how have so many others cracked iPhones and shared their findings with videos and how-to articles?

And given that you described it not as a back door but getting the dogs, you know, away so that you can pick the lock, their question was, what other intelligence community agencies has the FBI worked with, considering there's at least 12 in the government. Between all of these agencies, how is it that you haven't been able to call the dogs off and pick the lock?

COMEY:

Actually, 16 other members of the U.S. intelligence community. It pains me to say this, because I -- in a way we benefit from the myth that is the product of maybe too much television, the only thing that's true on television is we remain very attractive people, but we don't have the capabilities that people sometimes on TV imagine us to have.

If we could have done this quietly and privately, we would have done it. Right? This litigation is difficult. It's especially difficult as I said, for the people who were victimized in San Bernardino and so we really can't. As I said, there may be other models, other permutations and combinations where we have different capabilities.

But I'm here to tell you, here -- and again, maybe tonight someone will call us and say I thought of something. Apple is very good at what it does. It's a a wonderful company who makes wonderful products, right? They have set out to design a phone that can't be opened.

And they are darn near succeeding. I think with the 6 and beyond they will have succeeded. That doesn't make them bad people, that just poses a challenge for us that we're not yet up to meeting without intervention from courts.



BASS:

Since you can clone iPhone contents to compatible hardware and test passwords on the clones without putting the original at risk, can't you use so-called brute force methods to guess the pass code?

COMEY:

Not with -- I think this is what Mr. Issa was asking about. I think a lot of tech experts ask, why can't you mirror the phone in some way and then play with the mirror. For reasons I don't fully understand, not possible in this circumstance.

So we do want to try and brute force the phone, that is the multiple guesses. But we need first -- we'll do that ourselves, but we need removed the auto-erase function and the delay between guesses function which would make us take ten years to guess it.

If we have those removed, we can guess the phone's password with our computing power in 26 minutes is what we're told, because we have enormous computing power in the U.S. government. But we need to be able to bring it to bear without the phone killing itself.

BASS:

Thank you. I yield back the balance of my time.

GOODLATTE:

The chair recognizes the gentleman from Idaho, Mr. Labrador, for five minutes.

LABRADOR:

Thank you, Mr. Chairman, thank you Director for being here. Thank you for what you're doing. I know you have a very difficult job as you are trying to balance both security and privacy. I do have a few questions.

As you -- as you are looking at the laws that are in place like CALEA and FISA or the other different avenues that we're talking about, something that concerns me is that this is very different than some of the examples that have been given here.

For example, when you have -- when you're going into a home, if you're asking for a key, if you go to the landlord, the key's already made. And you can go to the landlord and you can say, I have a warrant here and that key is made. Can you please give me a key for that? Or the method of creating that key even if the key does not exist is already -- does already exist. This is very different than that. Would you agree?

COMEY:

Yes. Exactly right. There's a difference between, hey, landlord, you have this spare key. Judge directs you to give it to us. Hey, landlord, we need you to make a key for this lock. That's a legal question as to whether the particular statutory authority we're using here, the All Writs Act extends to that.

LABRADOR:

Right.

COMEY:

We think in the government, there's a reasonable argument to be made it does and should and on the other side, lawyers for Apple argue it doesn't and that's what the judge will sort out.

LABRADOR:

But this goes even one step further. In this scenario the landlord can create the key, has the ability to create the key and the technology to create this key already exists.

In the Apple case, that's not the case. They have never created the key that you're asking for, isn't that correct?

COMEY:

I don't know whether that's correct or not.

LABRADOR:

Well, as far as we know, as far as they're letting us know, there's no way for them as they're telling it -- because if not, I think they would be violating the judge's order. If they have an ability to do this, I do agree with you that they would be violating the judge's order, but what they're telling us that the ability does not exist. Isn't that correct?

COMEY:

I think that's right. I think obviously, their general counsels are very smart guys here, he can talk about this. But I think what they're saying is we can do it but it requires us to sit at a keyboard and write new code that doesn't currently exist.

Whether there's a meaningful distinction between that and someone who already has a key legally, is something a judge will have to sort out.

LABRADOR:

So what concerns me is the old legal maxim that you know, bad cases make bad law. This is clearly a bad case. We all want you to get access to this phone through legal means because maybe it would uncover some of the problems that we have in the Middle East.

LABRADOR:

Maybe there's some evidence in there that could really lead us to take some terrorists down. I think we are all there. But the problem is that this is a bad case. This is a person who obviously is dead, who does -- has never given his code to somebody else.

And -- and I'm concerned that -- that as we're looking down this road, what we're doing is we're opening the door for other -- other things that could actually be detrimental to -- to our safety and security. For example, I think you've testified many times that we're getting hacked all the time, isn't that correct?

COMEY:

Yes.

LABRADOR:

So maybe one of the reasons that Apple is refusing to do this, or -- or is hesitant to do something like this -- because they know that even they get hacked. And when you open -- when you create that key that doesn't exist at all right now, you're actually opening up every other phone that's out there.

Do you -- do you see how that could be a concern?

COMEY:

I see the argument. The question the judge will have to decide is, is that a reasonable argument.

(CROSSTALK)

LABRADOR:

I'm sorry, no, (inaudible).

COMEY:

OK.

LABRADOR:

You said that Apple is highly -- they are -- they are highly professional in keeping secrets. Would you say that the federal government also has very good people that are highly professional in keeping secrets?

COMEY:

Parts of it.

(UNKNOWN)

Me, too.

LABRADOR:

Recently, we've learned that there's been a hacking incident at the IRS. Are you -- are you familiar with that?

COMEY:

Yes.

LABRADOR:

So that's -- that's what I'm concerned about. The moment that you open up that door, the -- the moment that you open up that key that doesn't currently exist, you're actually allowing all these hackers that are out there -- and some of them are our enemies that are trying to do us harm, whether it's economic harm or whether it's actual terrorism -- they're out there looking for ways to actually get into your iPhone, into my iPhone, into everybody else's iPhone.

And at some point -- that's why you have such a difficult job, is we have to balance that safety and security. Do you think that this capability that you're asking for will -- can only be used pursuant to a warrant?

COMEY:

The capability that the judge has directed Apple to provide?

LABRADOR:

Correct (ph).

COMEY:

I think that's the way it's -- that's the procedural posture of it -- there's a warrant, and the judge is (ph) issued an order.

LABRADOR:

That's how it is issued right now. But do you think that that can only be obtained through a warrant? Or are you seeking to obtain it later through other means other than warrants?

COMEY:

I don't know how we would, if it's in Apple's possession, unless they voluntarily gave it to someone. There'd have to be judicial process...

LABRADOR:

OK.

COMEY:

... if they maintained it afterwards.

LABRADOR:

All right. Thank you very much. I've run out of time.

COMEY:

Thank you.

GOODLATTE:

The chair thanks the gentleman, recognizes the gentleman from Louisiana, Mr. Richmond, for five minutes.

RICHMOND:

Thank you -- thank you, Mr. Chairman. Before I start, I'd like to enter into the record two articles -- one is from the Toronto Star, titled "Encrypted evidence is increasingly hampering criminal investigations, police say".

And another one is from the Baton Rouge Advocate, which says, "The Brittney Mills murder case has put Baton Rouge in the middle of the national cell phone encryption debate".

GOODLATTE:

(OFF-MIKE)

RICHMOND:

Thank you, Mr. Chairman. And let me just say -- and, Director Comey, you have mentioned the Brittney Mills case a number of times. And I just want to paint the scenario for everyone in -- in the room, and put a face with it.

This is Brittney Mills, and this is Brittney Mills almost eight months pregnant with her daughter. In May of last year, Brittney was murdered in my district. She was a mother. She was eight months pregnant with her second child at the time. Someone came to her door and killed her. And a couple days later, her unborn child -- or born child -- also died.

And according to her family and her friends, she kept a very detailed diary in her phone. And her family, who are here today -- Ms. Mills, Ms. Barbara Mills, will you please stand -- and Tia and Roderick?

Her family would like the phone opened so that our district attorney, who is also here today -- thank you for standing -- our district attorney, who is also here today, Hillar Moore, can use that to attempt to find the murderer who committed this crime.

And I guess my question, as we balance privacy, public safety, and criminal justice -- that are we in danger of creating an underground criminal sanctuary for some very disturbed people? And how do we balance that?

COMEY:

We are in danger of that. Until these awesome devices -- and that's what makes it so painful -- they're wonderful -- until this, there was no closet in America, no safe in America, no garage in America, no basement in America that could not be entered with a judge's order.

We now live in a different world, and that's the point we're trying to make here. Before we drift to a place where a whole lot of other families in incredible pain look at other district attorneys and say, "what do you mean you can't, you have a court order?" -- before we drift to that place, we gotta talk about it, because privacy is awesome.

But stopping this kind of savagery and murder and pedophilia, and all the other things that hide in the dark spaces in American life, is also incredibly important to us.

That's why this conversation matters so much. But it's also why we have to talk to each other. There are no demons in this conversation. We care about the same things. But it is urgent, and there's no more painful circumstance to demonstrate it than in the death of that beautiful woman and her baby.

RICHMOND:

Well, and -- and I do appreciate you saying we have to talk to each other, because just in the small time that I was able to put the representatives of Apple and the district attorney in the room, I think we made some progress, and maybe some alternatives, and maybe we'll get somewhere.

But it is a -- a very difficult balancing act, and I think the people from Apple are very well-intentioned and have some real concerns.

But let me ask you this -- I took a congressional delegation trip over to the Ukraine. And we -- when we landed our plane, we were on the runway, and our security advisers came on to the back and said, "if you don't want your phone hacked and people to have access to your text messages, your pictures, your e-mails and everything else, we advise you to power your phone off and leave it on the plane.

"And no one is in close enough proximity right now to do it, so if you need to make a call, make a call. But when we get closer to the terminal, you need to power that phone down."

So, does Ukraine have better technology -- well, they were really worried about Russian hackers. But does Russia have that much of a technology advantage over us that they can get into my phone while I'm on it, and it's in my possession, and we can't get into a phone that we have in our possession?

COMEY:

The difference -- and I'm -- I'm going to be careful about what I say in an open setting, is that some countries have different control over their infrastructure, and require providers in their country to make accommodations that we do not require here, to give them greater surveillance capabilities than we would ever imagine in the United States.

That's the first thing. Second thing is, we are a rule of law country. The FBI is not cracking into your phone or listening to your communications, except under the rule of law and going to a judge. Those are the two big differences.

But countries have capabilities, and in part based on accommodations that device makers and providers have made in those countries that are different than this country.



RICHMOND:

Thank you, Mr. Chairman. I see my time has expired.

GOODLATTE:

The chair recognizes the gentlewoman from Washington state, Ms. DelBene, for five minutes.

DELBENE:

Thank you, Mr. Chair, and thank you, Director Comey, for being with us, and for all of your time.

I worked my career in technology, on e-mail and mobile communications, and constantly heard from customers -- both consumers and businesses and even the government -- to make sure that information was protected and that devices were secure.

And in your testimony, you state that you're simply asking to ensure that you can continue to obtain electronic information and evidence, and you seem to be asking technology companies to -- to freeze in place or revert back to systems that might have been easier to access.

But don't you think, in general that that's much -- an oversimplification of this issue? Because we all know that bad actors want to exploit vulnerabilities to -- breaking into any number of things, from a phone, a personal device, to our power grid.

These things aren't static. They're changing constantly, and they're getting smarter every day. The bad actors are getting smarter every day, and we need to be smarter every day in terms of protecting information.

So, in that type of environment, how would you expect a technology company not to continue to evolve their security measures to keep up with new threats that we see?

COMEY:

First of all, I would expect security companies and technology companies to continue to try and improve their security. That's why it's important that all of us talk about this, because it's not the company's job to worry about public safety. It's the FBI's job, Congress' job and a lot of other folks' in the government.

So I -- I don't put that on the companies. But the other thing that concerns me a little bit is this sense that, if we have a world where people comply with government warrants, it must be insecure.

And I don't buy that, because there are lots of providers today of e-mail service, of text (ph) service, who have highly secure systems, who, because of their business models, visualize the -- the information in plain text on their servers so they comply with court orders.

COMEY:

I have not heard people say their systems are insecure. They simply have chosen a different business model. So I actually don't think it's, again, a lot of people may disagree with me, I actually don't think in the main it's a technological problem. It's a business model problem. That doesn't solve it, but that gets us away from this "it's impossible" nonsense.

DELBENE:

But we know more and more, in fact we're seeing -- we're talking about phones today, but we're talking about the growth on the Internet of things of more and more personal devices where security will be even more critical. And so it's hard to say. You're talking about a world where it's combined to the way the world works today. I think that absolutely is not the situation that we're facing. We're seeing evolution every day. And these are devices that are connected to networks and information is flowing.

And that information might be someone's financial information or personal information that if it is exploited would create a security issue itself.

COMEY:

I agree.

DELBENE:

So don't you believe that encryption has an important role to play in protecting security?

COMEY:

Vital.

DELBENE:

So now we've talked about what role Congress plays versus what role the courts would play. And you've kind of talked about both in different scenarios. You've talked about privacy versus security, and that Congress should play a role there. But the courts should decide whether or not there's a security breach, if there's a piece of technology that breaks into a device and whether or not there is a concern that that will be widely available.

Yet, the tension isn't really between just privacy and security. It's between security and security, and protecting people's information. And -- and so, how do you -- where do you think Congress plays a role versus the courts, when you've talked about both of them in your testimony today?

COMEY:

I think the courts have a job to, in particular cases, interpret the laws that Congress has passed throughout the history of this country, to try and decide the government is seeking this relief; does that fit within the statute. That's -- that's the court's job and they're very, very good at it.

The larger societal problem we have is this collision, that I think you've said well, between privacy and security -- very difficult to solve it case by case by case. We have to ask ourselves: How do we want to govern ourselves? If you are a manufacturer of devices in the United States, or you provide communication services in the United States, what are our, as a country, what are our expectations of you and demands of you?

It's hard to me to see that being worked out on a common law basis, honestly. But it's going to be because the issue is joined every single day in our law enforcement work. If nobody else gets involved, the courts will have to figure it out.

DELBENE:

This -- this -- this isn't just an issue of U.S. companies alone, because clearly there's access to technology that could be developed in other countries that we'll not have access to, and that's widely available today and people can use.

But also, then, it is important we have laws that are centuries and decades old that have not kept up with the way the world works today. And so it is very important that Congress plays a role because the courts are going to be interpreting those laws, and those laws were written with no awareness of what's happening today. Then Congress needs to play a role of making sure we have laws that are up to date and setting standards that courts can then follow.

Thank you. I yield back, Mr. Chair.

GOODLATTE:

The chair thanks the gentlewoman.

And recognizes the gentleman from New York, Mr. Jeffries.

JEFFRIES:

Thank you, Mr. Chairman.

And thank you, Mr. Comey, for your presence here today. And as one of my colleagues mentioned, your candor and open dialogue and communication is much, much appreciated. It is not always the case with high-level government witnesses and others.

You testified today that you don't question Apple's motives in connection with the San Bernardino case. Is that correct?

COMEY:

Correct.

JEFFRIES:

And you also testified that there are no demons in this conversation.

True?

COMEY:

Correct. I hope not.

JEFFRIES:

But the Department of Justice has questioned the company's motives in defending the privacy of the American people. Isn't that right?

COMEY:

I don't think they question their motives, in the sense that attributed sort of that they're acting with evil intent or something. I think they -- I remember a filing the department said where they think a lot of Apple's position has to do with its market power, which I frankly think is not an illegitimate motive.

JEFFRIES:

In fact, in the motion to compel that you refer to, I believe the prosecutor said that Apple's current refusal to comply with the court's order, despite the technical feasibility of doing so, appears to be based on its concern for its business model and public brand marketing strategy. Is that the statement that you're referring to, sir?

COMEY:

Yes. And I think that's -- that's fair. I bet that's accurate. Apple has a legal obligation, because I used to be the general counsel of a public company, to maximize shareholder value. They're a business. And so I would hope that's part of their motivation and it's not a bad thing if it's entirely their motivation. Their job is not to worry about public safety. That's our job, and all of us in this room who work for the government.

JEFFRIES:

William Bratton is the police commissioner of the New York City Police Department. Is that right?

COMEY:

Yes.

JEFFRIES:

It's the largest department in the country?

COMEY:

Yes.

JEFFRIES:

And he's one of the most respected law enforcement professionals in the country. Would you agree with that?

COMEY:

I agree with that very, very much.

JEFFRIES:

Now, at a February 18th press conference in New York City, he publicly accused Apple of corporate irresponsibility. Are you familiar with that remark, sir?

COMEY:

I'm not.

JEFFRIES:

OK. Do you agree with that strident statement, that Apple is engaging in corporate irresponsibility by vindicating its (inaudible)?

COMEY:

I don't know that Bill said that, but I'm not going to characterize it that way. I don't think they're acting irresponsibly. I think they're acting as a corporation in their self-interest, which is the way -- which is the engine of innovation and enterprise in this country.

JEFFRIES:

Fundamentally, as it relates to the position of those of us who are on the Judiciary Committee, as well as members in the House and in the Senate, guardians of the Constitution, this is not about marketing or corporate irresponsibility. Correct? This debate?

COMEY:

I hope not. I mean, I hope part of it is, and that's a voice to listen to. But they sell phones. They don't sell civil liberties. They don't sell public safety. That's our business to worry about.

JEFFRIES:

Right, but in terms of our perspective, this is really about fundamental issues of importance as it relates to who we are as a country, the Fourth Amendment of the United States Constitution, the reasonableness of government intrusion, the rule of law, the legitimate centuries-old concern as it relates to government overreach and the damage that that can do. This is fundamentally a big-picture debate about some things that are very important to who we are as a country. Correct?

COMEY:

I agree completely.

JEFFRIES:

OK. Now, in terms of the technology that's available today, Americans seem to have the opportunity to choose between privacy or unfettered access to data which can reveal the far reaches of their life to a third party, to a government, to a bad actor. Would you agree that there's an opportunity that the technology is providing for Americans to choose privacy?

COMEY:

I don't agree with that framing because it sounds like you're framing as we either have privacy or we have unfettered access by bad actors. I don't accept that premise.

JEFFRIES:

OK. So let me ask a few questions. One of the obstacles to unfettered

access is the pass code. Correct? The pass code?

COMEY:

Yes.

JEFFRIES:

A (inaudible) or six-number pass code.

COMEY:

I naturally quibble because I'm a lawyer, but I'm just stuck on "unfettered."

JEFFRIES:

OK.

COMEY:

One of the obstacles to access to a device is the password.

JEFFRIES:

Let me drop "unfettered."

COMEY:

OK.

JEFFRIES:

The pass code is an obstacle. Correct?

COMEY:

Correct, correct.

JEFFRIES:

Now, you can choose a pass code or choose not to activate pass code.

Correct?



COMEY:

I think that's right.

JEFFRIES:

OK. Now, whether you back up your system or not is an issue as it relates to access. Correct? In other words, if you don't back up your system, you don't have access. Correct? To the cloud?

COMEY:

Yes. I think if you don't back up your system to the cloud, there's nothing in the cloud that could be obtained by a warrant.

JEFFRIES:

Right. Now, with respect to auto-erase, that is a choice that's being made. In other words, you have to actually affirmatively choose auto-erase. If you didn't choose it, in this particular case or any other case, eventually your computer is powerful enough to get access to the data. Correct?

COMEY:

I think that's right for the 5-C. I think that's -- and folks from Apple could tell you better. I think for the later models, it's not a choice, but I think it's a choice -- I'm reasonable confident it's a choice for the 5-C.

JEFFRIES:

My time is expired, but I think it's important as we frame this debate to understand that it is actually the American citizen that is choosing on at least three different occasions in three different ways, the value of privacy. And that's something that we should respect as Congress attempt to craft a solution.

COMEY:

OK.

GOODLATTE:

The chair thanks the gentleman.

And recognizes the gentleman from Rhode Island, Mr. Cicilline, for five minutes.

CICILLINE:

Thank you, Mr. Chairman.

Thank you, Director Comey, for your service to our country. Thank you for being here today and for the outstanding work of the men and women at the FBI.

We all, of course, acknowledge that incredible horrors of the San Bernardino attack. But I think in many ways what we're struggling is, as Ms. Delbene said, not necessarily security versus privacy, but security versus security. And the real argument that the danger that exists for the misuse of this new technology by foreign agents, by terrorists, by bad actors, by criminals will actually make us less safe in the long term.

And while it may achieve your objective in the short term in this particular case, the implications in terms of our own national security and personal security are -- pose greater dangers. And I think that's what, at least I'm struggling with.

CICILLINE:

I appreciate you said this is the hardest question you've confronted because I think it is a hard one.

But the first thing I want to ask is this is different, would you agree, than all the examples that have been used about producing items in your custody. This is a different kind of warrant because it's actually compelling a third party to produce and create intellectual property which doesn't exist today.

COMEY:

I understand that to be Apple's argument. I don't know enough about the other possible comparisons to give you a thoughtful response. But yes, I understand that.

CICILLINE:

But I mean -- but it's hard to even imagine how a court ultimately enforces that because you have to sort of get into the head of the engineers to figure out did they actually comply with what the government order is directing them to create.

I mean, I'm not saying it's not something you're not allowed to ask for, but it is different, it seems to me, than simply asking people to produce that which they are in possession of, custodians of.

COMEY:

Yeah, I see that. I mean, I heard someone earlier say there's a difference between a landlord that has a key in his pocket, you say you've got to give us the key, and you don't have one. Go make one for that door. And the question for the judge is...

CICILLINE:

Well, this is more than...

COMEY:

...what's the significance of this.

CICILLINE:

...not just go make one, because knowing how to make keys exists, but to develop a whole new technology and intellectual property. So I just want -- I raise that because I think we have to acknowledge it's different and then decide what to do with it.

But in addition to that, you've said repeatedly that the government doesn't have the ability to do this already. And as you know, there was a decision yesterday, Magistrate Judge Orenstein -- I'd ask unanimous consent that that memorandum and order be made part of the record -- in which he actually...

GOODLATTE:

It is already part of the record.

CICILLINE:

OK -- which he goes through and says the All Writs Act doesn't apply; CALEA (ph) prohibits this by omission and, I think, in a very clear way. But in addition to that, he goes on to say that the government argued in an unrelated case that the government actually has the ability to do this, that the Department of Homeland Security investigations, that they are in possession of technology that would allow its forensic technicians to override the pass code security feature on the subject iphone and obtain the data.

So I think this is a very important question for me. If, in fact -- is it, in fact, the case that the government doesn't have the ability, including the Department of Homeland Security investigations, and all of the other intelligence agencies, to do what it is that you claim is necessary to access this information?

COMEY:

Yes.

CICILLINE:

It is very -- the answer is yes?

COMEY:

That is correct. And I don't know, I think -- I could be wrong, but I think the phone in the case from Brooklyn is different. Maybe both the model and the IOS, the operating system is different. But for this -- I'm here to tell you -- and again, people know the sound of my voice. If you've got an idea, let us know. But 5C, IOS 9, we do not have that capability.

CICILLINE:

OK.

COMEY:

Again, to disable -- the problem is we can get into that phone with our computing power if they take off the auto erase and the delay between guesses function, we will get into that phone.

CICILLINE:

So do you agree, Director Comey, that if there is authority to be given to do what you are asking, that that authority has to come from Congress?

COMEY:

No, I don't agree with that.

CICILLINE:

So where do you think the authority comes from?

COMEY:

Well, the government has already asked the court and made the argument under the court that the All Writs Act vests in the judiciary the ability to order this relief. That's what -- that's what the court case is going to be about.

CICILLINE:

OK. So if the ruling made yesterday remains, which rejects the notion that the All Writs Act applies and that CALEA (ph) in fact is Congressional intention on this and the fact that we didn't act on it means you have authorization has not been provided, then would you agree that Congress is the only place that can authorize this? And if so, what would you recommend we do? What would that look like as we grapple with this question?

Because I can tell you, from me having read that, I think CALEA (ph) is clear it doesn't authorize it, it's clear the All Writs Act doesn't. So if there is to be authority, assuming we decide that there should be, it seems it must come from Congress. As director of the FBI, what do you think that would -- what would your recommendation be that would respond to what you see as your needs but also the national security interests of our country?

COMEY:

I'm not prepared to make a recommendation, but I think I get your question now. If the judges are right that you can't use the All Writs Act for this relief, what should Congress do to grant relief? And I'm not prepared to tell you specifically what to do. I do think it's something that Congress is going to have to wrestle with.

CICILLINE:

Thank you. I yield back. Thank you, Mr. Chairman. Thank you, Director.

GOODLATTE:

The chair would ask unanimous consent that letters from the Computer Communications Industry Association dated February 29, a statement for the record from Raynold Tariche, president of the FBI Agents Association and a letter dated February 29 from the American Civil Liberties Union all be made a part of the record.

Director Comey, you've given us three hours -- oh, I'm sorry. I'm jumping the gun here. The gentleman from California, Mr. Peters, is recognized for five minutes.

PETERS:

Director Comey, I want to -- first of all, thank you, Mr. Chairman. I want to thank you for being here.

I wanted to just conclude by saying that I did hear very -- did listen carefully to your opening statement. I thought it was very constructive. I think you appreciate the two objectives we have here, which is to both preserve privacy and to deal with San Bernardino. You've heard the comment hard cases make bad law. They're still hard cases, and the problem we see in terrorism now is the onesies and the twosies, and the notion that we would have invulnerable communications I think is something that we should all be concerned about.

I hope that you and the panel to follow you will all be part of a constructive discussion to figure out a way to serve both objectives and that the lines won't be too hard drawn on either side so that we can do that. And I appreciate, Mr. Chairman, the chance to thank Director Comey for being here, and look forward to the next panel.

COMEY:

Thank you.

PETERS:

Yield back.

GOODLATTE:

Chair thanks the gentleman. Director, you've donated three hours of your time to our efforts today -- or more, I'm sure, in getting ready. So we thank you very much for your participation and for answering a multitude of question. And we are looking for answers, so if you have more to add to the record later, we would welcome that later as well. Thank you very much.

COMEY:

Thank you, sir.

CQ Transcriptions, March 1, 2016

### **List of Panel Members and Witnesses**

PANEL MEMBERS:

REP. ROBERT W. GOODLATTE, R-VA. CHAIRMAN

REP. LAMAR SMITH, R-TEXAS

REP. JIM SENSENBRENNER, R-WIS.

REP. DARRELL ISSA, R-CALIF.

REP. J. RANDY FORBES, R-VA.

REP. STEVE KING, R-IOWA

REP. TRENT FRANKS, R-ARIZ.

REP. LOUIE GOHMERT, R-TEXAS

REP. JIM JORDAN, R-OHIO

REP. TED POE, R-TEXAS

REP. JASON CHAFFETZ, R-UTAH

REP. STEVE CHABOT, R-OHIO

REP. TOM MARINO, R-PA.

REP. TREY GOWDY, R-S.C.

REP. RAUL R. LABRADOR, R-IDAHO

REP. BLAKE FARENTHOLD, R-TEXAS

REP. DOUG COLLINS, R-GA.

REP. RON DESANTIS, R-FLA.

REP. MIKE BISHOP, R-MICH.

REP. KEN BUCK, R-COLO.

REP. JOHN RATCLIFFE, R-TEXAS

REP. DAVE TROTT, R-MICH.

REP. MIMI WALTERS, R-CALIF.

REP. JOHN CONYERS JR., D-MICH. RANKING MEMBER

REP. JERROLD NADLER, D-N.Y.

REP. ZOE LOFGREN, D-CALIF.

REP. SHEILA JACKSON LEE, D-TEXAS

REP. STEVE COHEN, D-TENN.

REP. HANK JOHNSON, D-GA.

RES. CMMSR. PEDRO R. PIERLUISI, D-P.R.

REP. JUDY CHU, D-CALIF.

REP. TED DEUTCH, D-FLA.

REP. LUIS V. GUTIERREZ, D-ILL.

REP. KAREN BASS, D-CALIF.

REP. CEDRIC L. RICHMOND, D-LA.

REP. SUZAN DELBENE, D-WASH.

REP. HAKEEM JEFFRIES, D-N.Y.

REP. DAVID CICILLINE, D-R.I.



REP. SCOTT PETERS, D-CALIF.

WITNESSES:

FBI DIRECTOR JAMES COMEY

---

Source: **CQ Transcriptions**

© 2016 CQ Roll Call All Rights Reserved.

# **Exhibit F**

CQ CONGRESSIONAL TRANSCRIPTS  
Congressional Hearings  
Feb. 25, 2016 - Final

## House Select Intelligence Committee Holds Hearing on World Wide Threats

### LIST OF PANEL MEMBERS AND WITNESSES

NUNES:

The committee will come to order. Today the committee will examine world wide threats.

I would like to welcome our witnesses - Director of National Intelligence, James Clapper. Director of the Central Intelligence Agency, John Brennan. Director of the Federal Bureau of Investigation, James Comey. Deputy Director of the National Security Agency, Richard Ledgett. Director of the Defense Intelligence Agency, Lieutenant General Vince Stewart. And Director of National Counterterrorism Center, Nick Rasmussen.

Thank you all for being here today. I recognize the challenges associated with discussing sensitive national security issues in public. But I hope you agree that this open forum is critical to help explain to the American people the serious threats we face and also to highlight the efforts of the brave men and women of the Intelligence Community to keep us safe.

I speak for the entire community when I thank you for your service, sacrifice, and dedication.

Director Clapper, this is your last World Wide Threats Hearing with this committee. I'd like to specially thank you for your 55 years of service to this great nation.

Director Clapper, I recall from last year's testimony that you were concerned about a vast array of threats. Remarkably, the number seems to have grown since then.

Generally, I share your assessment of the current threat environment. The truth is the United States faces the highest threat level since the 9/11 attacks. The American people don't need security clearance to understand the threats now facing the Western world.

They only need to read the headlines out of Paris, Brussels, San Bernadino and Boston. Al-Qaeda, ISIS, and other terror groups are rapidly expanding with more access to safe havens, recruits, and resources than ever before.

Without U.S. leadership this trend will continue. We have discussed Syria and Iraq with you at length in closed and open sessions. I believe the U.S. response to those conflicts is among the most mismanaged foreign policy blenders in recent history.

After consistently failing to block ISIS's expansion, we have to accept a new reality. ISIS is now in dozens of countries and has repeatedly demonstrated the ability to reach our homeland.

Instead of focusing on ISIS as if it were confined to Iraq and Syria, we urgently need an aggressive, comprehensive, and anti-terrorist strategy that stretches from Morocco to Southeast Asia.

At the same time, our adversaries are becoming more diverse. Throughout the next decade the U.S. must be prepared to check Chinese ambition (ph) in Asia, counter a resurgent Russia, defend against cyber threats, and manage delicate geopolitical forces in the Middle East. Including the growing schism (ph) between Sunni and Shia Muslims.

How does the president respond to these enormous challenges? His hallmark policy has been to strike a nuclear deal with Iran that greatly relieves pressure on the Iranian regime - the world's biggest state sponsor of terrorism. He also failed to prevent Russia from propping up Syrian dictator, Bashar al-Assad. A man who the president himself has insisted must surrender power.

Meanwhile, some of our closest allies in fighting terrorism - the Kurds, the Israelis and the Egyptians - often find themselves -- their concerns down played or dismissed within the administration.

Our partners around the world want to work with us but they can't rally behind American leadership if they don't understand what our foreign policy is trying to accomplish.

Although I disagree with the president's policies, the committee will continue to debride (ph) the Intelligence Community with the resources it needs to protect the nation.

With particular emphasis this year on preserving capabilities for the next president. Because the Intelligence Community is being stretched thin and is overwhelmed by a complex threat matrix, we must prioritize investments throughout the entire Intelligence Community.

Our committee's mission is clear - to help the Intelligence Community to protect the American people by providing oversight, direction, and resources to enable effective, efficient, and constitutional intelligence activities.

Additionally, amid the growing threats we face, it is critically important that we ensure the Intelligence Community act as careful steward of the tax payers dollars.

Over the next year, our committee will focus on making progress in the following five key areas.

First, encouraging efficient investment in areas such as space in which complex program and capability requirements routinely drive up costs in adopting new technology. Including data analytics, encryption, and technical training specifically in community wide projects like cloud computing, data security, and tool management.

Second, reassessing the effectiveness of the community's human intelligence enterprise and synchronizing community-wide resources. Especially at a time when several Intelligence Community agencies are implementing re-organizational plans.

This particularly applies to the recruitment and training of the next generation of collectors, cyber experts, and analysts to operate in non-traditional areas and deliver intelligence on hard to reach targets.

Third, producing objective and unbiased intelligence analysis. Particularly in the Department of Defense where there is a multi-committee effort to determine whether there are systematic problems across the intelligence enterprise and CENTCOM or any other pertinent intelligence organizations.

In this context, it is vital that this committee protect and seriously consider the testimony of the many whistle blowers who have provided information to us.

For example, we have been made aware that both files and emails have been deleted by personnel at CENTCOM. And we expect that the Department of Defense will provide these and all other relevant documents to the committee.

Fourth, improving the efficiency of intelligence support to Combatant Commands including efforts to curb facilities and personnel costs. It's alarming that this committee identified up to \$50 million dollars in annual savings for the Defense Intelligence Agency and more than \$300 million dollars in unneeded construction disguised as base consolidation.

In total, this was \$1.5 billion dollars in savings for one project. The response we received from the administration can only be described as delay, denial, and deception

This has led the Chairman of the Armed Services Committee, the Chairman of the Defense Appropriations Committee and me to ask the GAO to conduct a full investigation.

Furthermore, whistle blowers have provided this committee with documentation showing the Department of Defense has provided false information to Congress. This committee will now conduct another round of interviews and will turn over our findings to the House Committee on Oversight and Government Reform which already has an ongoing investigation into this matter. And to the Department of Defense Inspector General.

Finally, we've asked for data on all intelligence personnel and major support contractors at the Combatant Commands. This request was made in December and this is information that should be readily available.

Informants have made this committee aware that basing decisions at significant cost to the tax payer are being determined in order to maximize pay and benefits of small groups of individuals.

This includes both Department of Defense civilians and contractors. This brings into question hundreds of millions of dollars of contracts that are being awarded annually.

Fifth and finally, migrating cyber threats and improving cyber defense in light of the rapid pace of technological change. To address these problems, the committee helped pass the Cybersecurity Act of 2015.

While the Director of National Intelligence is establishing the Cyber Threat Intelligence Integration Center, we need to ensure that the new law is implemented properly and that the new center operates effectively.

Additionally, the latest challenges the government has met in gaining access to the iPhone used by one of the San Bernadino terrorists is emblematic of the growing problem posed by encryption.

Finally, we need to educate members of Congress on the importance of re-authorization of Section 702 of the Foreign Intelligent Surveillance Act. I look forward to hearing what the witnesses have to contribute on these five focus areas.

And with that, I'd like to recognize my Ranking Member, Mr. Schiff, for any comments he would like to make.

SCHIFF:

Thank you, Mr. Chairman. I want to join you in thanking our witnesses - Director Clapper, Director Brennan, Director Comey, Lieutenant General Stewart, Director Rasmussen, and Deputy Director Ledgett. We are very grateful for your efforts and for those of the men and women of the Intelligence Community.

The threats we face today are incredibly diverse and incredibly daunting. From cyber to terrorism, Russian aggression to North Korean nuclear belligerence, from threats to space to threats from below the sea - we are living in a very dangerous world.

Because of technology, some of these threats are new. The Internet of Things, for example, presents unique vulnerabilities to the most advanced nations like us as does the rise of artificial intelligence.

Other threats are more traditional but still potentially devastating. North Korea's January nuclear test and its recent space launch; Russia's interventions in Ukraine, Syria, and its threat to the Baltic States; China's activity in the South China Sea; and regional power struggles in the Middle East are a reminder that traditional state-based threats have not receded.

Far from it, they are getting worse. Still other threats are shifting. Even as coalition bombing has halted the group's expansion in Iraq and Syria, for example, ISIS has thrown off spores (ph) into places like Libya and has sought to insight attacks in Europe as we saw in Paris and to inspire attacks here in the United States as we saw in San Bernadino.

Many of these threats are also interrelated. ISIS virulence is compounded by its use of technology. Particularly social media and encrypted communications. Russia's terrestrial ambitions and China's naval designs are supported by a desire to counter the U.S. predominance in space.

And our greatest cyber capabilities are also our greatest vulnerabilities. To navigate through these treacherous shoals (ph), we look to the IC to sound the alarms as you are doing today and to find and enable solutions.

After the Senate's version of this hearing earlier this month, many were saying that the world was going to hell in a hand basket. And I can certainly understand why given the myriad of challenges that we face.

But I want to emphasize here that we're highlighting these threats so we can discuss how best to counter them. And we have faced and overcome far greater challenges in the past.

To that end, we have begun receiving and reviewing your budget submission. We look forward to many more sessions with you to make sure you have what you need to protect against these threats. And to do so in a way that is lawful, protective of privacy and civil liberties, cost effective and in keeping with the highest of American values.



Some solutions, particularly when it comes to the debates surrounding encryption, are not gonna come easily. The simple fact is exemplified by this month's case involving Apple.

One thing, however, is clear. The court's ruling, even if narrowly tailored to particular facts of this case, will have ripple effects that will significantly impact the law enforcement community, the intelligence community, the business community, and all of us individually.

This case and others like it implicate policy questions that can't be decided by the courts alone. The Congress, through inclusive discussion with tech companies, interest groups, the public, the global community, law enforcement, and the Intelligence Community and the White House must carefully weigh the competing policy considerations and arrive at sensible solutions.

As a first step, we need facts. That's why several months ago, Chairman Nunes and I asked the National Academy of Science for a report on this issue which will be completed this year.

That's also why I supported legislative commission on encryption and the president's broader Cyber Security Commission. A hard look at the most commonly advanced claims on all sides of the encryption debate would move us further from abstractions and towards solutions.

As a second step, we need to honestly acknowledge the complexity and not engage in absolutes. As this committee has shown with its leadership on surveillance reform and cyber information sharing legislation, privacy and liberty can and must coexist.

There is no doubt that terrorists are exploiting cheap and widely available encryption technology to do us harm. And they'll continue to do so. At the same time, there's no doubt that our cyber security and our privacy are under relentless attack from nation state and criminal hackers. And greater encryption provides a key defense. We can all agree that law enforcement and the Intelligence Community have an obligation to investigate crimes and prevent harm to Americans.

Similarly, there's no doubt that American companies have obligations to their shareholders to maximize profits in an increasingly competitive global world and to their customers to safeguard privacy. Our job in Congress is to reconcile these legitimate obligations and priorities. It is our job to draw lines.

I'm not advocating a broad mandate on decryption but nor do I favor a world where law enforcement is completely shut out of illicit communications when they have a court approved warrant.

What I am advocating is for a cooperative, fact-based approach to solving this very real problem. Congress can pose a solution if it must. But it would be far better for us to arrive at a resolution through a negotiation with all of the stakeholders that sets the standard for best practices and one that we can live here at home and champion around the world.

Yes, we are living in a dangerous world as well as a complex world. Make no mistake about it. But it's also a world of great opportunity. Some of the challenges we have today like that presented by encryption are born of incredible talent, creativity, and innovation of American businesses that are solving problems everyday.

We also have the best Intelligence Community in the world working tirelessly to make sure these advances are not used to propagate hate, violence, and terror through channels that are beyond reach.

The challenges and the answer to these challenges lies in finding solutions together. I thank you, Mr. Chairman. I yield back.

NUNES:

Gentleman yields back. I believe Mr. Clapper, you have opening statement. I think you're gonna speak for the entire panel?

CLAPPER:

Yes, sir. That's right.

NUNES:

Mr. Clapper, I want to again thank you for your 55 years of service. I don't know if this is your last World Wide Threats Hearing but -- but if it is I am sure you're happy about that. At least probably.

(LAUGHTER)

And with that, you're recognized.

CLAPPER:

Yes, I am. Chairman Nunes, Ranking Member Schiff and -- and members of the committee. We're here today to update you on some, but certainly not all, of the pressing intelligence and national security issues facing our nation.

So in the interest of time, to get to your questions, I'll cover just some of the wave (ph) tops and as you indicated, mine will be the only opening statement. And we'll be back next week - I will be on the third of March - to address budget and management issues that you raised, Chairman Nunes.

As I said last year, unpredictable instability has become the new normal. And this trend will continue, we think, for the foreseeable future. Violent extremists are operationally active in about 40 countries.

Seven countries are experiencing a collapse of central government and authority. And 14 others face regime threatening or violent instability or both. Another 59 countries face a significant risk of instability through 2016.

The record level of migrants - more than a million - arriving in -- in Europe is likely to grow further this year. Migration and displacement will strain countries in Europe, Asia, Africa, and the Americas.

Some 60 million people are considered displaced globally. The most since the end of World War II when the United Nations first started keeping such records.

Extreme weather, climate change, environmental degradation, rising demand for food and water, poor policy decisions, and inadequate infrastructure will magnify that -- that instability.

Infectious diseases and vulnerabilities of the global supply chain for medical counter measures will continue to pose threats. For example, the Zegla (ph) Virus - first detected in the Western Hemisphere in 2014 - has reached the United States and is projected to cause up to four million cases in this hemisphere.

With that preface, I want to briefly comment on both technology and cyber. Technological innovation during the next few years will have an even more significant impact on our way of life.

This innovation is central to our economic prosperity but it will bring new security vulnerabilities. The Internet of Things will connect tens of billions of new physical devices that could be exploited.

Artificial intelligence will enable computers to make autonomous decisions about data and physical systems that potentially disrupt labor markets. Russia and China continue to have the most sophisticated cyber programs.

China continues cyber espionage against the United States. And whether their commitment of last September moderates its economic espionage remains to be seen. Iran and North Korea continue to conduct cyber espionage as they enhance their attack capabilities.

Non-state actors also pose cyber threats. ISIL has used cyber to its great advantage. Not only for recruitment and propaganda but also to hack and release sensitive information about U.S. military personnel.

As a non-state actor, ISIL displays unprecedented online proficiency. Cyber criminals remain the most pervasive cyber threat to the U.S. financial sector. They use cyber to conduct theft, extortion, and other criminal activities.

Turning to terrorism, there are now more Sunni violent extremist groups, members, and safe havens than at any time in history. The rate of foreign fighters traveling to the conflict zones in Syria and Iraq in the past few years is without precedent.

At least 38,200 foreign fighters, including at least 6,900 from Western countries, have traveled to Syria from at least 120 countries since the beginning of the conflict in 2012.

As we saw in the November Paris attacks, returning foreign fighters with first hand battle field experience pose a dangerous operational threat. ISIL has demonstrated its sophisticated attack tactics and trade craft, as we saw.

ISIL, including its eight established and several more emerging branches, has become the pre-eminent global terrorist threat. ISIL has attempted or conducted scores of attacks outside of Syria and Iraq in the past 15 months.

ISIL's estimated strength now exceeds that globally of Al-Qaeda. ISIL's leaders seek to strike the U.S. homeland beyond inspiring home grown violent extremist attacks. Although the U.S. is a harder target than Europe, ISIL external operations remain a critical factor in our threat assessment of 2016.

Al-Qaeda's affiliates also have proven resilience. Despite counterterrorism pressure that's largely disseminated the core leadership in Afghanistan and Pakistan, Al-Qaeda affiliates are in a position to make gains in 2016.

Al-Qaeda in the Arabian peninsula and the al-Nusra Front - the Al-Qaeda chapter in Syria - are the two most capable Al-Qaeda branches. The increased use by violent extremist of encrypted and secure Internet and mobile-based technology enables terrorist actors to go dark and serves to undercut intelligence and law enforcement efforts.

Iran continues to be the foremost state sponsor of terrorism and exert its influence in regional crises in the Mid East through the Islamic Revolutionary Guard Corps, Quds Force - its terrorist partner, Lebanese Hezbollah, and proxy groups.

Iran and Hezbollah remain a continuing terrorist threat to U.S. interests and partners worldwide. We saw first hand the threat posed in the United States by homegrown violent extremists in the July attack in Chattanooga and the attack in San Bernadino.

In 2014, the FBI arrested nine ISIL supporters. In 2015, that number increased more than five-fold.

Moving to weapons of mass destruction. North Korea continues to conduct test activities of concern to the United States. Earlier this month, Pyongyang conducted a satellite launch and subsequently claimed that the satellite was successfully placed in orbit.

Additionally in January, North Korea carried out its fourth nuclear test claiming it was a hydrogen bomb. But the yield was too low for it to have been a successful test of a stage thermonuclear device.

Pyongyang continues to produce fissile (ph) material and develop a submarine launch ballistic missile. It's also committed to developing a long-range nuclear arm missile that's capable of posing a direct threat to the United States although the system has not been flight tested.

Despite its economic challenges, Russia continues its aggressive military modernization program. It has the largest and most capable foreign nuclear arm ballistic missile force.

It has developed a cruise missile that violates the Intermediate- Range Nuclear Forces - or INF Treaty. China continues to modernize its nuclear missile force. And in striving for a secure second strike capability, it continues to profess a no-first use doctrine. The Joint Comprehensive Plan of Action - or JCPOA - provides us greater transparency into Iran's fissile material production.

It increases the time the Iranians would need to produce enough weapons grade (ph) uranium for a nuclear weapon from a few months to about a year. Iran probably views the JCPOA as a means to remove sanctions while preserving nuclear capabilities.

This perception of how the JCPOA helps to achieve its overall strategic goals will dictate its level of adherence to the agreement over time. Thus far, the Iranians appear to be in compliance.

Chemical weapons continue to pose a threat in Syria and Iraq. Damascus has used chemicals against the opposition on multiple occasions since Syria joined the chemical weapons convention.

ISIL has also used toxic chemicals in Iraq and Syria including the blister agent Sulfur Mustard. The first time an extremist group has produced and used a chemical warfare agent in an attack since Aum Shinrikyo used sarin in Japan in 1995.

In the space and counter-space realm, about 80 countries now are engaged in the space domain. Russia and China understand how our military fights and how I believe we rely on space. They're each pursuing destructive and disruptive anti-satellite systems. China continues to make progress on its anti-satellite missile program.

Moving to counterintelligence. The threat from foreign intelligence entities - both state and non-state - is persistent, complex and evolving. Targeting collection of U.S. political, military, economic, and technical information by foreign intelligence services continue unabated.

Russia and China pose the greatest threat followed by Iran and Cuba on a lesser scale. As well the threat from insiders taking advantage of their access to -- to collect and remove the sense of NASA (ph) security information, it will remain a persistent challenge.

With respect to transnational organized crime - I do want to touch on one crime issue - specifically drug trafficking. The Southwest border seizures of heroin in the United States have doubled since 2010. Over 10,000 people died of heroin overdoses in 2014 - much of it laced with Fentanyl - which is 30 to 50 times more potent than heroin.

In that same year, more than 28,000 died from opioid overdoses. Cocaine production in Colombia, from which most U.S. supplies originate, has increased significantly.

Now let me quickly move through a few regional issues. In East Asia, China's leaders are pursuing an act of foreign policy while dealing with much slower economic growth.

Chinese leaders have also embarked on a most ambitious military reform in -- in its history. Regional tension will continue as China pursues construction of its outposts in the South China Sea.

Russia has demonstrated its military capabilities to project itself as a global power of command respect for the West, maintain domestic support for the regime, and advance Russian interests globally.

Moscow's objectives in Ukraine will probably remain unchanged including maintaining long-term influence over Kiev and frustrating its attempt to integrate into Western institutions.

Putin is the first leader since Stalin to expand Russia's territory. Moscow's military venture into Syria marks its first use since its foray into Afghanistan. A significant expeditionary combat power outside the post soviet space.

Its interventions demonstrate the improvements in Russian military capabilities and the Kremlin's confidence of using them. Moscow faces the reality, however, of economic recession driven in large part by falling oil prices as well as sanctions.

Russia's nearly four percent GDP contraction last year will probably extend into 2016. In the Mid East and South Asia, there are more cross border military operations underway in the Mid East region than at anytime since the 1973 Arab-Israeli War.

And Iraq and ISIL forces will probably make incremental gains through this spring - several of those made in Baiji and Ramadi in the past few months. ISIL is now somewhat on the defensive and its territory and manpower are shrinking but it remains a formidable threat.

In Syria, pro-regime forces have the initiative having made some strategic gains near Aleppo and Latakia in the north as well as in Southern Syria.

Manpower shortages will continue to undermine the Syrian regime's ability to accomplish strategic battlefield objectives. The opposition has less equipment and fire power and its -- and its groups lack unity.

They sometimes have competing battlefield interests and fight among themselves. Some 250,000 have been killed as this war has -- has dragged on. Which is probably a low side estimate.

Meanwhile, the humanitarian situation in Syria continues to deteriorate. As of last month, there were approximately 4.4 million Syrian refugees and another six and a half million internally displaced persons. Which together represent about half of Syria's pre-conflict population.

In Libya, despite the December agreement to form new government in the national accord, establishing authority and security across the country will be difficult with hundreds of militia groups operating throughout the country.

ISIL has established its most developed branch outside of Syria and Iraq in Libya and maintains a presence in Sirte, Benghazi, Tripoli, and other areas of the country.

The Yemeni conflict will probably remain stalemated through at least mid-2016. Meanwhile, AQAP and ISIL's affiliates in Yemen have exploited the conflict and the collapse of government authority to recruit and expand territorial control. The country's economic and humanitarian situation also continues to worsen.



Iran -- Iran deepened its involvement in the Syrian, Iraqi, and Yemeni conflicts in 2015. It also increased military cooperation with Russia highlighted by its battlefield alliance in Syria in support of the regime.

Iran's supreme leader continues to view the United States as a major threat. We assess that his views will not change despite the implementation of the JCPOA deal, the exchange of detainees, and the release of the 10 sailors.

In South Asia, Afghanistan is at serious risk of a political breakdown during 2016 occasioned by mounting political, economic, and security challenges. Waning political cohesion, increasingly assertive local power breakers, financial shortfalls, and sustained country-wide Taliban attacks are eroding stability.

Needless to say, there are many more threats to U.S. interests worldwide that we can address. Most of which are covered in our statement for the record. But I'll stop the litany of doom and we'll address your questions.

NUNES:

Thank you, Director Clapper. I'm gonna go first to Director Comey. Director, there's been a lot recently in the news, as you're well aware, involving the iPhone owned by the San Bernadino shooter.

What exactly are you asking Apple to do? How does this differ from the other times you have asked Apple to help you lawfully obtain communications?

COMEY:

Thank you, Mr. Chairman. In the case in San Bernadino, the judge -- the federal judge has ordered the maker of the phone to do two things. That is, disable the auto-erase function on the phone so that if the FBI is trying to guess the passcode to the phone, it doesn't automatically delete the contents essentially after the 10th try.

And second, to disable the delay between tries function so that if we're gonna try to guess the code, it doesn't take years and years and years but instead, we're able to do it in minutes or in hours.

And to do that through the remote pulsing of codes to the phone. That's what the order is about. And I -- I don't know whether this particular relief has been sought in another court proceeding. I don't think so. Given the nature of this particular phone and its operating system it's possible, but I'm not aware of it.

NUNES:

Well, I'm sure you're gonna be getting more questions from this committee and I know that you're testifying also, I think, next week before the Judiciary Committee.

COMEY:

Yes, I am.

NUNES:

I know this has been an ongoing debate. I want to switch over to Director Stewart. On February 15, 2016, the Daily Beast ran a long report titled, and I quote, "Whistle Blowers Warn Top Spy About Skewed ISIS Intel."

Shortly afterward, our committee was contacted and briefed by ODNI on the survey results. Which indicated that over 40 percent of the analysts at CENTCOM feel there are problems with analytic integrity and CENTCOM processes.

With troops and warfighters, war fighting all over the CENTCOM AOR, is it appropriate that we wait 18 months or longer for the Inspector General report before we even begin to rectify these problems?

STEWART:

Mr. Chairman, I have no control over the pace at which the DOD IG does its investigation. And so while it would be very good for all involved to get closure on exactly the extent of this allegation, we have no control over that process.

And I probably won't comment any further on the investigation. But the survey itself represents just a sampling of the 16,000 plus members that we have in this enterprise. And that enterprise where we put very strict measures to ensure that we comply with analytic standards.

To ensure that we have a process where those who believe that their views are not being heard through red-teaming, through devil's advocate programs, through a sampling of our products.

We think we have in place a pretty good standard and pretty good approach to look at the quality of our analysis and the integrity of our analysis. And I'll leave it at that.

NUNES:

Well it -- it appears like -- at least there was a process in place to get input from the analysts. And to me, it seems like that 40 percent of analysts that are concerned at CENTCOM, you know, that's just something that can't be ignored, you know, regardless of the investigation.

I know that that will take place but, you know, if you have 40 percent of the analysts - I don't know if there's a way. Are you gonna go back in and -- and poll them again or is this -- is this an annual process that the ODNI goes through?

But you know, what changes can be made in the short-term with the -- with the, I guess, for a lack of a better term, the unhappiness of the analysts at CENTCOM?

STEWART:

This is an annual DNI (ph) process. We'll certainly continue to look at ways that we can improve our training. We've done that already.

We've already had requests where there's been a dispute at CENTCOM where we've sent our ombudsman (ph) to look at the analytic rigor and to look at the different views. So we continue to do this process even as this investigation goes on.

NUNES:

Would you consider though the 40 percent to be unusual? Unusually high or is this a normal . . .

STEWART:

I would consider that an unusually high estimate (ph), Mr. Chairman.

NUNES:

Mr. Schiff?

SCHIFF:

Thank you, Mr. Chairman. Director Comey, I want to ask you about the Apple case as well.

The -- the facts of the San Bernadino case are obviously pretty compelling in terms of wanting to know what's on that phone. Whether there were other parties involved or other plans or -- or targets of attack.

And while that application, as you pointed out, is focused solely on that phone - when I read the emotion and support of the application under the All Writs Act, I don't see a limiting principle.

By that I mean that if that argument is accepted by the court in this case, won't it lead district attorneys and other prosecutors around the country to essentially make the same argument in their cases? And some of those may be compelling. I think you pointed to a pregnant woman who was murdered, I think, in Arkansas and that phone may be the only key to who her killer is.

But nonetheless, that -- that application may be good in misdemeanor cases involving non-violent offenses. And so while the result may only affect this phone, the precedent will be there for many others.

And I guess what I'd like to ask you is is there a limiting principle here? Is there a way through negotiation that we can arrive at cases where it's appropriate to seek this relief and cases where it's not? Do you acknowledge, sort of, the broader policy implications of a uniform application under the All Writs Act?

I realize this may be mooted by the next generation of operating systems which may not allow this kind of relief. But nonetheless, if it is technologically feasible, even with the next generation operating system for Apple to help with the opening of a phone, it seems to me that the argument you're making in this case will apply to those new operating systems as well.

So is there a limiting principle here and is there any way to resolve this through negotiation? Because at least the initial positions of the parties are we need access and we have legal warrant. And the other side is saying we can never provide access because if we do here, we'll have to do it everywhere.

COMEY:

OK. Thank you, Mr. Schiff. And I should say I very much agree with the way you framed it in your opening statement. This case and all cases are very, very important.

But there's a broader policy question that is far larger than any individual case that we all have to grapple with. But to the case - first I think the answer would best come from a technical expert and a good lawyer. I'm neither of those.

But I will take a shot at it. I do think that it is potentially -- whatever the judge's decision is in California, and I'm sure that it will be appealed no matter how it ends up -- will be instructive for other courts.

And there may well be other cases that involve the same kind of phone and the same operating system. What the experts have told me is the combination -- here's where I'm gonna get well out of my depth -- of a 5C and this particular operating system is sufficiently unusual that its unlikely to be a trail blazer because of technology being the limiting principle.

But sure, a decision by a judge -- there's a judge weighing a decision in Brooklyn right now. All of those decisions will guide how other courts handle similar requests.

The All Writs Act, as you mentioned, is a tool that I used as a young prosecutor. We've used for hundreds of years so that courts can have their orders given effect and how judges now interpret that in any particular jurisdiction is not binding on others but will be important.

So I think that's fair to say. But I do think a larger question is not gonna be answered in the courts and shouldn't be. Because it's really about who do we want to be as a country and how do we want to govern ourselves?

SCHIFF:

Let me ask you: what about that broader policy question from the Bureau's perspective? And that is, can you live with a policy -- can law enforcement live with a policy that says only in certain cases - whether they're violent crimes or other very serious cases, terrorism related - that we would allow into the All Writs Act and Congress could specify to which purposes the All Writs Act or a change to CALEA (ph) would apply?

Is that something that the law enforcement community, Intelligence Community, you think, could negotiate with privacy, stakeholders, and with the technology sector?

COMEY:

I think conversation and negotiation is the key to resolving this. This is the hardest question I've seen in government and it's gonna require negotiation and conversation.

But I've been very keen to keep the Bureau out of the policy making business. I think we have two roles in this context. One is in the cases we must do a competent investigation following the murder of 14 people in San Bernadino. And we will.

And we'll use whatever lawful tools are available to us. But in the larger conversation, I think our role is just to make sure folks understand what are the costs associated with moving to a world of universal strong encryption.

There's tons of benefits. I love encryption. I love privacy and when I hear corporations saying we're gonna take you to a world where no one can look at your stuff, part of me thinks, "that's great. I don't want anybody looking at my stuff."

But then I step back and say you know, law enforcement, which I'm part of, really does save people's lives, rescue kids, rescue neighborhoods from terrorists. And we do that a whole lot through court orders that are search warrants. And we do it a whole lot through search warrants of mobile devices.

So we're gonna move to a world where that is not possible anymore?  
The world will not end, but it will be a different world than where we are today and where we were in 2014.

And so we just have to make sure that the Bureau explains to folks what the costs are so that people don't look at us five years from now and say, "where were you guys when this happened"?

This is too important to let us drift. And so my goal is to have the Bureau be a factual input so we have a really robust conversation that's well informed.

SCHIFF:

Thank you, Director. And I know my colleagues will have more questions so I -- I -- I, you know, defer to them. There's one other matter I wanted to raise though and that's the subject of Libya

Deeply concerned that as the size of the tumor in Syria and Iraq decreases, that we're seeing a growth of a new malignancy in Libya. There seems to be a concern with taking more aggressive military action against ISIS and Libya. That it would somehow interfere with the ongoing, never ending it seems, negotiations to try to get the two political parties together and form a common government.

From an Intel perspective, do you think that we could take more aggressive military action against ISIS in parallel with the political negotiations or do you think we have to choose between them?

Because I'm concerned that if the -- the pace of those negotiations which seemed endless, that we may get to the point where ISIS is so firmly entrenched in Libya that we have to embark on the same multi-year project that we're undertaking in Iraq and Syria.

CLAPPER:

Well, I'll start that and others can contribute. I -- I think you've very aptly characterized the dilemma here is, in terms of a more robust military intervention in Libya, and the potential jeopardy that imposes to a very fragile evolving political process.

There's great hope for this new government of national accord. We'd like nothing better than to have a government in place in Libya with whom we could work and from whom we could gain consent for engaging militarily in Libya

That is a -- a subject of active discussion as I speak. John, you want to...

BRENNAN:

I think there was recognition that there was a relationship between government building. Trying to get this government of the national accord off the ground and kind of terrorism operations. And the discussions that I think Jim and I and others have been in recognize that sometimes.

So what you do in one environment affects the other. But I think the -- the purpose is to try to pursue both with -- with vigor and simultaneously recognizing that you cannot put off the counterterrorism operations as this long process of government building continues to take place.

SCHIFF:

Just to drill down a bit further on that. Do either of the political factions that are trying to form a common government - do either of them take issue with the necessity of military action against ISIS?

I'm trying to get an understanding as to why, in an effort that I hope would be more fully integrated with European military leadership, a more aggressive approach against ISIS and Libya would somehow interfere with political negotiations.

CLAPPER:

Well, the governments that -- the two competing governments also -- neither of them are monolithic. There are a spectrum of political views within each one of those.

So I think there is, to the extent that there can be in Libya, a fair amount of agreement that ISIL poses a threat to -- to Libya as -- as -- as a nation state and I think there is sentiment among the -- most parties but not all -- that this represents a threat to -- to the country.



But there is not -- and that's the difficulty here -- there is a -- a wide range of -- of views among -- in the political spectrum in Libya.

SCHIFF:

Thank you, Mr. Chairman. I yield back.

NUNES:

Mr. Miller?

MILLER:

Thank you very much, Mr. Chairman. As the Chairman eluded to in his opening statement, there's a lot of education that's gonna be taking place about Section 702. And Director Clapper, Brennan, Director Comey - if you would, in this open session - please elaborate briefly, if you will, how important Section 702 is to your respective agencies.

CLAPPER:

Well, I'll start but -- and I would also invite Rick Ledgett, the Deputy Director of NSA -- but all of us have an equity here. 702 represents a vital capability -- intelligence capability for all of us. And just to be clear, this -- this is the provision in the Foreign Surveillance Act that governs a collection on non-U.S. persons overseas.

And the current law expires in -- in December of 2017. And so we are already embarked on, kind of, an education campaign in the Congress to ensure people understand what a vital tool this is.

Let me turn first to Mr. Ledgett.

LEDGETT:

Thank you, sir. I agree with what the -- what the Director said that it -- it is in fact a vital tool for our intelligence efforts against valid foreign intelligence targets - non- U.S. persons who are overseas.

And it does not permit the targeting of U.S. persons that would require a separate court order to do that.

In the course of conducting -- conducting collection under Section 702, if a -- if a U.S. person is in contact with a valid foreign intelligence target, there are minimization procedures that we use to minimize the -- the retention and the disclosure of the identity of that person because it's not a foreign intelligence value. And those are reviewed annually by the court.

MILLER:  
John?

BRENNAN:  
702 is a -- is a critical tool for CIA for the collection of foreign intelligence as well as our operational activities. Whether they be on a counterterrorism front, counterproliferation -- counterproliferation front, or as well as others.

There have been numerous instances over the years where 702 has been instrumental in our ability to uncover and also help disrupt activities that are a threat to our national security interests.

And as you can imagine, open sessions typical to go into some of those. But let me just mention at least one. In late 2014, a long time Libyan extremist operative was arrested by local authorities in Europe following several trips into Syria and Libya while he met with senior extremist operatives.

At the time of his arrest, CIA assessed that he was involved in external operational planning and CIA provided this lead information from Section 702 collection to assist the local governments in their investigation that led to the arrest of that individual.

That is, I think, epitomizes in many respects the way that 702 intelligence is used by CIA working frequently in constant with their partners around the world to disrupt these activities that frequently have a terrorist mention to them or a proliferation mention (ph) to them.

COMEY:  
The only thing I'd add, Mr. Miller, is reasonable people could and did argue about how important the telephone metadata collection was. This is not even a close call.

This is -- if we lost this tool, it would be a very bad thing for us. And so it's very important to have this conversation early. So I thank you for the question.

MILLER:

Thank you, Mr. Comey. I yield back.

NUNES:

Gentleman yields back. Mr. Himes?

HIMES:

Thank you, Mr. Chairman. Gentlemen, thank you for being here. Director Comey, I want to pick up the line of questioning on the Apple FBI. As Mr. Schiff said that the facts are compelling in this case.

Some of the issues, as you have acknowledged are -- are novel and challenging. It is this body that should be determining the answer to the questions that you ask and that will be resolved in the judiciary.

And of course, we will once again shirk our constitutional duty as we have on an authorization for the use of military force as we're preparing to do with respect to advice and consent on a supreme court nominee and we will again on this issue which is sad.

So it leads me to two questions to you, Director, about I guess the thinking of the FBI. And the first question really is -- is a follow on to Mr. Schiff's.

It's my understanding that the position of the FBI is a very narrow one. That the request of Apple really pertains to this device in this instance.

There's a legitimate worry, though, that a decision in favor of the FBI could be the narrow end of a very wide wedge. And Mr. Schiff asked about the legal domain of cases to which this might apply.

I want to ask about the authority. If the FBI prevails, Apple will be required to write some code at the behest of the government. My question is: where does this authority end?

For example, is it the position of the FBI that it has the authority to compel the inclusion of code into a new device? Can you paint a very bright line for us with respect to where you think that authority ends that might reassure those people who say, "where does it end"?

COMEY:

Thank you, Mr. Himes. I don't think I can by virtue of expertise, or should by virtue of my role. I -- I really do think the Department of Justice, the lawyers who are representing the government in this case, are best situated to do that.

I think these are reasonable questions because judges on both coasts, and probably in lots of other places, are gonna have to interpret what is the meaning of the All Writs Act and what is reasonable assistance. And I'm really not somebody qualified to offer you a good answer to that one.

HIMES:

OK. So it's not, at this point in time, a belief of the FBI that the authority could go beyond what it has requested in this particular case?

COMEY:

Yeah, I actually have not thought of it. Here's the way I think of it. The FBI focuses on case and then case and then case. I've said this to folks and I've said it because it's true - the San Bernadino litigation is not about us trying to send a message or establish some precedent. It really isn't.

It's about trying to be competent in investigating something that is an active investigation. And so I don't know how lawyers and judges will think about what is the limiting principle on the legal side. I just don't know.

HIMES:

OK. Thank you. My second question, really, is about a different way to think about this. Right now we're having this conversation primarily in terms of the tension between privacy and security.

But there's a different tension which is security versus security. If you prevail and if this code is written, presumably as Mr. Schiff pointed out, it will be the subject of other requests for law enforcement. This code will exist presumably on a server at Apple.

And that creates a very substantial threat. It will -- if this code exists on a server at Apple -- it will presumably become the target of our sovereign adversaries, of criminal enterprises, of terrorists.

And you don't need to think too hard to spin some pretty ugly scenarios if that code gets out into the wild. Now a terrorist entity maybe knows my precise location, gets photos of my children.

So I -- I wonder if you could give us a sense for, in taking the position that the FBI has, how did you think about the trade-off between the very compelling desire to get the information on this particular San Bernadino case with the risks that would be posed by the existence of this code should it exist and -- and ultimately perhaps get out into the wild?

COMEY:

Again, I think that's something that the court is gonna sort out. And I'm trying to be cautious in answering because I'm not an expert. But what the experts have told me, and I'm sure this will be sorted out by the judge, is the code the judge has directed Apple to write works only on this one phone.

And so the idea of it getting out into the wild and working on my phone or your phone, at least the experts tell me, is not a real thing. The second thing -- and the second thing is that the -- the code will be at Apple.

Which I think has done a pretty darn good job of protecting its code. Before 2014 they were able to unlock any phone and I don't remember any code getting out that let that ability lose upon the land. But again, I'm not an expert and I do think that's something the judge is gonna have to sort out.

HIMES:

Thank you, Director. Director Clapper, in my limited time, I wanted to thank you for raising the issue of cyber security in your written testimony. I wonder -- agreements were made when the Chinese

president visited our president -- I wonder if you could characterize whether those agreements have been effective in reducing the amount of cyber espionage and cyber activity that we've seen out of China.

CLAPPER:

We did probably go into that in more detail on a closed session. As I indicated in my oral remarks, I think the jury's out. We have seen some reduction but I don't think we're in a position to say at this point whether they're in strict compliance. And we can go into that in more detail in a closed session.

HIMES:

Thank you. Thank you, Mr. Chairman.

NUNES:

Gentleman yields back. Mr. King?

KING:

Thank you, Mr. Chairman. I'd say two main questions to Director Comey on Apple. One is: were there any negotiations between the FBI and Apple leading up to the court proceeding?

COMEY:

Yes, plenty.

KING:

Like what?

COMEY:

They were very helpful, by the way. I want to be sure people understand. No demons in this dispute or the larger dispute. Apple's been very cooperative. We just got to a place where they were not willing to offer the relief that the government was asking for.

KING:

And secondly, just to knock down a media story. I've heard several people in -- in the media say that the FBI could do this if they wanted to but they are trying to establish a case here just given the opportunity to -- what do you think about that?

COMEY:

It's the product of people watching too many TV shows. I don't mind TV shows about FBI but sometimes we're not as attractive or as technologically talented as we appear on TV.

(LAUGHTER)

KING:

OK. I yield back.

NUNES:

Mr. Quigley?

QUIGLEY:

Thank you, Mr. Chairman. Thank you, gentlemen. Diving in a little deeper into Ukraine and Russians. I don't know who wants to comment on this first but some sense of their strategic goals here.

Obviously, the impact of sanctions is pretty dramatic to their economy. Is this, I guess, a frozen conflict and what else can we anticipate?

CLAPPER:

Well, the -- what's had the greater impact on Russia -- Russia's economy has been the precipitated drop in the price of oil. Where (inaudible) crude is running around \$37 or \$38 dollars, if that, a barrel.

And the planning factor that the Russians have consistently used in their budgeting is \$50 dollars a barrel. So sanctions have certainly contributed to that. But the -- the major impact has been with oil.

I think the Russians consider Ukraine "Little Russia." It's -- I think it's deeply steeped in their history and their culture. And so they are going to attempt to sustain influence, particularly in the two separatist

republics - Donetsk and Luhansk. And obviously what the Russians most fear and they're most concerned about is Ukraine gravitating to the West more than it already has.

Meaning becoming part of the European Union or worse, NATO. So Russia will continue, I think to, via proxies - the separatists (ph) sustain their influence in -- in the Ukraine in that matter.

QUIGLEY:

Do you see the status continuing the way it is or some -- obviously there's -- there is renewed conflict at different times but no dramatic change recently.

CLAPPER:

That's right. I think they will, for now, maintain more or less the status quo. That's creating some issues among the separatists from a moral standpoint.

And a lot of the incidence that are occurring along the -- the line that has been drawn via the Minsk Agreement are occasion by upstart separatists whom this -- the Russians don't completely control.

John, do you want to add to that?

BRENNAN:

There has been some -- some movement as far as negotiations with the Minsk Agreement. But there still is shortcomings as far as implementation of that.

But your characterization of a -- of a frozen conflict, I think there's still uncertainty about how the -- the Russians themselves are going to execrate (ph) themselves from this which is taking a toll in addition to the oil prices because of sanctions.

QUIGLEY:

Well, given the economy for whatever reasons and the two conflicts they're most involved with, do you sense that Putin feels they have their hands full or do you -- do you have concerns about efforts to destabilize the Baltic region?



CLAPPER:

Well, there are concerns about that. Although right now that's more in the soft arena, if you will. And the information and operations are cyber realm rather than hard military assault on the Baltics. That doesn't seem to be in the cards right now.

I do think the Russians are preoccupied right now with -- with Syria. And they've put a lot into that. They are confronting the possibility, I think, or considering whether they're gonna put more ground forces in.

Of course, I think the constraining factor for them is a -- is a memory of Afghanistan. Getting into, kind of, a bottomless pit. And I think that does affect Russian thinking and is a reason -- one of the reasons why I think there is apparent interest in a cessation of -- of hostilities.

QUIGLEY:

Thank you, gentlemen.

NUNES:

Gentleman yields back. Mr. Westmoreland is recognized.

WESTMORELAND:

Thank you, Mr. Chairman. And thank you all for being here. Excuse my voice.

Director Comey, this warrant that you went to the court to get. It was really no different of a process of what you do for a Pfizer (ph) or any other warrant that you would want to get to check on some evidence.

I mean, you were just trying to get where you could get into the phone. Not do anything else, is that correct?

COMEY:

That's correct. As in thousands of other criminal investigations across the country who want to search. Go to a federal judge, make a showing of probable cause to believe there is evidence relevant to the investigation on the device, and get a search warrant from the court for the device.

And then what happened here is then, because the device was unable to be opened, the judge issued a separate order under this thing called the All Writs Act to try to give effect to the court's search warrant that told the manufacturer, "you must assist in disabling this auto-erase function so they can try to guess it," and execute the search warrant.

WESTMORELAND:

To me, you know, just from a common man, you know, I would think it's different if you've got two people that have killed 14 other folks in a terrorist attack and you're just trying to get through the security code to get into the device versus some divorce lawyer trying to find out what a philandering husband they have been talking to.

So I think there is a total difference to that. And I think the American people sense that this isn't -- these are people who have committed a crime.

The next thing I wanted to ask is, you know, we've been going through a lot of the Iran nuclear deal and we have given them a large sum of money. Different varying figures of that.

But I know that a lot of your agencies take part in monitoring the financing of ISIL and whether that's in Libya or Iraq or -- or Syria. And how are we monitoring what the Iranians are able to do or are doing?

And it's an open question, any of you can jump in there -- as far as what these funds are. Because to me, it gives a perfect opportunity with them going to France and other places and making these large purchases. Just another great opportunity to laundry money.

CLAPPER:

Sir, we can maybe go into detail in a -- in a closed session. I think I'd say here that of the money that was released or freed up by virtue of the JCPOA, that much of it is encumbered either for debt or for demanding domestic needs of the -- of the Iranian economy.

And some money has flowed to -- and you know, the organization we worry most about I guess is the IRGC. In particular, the Quds Force. Some money is flowed to them but they -- not as nearly as much as they wanted.

And I think as far as how tracking finances and -- and financial data, this would be best -- the details of that would be best left to a closed session.

WESTMORELAND:

Thank you, gentlemen. I yield back.

NUNES:

Gentleman yields back. Ms. Sewell?

SEWELL:

Thank you, Mr. Chairman. Thank you gentlemen for your testimony today.

Director Clapper, I think I -- I want to turn back to cyber security and I wanted to see if you could talk a little bit about what you think your assessment is of IC's - Intelligence Community's ability to counter cyber threats. And talk a little bit about what you see as future threats that we would face and whether or not we are able to meet those challenges.

CLAPPER:

Well, the Intelligence Community's role in all this, of course, is classically the intelligence. That is, to collect and analyze information on -- on threats in the -- in the cyber domain.

And then in support of others who are more directly responsible for either planning attacks or -- or -- or for defense. In our forthcoming budget, in fact, in our budget submission -- and I'll speak to it next week as to what we're actually investing or asking for in 2017.

I think the general threat environment is -- is quite daunting. Both from the standpoint of the capability of the nation state - prime among them Russia and China - and then non-state actors.

There is an inverse relationship between the ability -- the capabilities that countries have. China and Russia being the most formidable. Perhaps less -- less threatening in terms of their intent whereas you have, you know, second tier countries of the likes of Iran and particularly North Korea. Lesser capabilities...

SEWELL:

What do you -- what do you see as our ability to counter...

(CROSSTALK)

SEWELL:

How -- how would you assess our ability to counter those threats?

CLAPPER:

Well, by countering them or collecting against them?

SEWELL:

Both, actually.

CLAPPER:

Well, countering them in one dimension is, I think, our ability to defend. Which is not just a government thing but, you know, the private sector as well. So when you say defend, that is a -- that's a big domain.

I think our concern, our responsibility and -- and our intent, of course, is to be able to collect the threat information so we convey to those who are responsible for defending. And in the case of say CYBERCOM attacking, that they have the adequate intelligence to bring to bear for that.

SEWELL:

With respect to space sector, can you tell us a little bit about -- I know you -- you have in your report more detail. But our ability to -- to defend against or counter some of the Russian and Chinese anti-satellite missile system?

CLAPPER:

Again, this is a subject that's left perhaps in detail for closed session. But I'll just say that both the Russians and the Chinese have embarked on a very aggressive and versatile and diverse set of capabilities in the space domain.

And this has prompted a lot of attention on both the part of the Department of Defense as well as the Intelligence Community to provide an array of defenses and resilience and reconstitution, if necessary, should we lose our viable space assets.

This is a commentary, I think, on both Russian and Chinese insight and understanding about how heavily the United States depends on space for a whole variety of needs.

SEWELL:

Thank you. I yield back the rest of my time.

NUNES:

Gentlelady yields back. Dr. Heck?

HECK:

Thank you, Mr. Chairman. Thank you all for appearing here today and for your long service to our country and through you, our thanks to the many men and women who your agencies represent.

Director Comey, not to beat the Apple issue to death but one quick question. Has Apple clearly articulated what their reasons are to not cooperate to the extent that you've requested?

Is it the, you know, slippery slope, Fourth Amendment, civil liberties? Or is it more of an economic issue to them where they're cooperation in showing the world that they might be able to accomplish what's requested makes their device less desirable and therefore lose market share?

COMEY:

I don't think that's a question, Dr. Heck, that I -- I can or should answer. I don't -- obviously I don't want to talk about our private conversations in the course of this investigation about Apple.

I know there's been a bunch of stuff in the press. And they'll obviously have an opportunity to file in the court, I think today or tomorrow, to explain why they don't believe the order is legally and factually appropriate. So I think I got to leave it there.

HECK:

Alright. I -- I appreciate that. We'll wait for the court filing then to see what their claims may be and I yield back, Mr. Chair.

NUNES:

Mr. Carson?

CARSON:

Thank you, Mr. Chair. Director Comey, without getting into classified territory - can you describe how the FBI makes a determination to determine which communities warrant proactive outreach and engagement to prevent radicalization and -- and recruitment under the CVE umbrella?

COMEY:

I think so. Any community where either we or the community believe there is a risk of people turning towards violence. And sometimes that's an ethnic community, immigrant community, sometimes it's a -- it's a particular community with a particular flavor of anti-government sentiment. Whoever there's -- especially young people might turn to violence. There we try and engage with folks in that community.

CARSON:

Is -- is -- is the intention to include more of a holistic approach by bringing in not only the community leaders but educators within the community? Psychologists within the community?

COMEY:

Yes.

CARSON:

To prevent the kind of self-radicalization that's taking place?

COMEY:

Yes, sir. It has to be an entire community thing. It can't be a law enforcement thing, it can't be a religious institution thing. It's gotta be parents and educators and physicians and law enforcement and social workers.

To one of the things the Bureau is trying to do as part of our countering violent extremism effort is bring together those talented people from all different perspectives in the community.

So especially if we encounter a young person who hasn't yet moved to the place where we're gonna have to lock them up. That there's the -- the prospect of a group coming together and redirecting that person. But it has to be a whole lot of folks besides us.

CARSON:

Has the Citizens Academy been an effective tool in creating some kind of buy-in with those communities?

COMEY:

Yes. Because the Citizens Academy, which Congressman you know well, is an effort the FBI runs in all 56 of our field offices.

We invite in people from all walks of life to spend time getting to know how we do our work, ask us hard questions, and then stay involved with us to give us feedback on how we're doing and to connect us to all different parts of the community. So it's a vital tool.

CARSON:

Thank you. Mr. Chairman, I yield back.

NUNES:

Dr. Wenstrup's recognized.

WENSTRUP:

Thank you, Mr. Chairman. And I do want to thank all of you for being here and as Dr. Heck said, all those that you represent and the work that you do.

I have a question more for later in closed session but one thing that I -- I think we can't ignore, as we sit here on the side of Congress, you know, Admiral Mullen spoke years ago about our debt being a threat to our national security.

And so I want to ask you, Director Clapper, you know, as we face all these increased external threats to our nation, how does this basically internal threat of our debt affect our capabilities in the work that you do?

CLAPPER:

Well, it's -- it affects this if -- if -- to the extent that that has inhibition on our -- our -- our resources. Meaning our funding. So that's why, you know, we've been very concerned about the impacts of sequestration. Which we're not through yet.

So in that respect, it -- it, you know, it -- it is a concern. I have to say that, thanks to the Congress, we've done reasonably well in our funding requests and I hope the same is true in 2017.

Certainly, I'll just say as a citizen, I think I do worry about our debt as a country. And so I -- I worry about it from that respect.

WENSTRUP:

Well, in the -- in the line of national security, I -- I think that we need to continue to address your needs and it's helpful to us when you discuss whether you have the appropriate wherewithal to do your job as we make decisions here.

Thank you for that input and I yield back.

NUNES:

Gentleman yields back. Mr. Stewart is recognized.

STEWART:

Thank you, Mr. Chairman. And to you gentlemen I express my appreciation and gratitude. And sincerely on behalf of millions of Americans who may or may not recognize the -- the -- the really wonderful work that your organizations do and the many dedicated men and women who sacrifice to do that - thank you.



I -- I would like to -- I suppose I could ask this question to nearly all of you although, Director Brennan or perhaps Mr. Comey as well, you might be best suited. Although Mr. Ledgett, I appreciate your opinion as well.

In this conversation with Apple which is taking a fair amount of our time here, the longer term problem - and we've had opportunities to talk about this with all of you - is the prospect that within a few short years, we may be, you know, use the phrase "dark with heavy encryption," that doesn't allow us to -- to use law enforcement mechanisms or national security tools. And I'm wondering if you would elaborate on what that really means.

Could we help the American people understand that the encryption which we may not control - they may not be U.S. companies that are developing this encryption. That it's becoming widely available and how that's going to make it more difficult for you to keep us, as we expect, to keep American people safe.

Dr. Comey, yes. If we could...

COMNEY:

This is a problem that all of us in the Intelligence Community have been talking about to sound an alarm. Because we see increasingly in our national security work - and the Bureau has significant criminal responsibilities in our criminal investigative work. Increasing situations where we cannot, with lawful court orders read the communications of terrorists, gangbangers, pedophiles - all different kinds of bad people.

And with again, lawful court orders and search warrants were increasingly unable to make that search warrant effective, alright? And enter a device with the court's permission and get what's on there.

That affects all of our work. You've seen it. This committee obviously knows a lot about it. Most prominently in the counterterrorism side with ISIL. Which is reaching into the United States. Trying to motivate people to either come to their so-called caliphate or kill in the United States.

And when they find someone they think will either come or kill, they move them to an -- a mobile messaging app that's end-to-end encrypted that we can't read with court orders.

And that is a big problem for us. There are substitutes around the edges of it. People talk about metadata, which is the information about who contacted whom. That's useful but it's no substitute for knowing what they're talking about.

Sometimes physical surveillance is useful. Sometimes informants are useful. But there really is no substitute - anybody who knows our work will tell you this - there's no substitute for being able to have a judge order access to the content.

And so our job is not to tell the American people what to do about it. We're just here to tell you there is a big problem and that darkness is gonna grow and grow and grow and change our world.

STEWART:

Director Brennan, would you or Mr. Ledgett elaborate on that from -- from more of an international perspective in the work we're trying to do overseas and the encryption and how that affects that?

BRENNAN:

Well, I'll start and then I know Rick will have some comments. One of the most important missions for CIA is the collection of foreign intelligence. And increasingly, the cost of the terrorist threat we face, we need to get that intelligence that resides within intelligence organizations.

The ability of these terrorists to communicate with one another in manners that make it very difficult for us to uncover. It has been increasing. And it is very frustrating but also very concerning because they follow the press, they follow these discussions.

They are very sophisticated. A lot of them have grown up in an era of technological revolution and they've been able to take advantage of that. And so it has made our -- our challenges very difficult.

So from my perspective, on the foreign intelligence front, the more intelligence that we can obtain through our lawful authorities the better able we are to protect the American people.

NUNES:

Rick?

LEDGETT:

Yes, thank you, sir. I -- I agree with -- with both Director Comey and Director Brennan on the -- on the importance of this and the impact it has.

We track when our foreign intelligence targets talk about the communication or the security of their communications. And we see a growing number of them because of the -- the information that's in the press about -- about the value of encryption moving towards that in a way that inhibits our ability to understand what they're doing.

And what Director Comey said about the difference between metadata and content is hugely important and often overlooked. It's one thing to know that a person is in a particular place at a particular time.

It's something else entirely and necessary to understanding in defeating terrorist plots to know what the target is, what the timing is, how the attack is going to develop.

STEWART:

Well, in conclusion I would just say this. I appreciate your conversation with Apple and -- and Director Comey, you -- you, I think, stated it well.

This is a conversation I think the American people need to have. We -- we talked a little bit about 702 and -- and, you know, the pathway forward with that as well.

But it seems to me that technologically some of these conversations may become moot because we may not have access to that information regardless just because technology makes it impossible for us in the future. And how we grapple with that is something I think we should consider as well.

But Mr. Chairman, thank you and I yield back.

NUNES:

Gentleman yields back. I want to thank the panel for the open session portion of the World Wide Threats Hearing. We will hopefully reconvene about 10:30 down in the classified spaces.

CQ Transcriptions, Feb. 25, 2016

### **List of Panel Members and Witnesses**

PANEL MEMBERS:

REP. DEVIN NUNES, R-CALIF. CHAIRMAN

REP. JEFF MILLER, R-FLA.

REP. K. MICHAEL CONAWAY, R-TEXAS

REP. PETER T. KING, R-N.Y.

REP. FRANK A. LOBIONDO, R-N.J.

REP. LYNN WESTMORELAND, R-GA.

REP. JOE HECK, R-NEV.

REP. TOM ROONEY, R-FLA.

REP. MIKE POMPEO, R-KAN.

REP. ILEANA ROS-LEHTINEN, R-FLA.

REP. CHRIS STEWART, R-UTAH

REP. MICHAEL R. TURNER, R-OHIO

REP. BRAD WENSTRUP, R-OHIO

REP. PAUL D. RYAN, R-WIS. EX OFFICIO

REP. ADAM B. SCHIFF, D-CALIF. RANKING MEMBER

REP. LUIS V. GUTIERREZ, D-ILL.

REP. JIM HIMES, D-CONN.

REP. TERRI A. SEWELL, D-ALA.

REP. ANDRE CARSON, D-IND.

REP. MIKE QUIGLEY, D-ILL.

REP. JACKIE SPEIER, D-CALIF.

REP. ERIC SWALWELL, D-CALIF.

REP. PATRICK MURPHY, D-FLA.

REP. NANCY PELOSI, D-CALIF. EX OFFICIO

WITNESSES:

JAMES R. CLAPPER JR., DIRECTOR OF NATIONAL INTELLIGENCE

JOHN O. BRENNAN, DIRECTOR, CIA

FBI DIRECTOR JAMES COMEY

NICHOLAS J. RASMUSSEN, DIRECTOR OF THE NATIONAL  
TERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL  
INTELLIGENCE

LIEUTENANT GENERAL VINCENT STEWART (USMC), DIRECTOR,  
DEFENSE INTELLIGENCE AGENCY

RICK LEDGETT, DEPUTY DIRECTOR, NATIONAL SECURITY  
AGENCY

---

Source: **CQ Transcriptions**

© 2016 CQ Roll Call All Rights Reserved.

# **Exhibit G**

**SFGATE**

<http://www.sfgate.com/business/article/As-Apple-FBI-spar-Feinstein-pushes-bill-to-7237590.php>

## As Apple, FBI spar, Feinstein pushes bill to require decryption

By **Sean Sposito and Carolyn Lochhead** Updated 7:57 pm, Friday, April 8, 2016



IMAGE 1 OF 3

[Buy Photo](#)

United States Senator Dianne Feinstein talks to the editorial board at the San Francisco Chronicle in San Francisco, Calif. on Tuesday March 29, 2016.

California Sen. Dianne Feinstein confirmed Friday she is seeking new legislation to compel technology companies to assist government agencies in gaining access to encrypted technology, opening a new front in a continuing battle over the issue.

A leaked draft of the legislation co-sponsored by Feinstein appeared online as the Department of Justice renewed its efforts to obtain access to an iPhone in a Brooklyn drug-dealing case and an Apple executive accused the government of attempting to expand its powers beyond what the law allows.

The rapid-fire series of events shows how the debate over encryption — the technology

that safeguards government secrets, online bank transactions, medical records, and an increasing swath of personal communications — is moving to a new stage, with battle lines more clearly drawn than before.

Feinstein represents a faction in the government and law enforcement who are seeking to limit the use of encryption and force companies to build products with back doors that law enforcement agents can access.

Technology companies, alarmed by revelations of government spying and concerned that consumers will distrust them and stop using their products, want to include encryption tools that even company officials and engineers can't break. That way, even if served with a court order, they would not be able to decode and turn over user data.

### **Bill draft gets leaked**

Feinstein's office confirmed to The Chronicle Friday that the senator was working with Sen. Richard Burr, R-North Carolina, on legislation to address encryption. The leaked draft called the bill the "Compliance with Court Orders Act of 2016."

"All providers of communications services and products (including software) should protect the privacy of United States persons through implementation of appropriate data security and still respect the rules of law and comply with all legal requirements and court orders," reads the draft, which was [posted online Thursday by The Hill reporter Cory Bennett](#).

In a joint statement, Burr and Feinstein said the bill remains a "discussion draft," and would not comment on the specific language of the leaked document.

"However, the underlying goal is simple: when there's a court order to render technical assistance to law enforcement or provide decrypted information, that court order is carried out," the senators said. "No individual or company is above the law."

### **'Soliciting input' now**

Feinstein and Burr said they were still "soliciting input from stakeholders and hope to have final language ready soon."



Such controversial legislation is highly unlikely to pass the Senate during an election year.

Reuters reported Thursday that White House sources said the legislation would also lack administration support. Reuters pointed to President Obama's remarks last month suggesting the government should have access to encrypted information, but also to White House press secretary Josh Earnest's remarks saying he was skeptical of legislative attempts to solve the problem.

The American Civil Liberties Union called the Feinstein-Burr bill "a clear threat to everyone's privacy and security ... that ignores economic, security, and technical reality."

### **'Easy prey for bad actors'**

Linda Moore, president and CEO of TechNet, a group representing industry executives, said the bill "could establish standards that force companies to eliminate security features that may be exploited by others who do not share law enforcement's good intentions." Moore warned that should it pass, "common transactions will become easy prey for bad actors" and cause customers everywhere to "lose faith in the trustworthiness of American products and choose alternatives that don't have the same vulnerabilities."

Meanwhile, on Friday morning, Department of Justice lawyers sent a letter to Eastern District of New York Judge Margo K. Brodie stating that the FBI continued to be unable to break into a drug dealer's iPhone.

In late February, U.S. Magistrate James Orenstein of Brooklyn **denied the Justice Department's original request** to compel Apple to assist the FBI in accessing data on the phone, saying that the government lacked legal authority to do so.

The wording of the leaked legislation suggests that its authors are trying to find a way to give law-enforcement agencies legal room to maneuver in such cases.

In March, after the FBI announced it had found a way to unlock an iPhone used by San Bernardino shooter Syed Rizwan Farook, Apple asked the Brooklyn court to postpone a hearing on the order. Company lawyers argued that the outcome of that case would

affect the Brooklyn case.

“In this case, we still need Apple’s help in accessing the data, which they have done with little effort in at least 70 other cases when presented with court orders for comparable phones,” Justice Department spokeswoman Emily Pierce said.

This week, FBI Director James Comey made a speech at Kenyon College where he said that the scope of the technique used on the San Bernardino shooter’s iPhone was limited.

Various iPhone models have different hardware features and run different versions of Apple’s mobile operating system. Techniques used to defeat Apple’s protections often depend on a device’s specific configurations and can’t be applied across the board. In the San Bernardino case, for example, the iPhone was a 5C and the Brooklyn phone was a 5S, a newer model. Yet the Brooklyn phone was running an older operating system. For law-enforcement agents, dealing with all these complexities is just part of the challenge.

As Comey put it, the San Bernardino phone was “a bit of a technological corner case.”

“The world is moving on to (iPhone) 6s. This (technique) doesn't work in 6s, it doesn't work in a 5S, and so we have a tool that works on a narrow slice of phones.”

### **Setting a precedent**

An Apple executive who spoke to reporters on a conference call Friday morning on the condition that he not be named, said the Department of Justice was trying to set a precedent in the Brooklyn case.

There reportedly are hundreds of iPhones — as well as other models of smartphones — held as evidence in cases where law-enforcement officials have said they can’t access data on the devices.

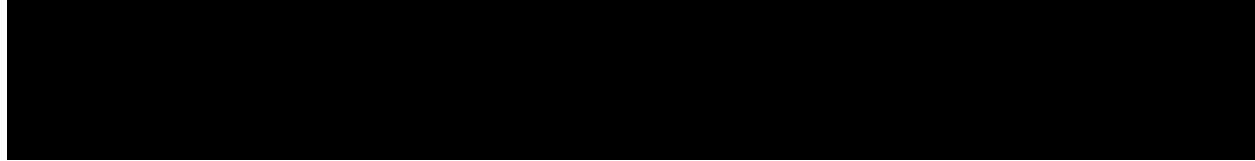
Apple is expected to file a brief in the Brooklyn case on Thursday.

*Sean Sposito and Carolyn Lochhead are San Francisco Chronicle staff writers. Email:*

*ssposito@sfgate.com clochhead@sfgate.com Twitter: @seansposito  
@carolynlochhead*

© 2016 Hearst Communications, Inc.

**H E A R S T**



ADVERTISEMENT

# **Exhibit H**



# iOS Security

iOS 9.0 or later

September 2015

# Contents

<b>Page 4</b>	<b>Introduction</b>
<b>Page 5</b>	<b>System Security</b> Secure boot chain System Software Authorization Secure Enclave Touch ID
<b>Page 10</b>	<b>Encryption and Data Protection</b> Hardware security features File Data Protection Passcodes Data Protection classes Keychain Data Protection Access to Safari saved passwords Keybags Security Certifications and programs
<b>Page 18</b>	<b>App Security</b> App code signing Runtime process security Extensions App Groups Data Protection in apps Accessories HomeKit HealthKit Apple Watch
<b>Page 27</b>	<b>Network Security</b> TLS VPN Wi-Fi Bluetooth Single Sign-on AirDrop security
<b>Page 31</b>	<b>Apple Pay</b> Apple Pay components How Apple Pay uses the Secure Element How Apple Pay uses the NFC controller Credit and debit card provisioning Payment authorization Transaction-specific dynamic security code Contactless payments with Apple Pay Paying with Apple Pay within apps Rewards cards Suspending, removing, and erasing cards

**Page 38 Internet Services**

- Apple ID
- iMessage
- FaceTime
- iCloud
- iCloud Keychain
- Siri
- Continuity
- Spotlight Suggestions

**Page 50 Device Controls**

- Passcode protection
- iOS pairing model
- Configuration enforcement
- Mobile device management (MDM)
- Device Enrollment Program
- Apple Configurator
- Device restrictions
- Supervised-only restrictions
- Remote wipe
- Find My iPhone and Activation Lock

**Page 56 Privacy Controls**

- Location Services
- Access to personal data
- Privacy policy

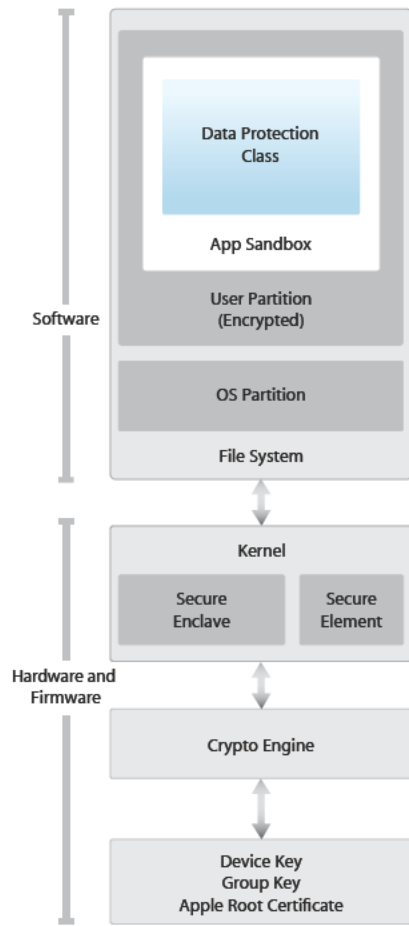
**Page 57 Conclusion**

- A commitment to security

**Page 58 Glossary**

**Page 60 Document Revision History**

# Introduction



Security architecture diagram of iOS provides a visual overview of the different technologies discussed in this document.

Apple designed the iOS platform with security at its core. When we set out to create the best possible mobile platform, we drew from decades of experience to build an entirely new architecture. We thought about the security hazards of the desktop environment, and established a new approach to security in the design of iOS. We developed and incorporated innovative features that tighten mobile security and protect the entire system by default. As a result, iOS is a major leap forward in security for mobile devices.

Every iOS device combines software, hardware, and services designed to work together for maximum security and a transparent user experience. iOS protects not only the device and its data at rest, but the entire ecosystem, including everything users do locally, on networks, and with key Internet services.

iOS and iOS devices provide advanced security features, and yet they're also easy to use. Many of these features are enabled by default, so IT departments don't need to perform extensive configurations. And key security features like device encryption are not configurable, so users can't disable them by mistake. Other features, such as Touch ID, enhance the user experience by making it simpler and more intuitive to secure the device.

This document provides details about how security technology and features are implemented within the iOS platform. It will also help organizations combine iOS platform security technology and features with their own policies and procedures to meet their specific security needs.

This document is organized into the following topic areas:

- **System security:** The integrated and secure software and hardware that are the platform for iPhone, iPad, and iPod touch.
- **Encryption and data protection:** The architecture and design that protects user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it.
- **App security:** The systems that enable apps to run securely and without compromising platform integrity.
- **Network security:** Industry-standard networking protocols that provide secure authentication and encryption of data in transmission.
- **Apple Pay:** Apple's implementation of secure payments.
- **Internet services:** Apple's network-based infrastructure for messaging, syncing, and backup.
- **Device controls:** Methods that prevent unauthorized use of the device and enable it to be remotely wiped if lost or stolen.
- **Privacy controls:** Capabilities of iOS that can be used to control access to Location Services and user data.



# System Security

## Entering Device Firmware Upgrade (DFU) mode

Restoring a device after it enters DFU mode returns it to a known good state with the certainty that only unmodified Apple-signed code is present. DFU mode can be entered manually: First connect the device to a computer using a USB cable, then hold down both the Home and Sleep/Wake buttons. After 8 seconds, release the Sleep/Wake button while continuing to hold down the Home button. Note: Nothing will be displayed on the screen when the device is in DFU mode. If the Apple logo appears, the Sleep/Wake button was held down too long.

System security is designed so that both software and hardware are secure across all core components of every iOS device. This includes the boot-up process, software updates, and Secure Enclave. This architecture is central to security in iOS, and never gets in the way of device usability.

The tight integration of hardware and software on iOS devices ensures that each component of the system is trusted, and validates the system as a whole. From initial boot-up to iOS software updates to third-party apps, each step is analyzed and vetted to help ensure that the hardware and software are performing optimally together and using resources properly.

## Secure boot chain

Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware.

When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code, known as the hardware root of trust, is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.

This secure boot chain helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices.

For devices with cellular access, the baseband subsystem also utilizes its own similar process of secure booting with signed software and keys verified by the baseband processor.

For devices with an A7 or later A-series processor, the Secure Enclave coprocessor also utilizes a secure boot process that ensures its separate software is verified and signed by Apple.

If one step of this boot process is unable to load or verify the next process, startup is stopped and the device displays the “Connect to iTunes” screen. This is called recovery mode. If the Boot ROM is not able to load or verify LLB, it enters DFU (Device Firmware Upgrade) mode. In both cases, the device must be connected to iTunes via USB and restored to factory default settings. For more information on manually entering recovery mode, see <https://support.apple.com/kb/HT1808>.

## System Software Authorization

Apple regularly releases software updates to address emerging security concerns and also provide new features; these updates are provided for all supported devices simultaneously. Users receive iOS update notifications on the device and through iTunes, and updates are delivered wirelessly, encouraging rapid adoption of the latest security fixes.

The startup process described above helps ensure that only Apple-signed code can be installed on a device. To prevent devices from being downgraded to older versions that lack the latest security updates, iOS uses a process called *System Software Authorization*. If downgrades were possible, an attacker who gains possession of a device could install an older version of iOS and exploit a vulnerability that's been fixed in the newer version.

On a device with an A7 or later A-series processor, the Secure Enclave coprocessor also utilizes System Software Authorization to ensure the integrity of its software and prevent downgrade installations. See "Secure Enclave," below.

iOS software updates can be installed using iTunes or over the air (OTA) on the device. With iTunes, a full copy of iOS is downloaded and installed. OTA software updates download only the components required to complete an update, improving network efficiency, rather than downloading the entire OS. Additionally, software updates can be cached on a local network server running the caching service on OS X Server so that iOS devices do not need to access Apple servers to obtain the necessary update data.

During an iOS upgrade, iTunes (or the device itself, in the case of OTA software updates) connects to the Apple installation authorization server and sends it a list of cryptographic measurements for each part of the installation bundle to be installed (for example, LLB, iBoot, the kernel, and OS image), a random anti-replay value (nonce), and the device's unique ID (ECID).

The authorization server checks the presented list of measurements against versions for which installation is permitted and, if it finds a match, adds the ECID to the measurement and signs the result. The server passes a complete set of signed data to the device as part of the upgrade process. Adding the ECID "personalizes" the authorization for the requesting device. By authorizing and signing only for known measurements, the server ensures that the update takes place exactly as provided by Apple.

The boot-time chain-of-trust evaluation verifies that the signature comes from Apple and that the measurement of the item loaded from disk, combined with the device's ECID, matches what was covered by the signature.

These steps ensure that the authorization is for a specific device and that an old iOS version from one device can't be copied to another. The nonce prevents an attacker from saving the server's response and using it to tamper with a device or otherwise alter the system software.

## Secure Enclave

The Secure Enclave is a coprocessor fabricated in the Apple A7 or later A-series processor. It utilizes its own secure boot and personalized software update separate from the application processor. It provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised.

The Secure Enclave uses encrypted memory and includes a hardware random number generator. Its microkernel is based on the L4 family, with modifications by Apple. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

Each Secure Enclave is provisioned during fabrication with its own UID (Unique ID) that is not accessible to other parts of the system and is not known to Apple. When the device starts up, an ephemeral key is created, entangled with its UID, and used to encrypt the Secure Enclave's portion of the device's memory space.

Additionally, data that is saved to the file system by the Secure Enclave is encrypted with a key entangled with the UID and an anti-replay counter.

The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure Enclave but cannot read it. It's encrypted and authenticated with a session key that is negotiated using the device's shared key that is provisioned for the Touch ID sensor and the Secure Enclave. The session key exchange uses AES key wrapping with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption.

## Touch ID

Touch ID is the fingerprint sensing system that makes secure access to the device faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use.

Touch ID makes using a longer, more complex passcode far more practical because users won't have to enter it as frequently. Touch ID also overcomes the inconvenience of a passcode-based lock, not by replacing it but by securely providing access to the device within thoughtful boundaries and time constraints.

### Touch ID and passcodes

To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances:

- The device has just been turned on or restarted.
- The device has not been unlocked for more than 48 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match a fingerprint.
- When setting up or enrolling new fingers with Touch ID.

When Touch ID is enabled, the device immediately locks when the Sleep/Wake button is pressed. With passcode-only security, many users set an unlocking grace period to avoid having to enter a passcode each time the device is used. With Touch ID, the device locks every time it goes to sleep, and requires a fingerprint—or optionally the passcode—at every wake.

Touch ID can be trained to recognize up to five different fingers. With one finger enrolled, the chance of a random match with someone else is 1 in 50,000. However, Touch ID allows only five unsuccessful fingerprint match attempts before the user is required to enter a passcode to obtain access.

### **Other uses for Touch ID**

Touch ID can also be configured to approve purchases from the iTunes Store, the App Store, and the iBooks Store, so users don't have to enter an Apple ID password. When they choose to authorize a purchase, authentication tokens are exchanged between the device and the store. The token and cryptographic nonce are held in the Secure Enclave. The nonce is signed with a Secure Enclave key shared by all devices and the iTunes Store.

Touch ID can also be used with Apple Pay, Apple's implementation of secure payments. For more information, see the Apple Pay section of this document.

Additionally, third-party apps can use system-provided APIs to ask the user to authenticate using Touch ID or a passcode. The app is only notified as to whether the authentication was successful; it cannot access Touch ID or the data associated with the enrolled fingerprint.

Keychain items can also be protected with Touch ID, to be released by the Secured Enclave only by a fingerprint match or the device passcode. App developers also have APIs to verify that a passcode has been set by the user and therefore able to authenticate or unlock keychain items using Touch ID.

With iOS 9, developers can require that Touch ID API operations don't fall back to an application password or the device passcode. Along with the ability to retrieve a representation of the state of enrolled fingers, this allows Touch ID to be used as a second factor in security sensitive apps.

### **Touch ID security**

The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave.

The raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes sub-dermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes.

### **How Touch ID unlocks an iOS device**

If Touch ID is turned off, when a device locks, the keys for Data Protection class Complete, which are held in the Secure Enclave, are discarded. The files and keychain items in that class are inaccessible until the user unlocks the device by entering his or her passcode.

With Touch ID turned on, the keys are not discarded when the device locks; instead, they're wrapped with a key that is given to the Touch ID subsystem inside the Secure Enclave. When a user attempts to unlock the device, if Touch ID recognizes the user's fingerprint, it provides the key for unwrapping the Data Protection keys, and the device is unlocked. This process provides additional protection by requiring the Data Protection and Touch ID subsystems to cooperate in order to unlock the device.

The keys needed for Touch ID to unlock the device are lost if the device reboots and are discarded by the Secure Enclave after 48 hours or five failed Touch ID recognition attempts.

# Encryption and Data Protection

The secure boot chain, code signing, and runtime process security all help to ensure that only trusted code and apps can run on a device. iOS has additional encryption and data protection features to safeguard user data, even in cases where other parts of the security infrastructure have been compromised (for example, on a device with unauthorized modifications). This provides important benefits for both users and IT administrators, protecting personal and corporate information at all times and providing methods for instant and complete remote wipe in the case of device theft or loss.

## Hardware security features

On mobile devices, speed and power efficiency are critical. Cryptographic operations are complex and can introduce performance or battery life problems if not designed and implemented with these priorities in mind.

Every iOS device has a dedicated AES 256 crypto engine built into the DMA path between the flash storage and main system memory, making file encryption highly efficient.

The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused (UID) or compiled (GID) into the application processor and Secure Enclave during manufacturing. No software or firmware can read them directly; they can see only the results of encryption or decryption operations performed by dedicated AES engines implemented in silicon using the UID or GID as a key. Additionally, the Secure Enclave's UID and GID can only be used by the AES engine dedicated to the Secure Enclave. The UIDs are unique to each device and are not recorded by Apple or any of its suppliers. The GIDs are common to all processors in a class of devices (for example, all devices using the Apple A8 processor), and are used for non security-critical tasks such as when delivering system software during installation and restore. Integrating these keys into the silicon helps prevent them from being tampered with or bypassed, or accessed outside the AES engine. The UIDs and GIDs are also not available via JTAG or other debugging interfaces.

The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if the memory chips are physically moved from one device to another, the files are inaccessible. The UID is not related to any other identifier on the device.

### Erase all content and settings

The "Erase all content and settings" option in Settings obliterates all the keys in Effaceable Storage, rendering all user data on the device cryptographically inaccessible. Therefore, it's an ideal way to be sure all personal information is removed from a device before giving it to somebody else or returning it for service. Important: Do not use the "Erase all content and settings" option until the device has been backed up, as there is no way to recover the erased data.

Apart from the UID and GID, all other cryptographic keys are created by the system's random number generator (RNG) using an algorithm based on CTR\_DRBG. System entropy is generated from timing variations during boot, and additionally from interrupt timing once the device has booted. Keys generated inside the Secure Enclave use its true hardware random number generator based on multiple ring oscillators post processed with CTR\_DRBG.

Securely erasing saved keys is just as important as generating them. It's especially challenging to do so on flash storage, where wear-leveling might mean multiple copies of data need to be erased. To address this issue, iOS devices include a feature dedicated to secure data erasure called Effaceable Storage. This feature accesses the underlying storage technology (for example, NAND) to directly address and erase a small number of blocks at a very low level.

## File Data Protection

In addition to the hardware encryption features built into iOS devices, Apple uses a technology called Data Protection to further protect data stored in flash memory on the device. Data Protection allows the device to respond to common events such as incoming phone calls, but also enables a high level of encryption for user data. Key system apps, such as Messages, Mail, Calendar, Contacts, Photos, and Health data values use Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically.

Data Protection is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into each iOS device. Data Protection is controlled on a per-file basis by assigning each file to a class; accessibility is determined by whether the class keys have been unlocked.

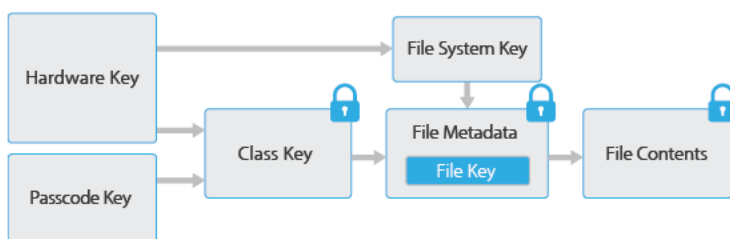
### Architecture overview

Every time a file on the data partition is created, Data Protection creates a new 256-bit key (the “per-file” key) and gives it to the hardware AES engine, which uses the key to encrypt the file as it is written to flash memory using AES CBC mode. (On devices with an A8 processor, AES-XTS is used.) The initialization vector (IV) is calculated with the block offset into the file, encrypted with the SHA-1 hash of the per-file key.

The per-file key is wrapped with one of several class keys, depending on the circumstances under which the file should be accessible. Like all other wrappings, this is performed using NIST AES key wrapping, per RFC 3394. The wrapped per-file key is stored in the file’s metadata.

When a file is opened, its metadata is decrypted with the file system key, revealing the wrapped per-file key and a notation on which class protects it. The per-file key is unwrapped with the class key, then supplied to the hardware AES engine, which decrypts the file as it is read from flash memory. All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the application processor. At boot, the Secure Enclave negotiates an ephemeral key with the AES engine. When the Secure Enclave unwraps a file’s keys, they are rewrapped with the ephemeral key and sent back to the application processor.

The metadata of all files in the file system is encrypted with a random key, which is created when iOS is first installed or when the device is wiped by a user. The file system key is stored in Efficable Storage. Since it’s stored on the device, this key is not used to maintain the confidentiality of data; instead, it’s designed to be quickly erased on demand (by the user, with the “Erase all content and settings” option, or by a user or administrator issuing a remote wipe command from a mobile device management (MDM) server, Exchange ActiveSync, or iCloud). Erasing the key in this manner renders all files cryptographically inaccessible.



The content of a file is encrypted with a per-file key, which is wrapped with a class key and stored in a file's metadata, which is in turn encrypted with the file system key. The class key is protected with the hardware UID and, for some classes, the user's passcode. This hierarchy provides both flexibility and performance. For example, changing a file's class only requires rewrapping its per-file key, and a change of passcode just rewraps the class key.

#### Passcode considerations

If a long password that contains only numbers is entered, a numeric keypad is displayed at the Lock screen instead of the full keyboard. A longer numeric passcode may be easier to enter than a shorter alphanumeric passcode, while providing similar security.

#### Delays between passcode attempts

Attempts	Delay Enforced
1-4	none
5	1 minute
6	5 minutes
7-8	15 minutes
9	1 hour

## Passcodes

By setting up a device passcode, the user automatically enables Data Protection. iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys. This means an attacker in possession of a device can't get access to data in specific protection classes without the passcode.

The passcode is entangled with the device's UID, so brute-force attempts must be performed on the device under attack. A large iteration count is used to make each attempt slower. The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.

The stronger the user passcode is, the stronger the encryption key becomes. Touch ID can be used to enhance this equation by enabling the user to establish a much stronger passcode than would otherwise be practical. This increases the effective amount of entropy protecting the encryption keys used for Data Protection, without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day.

To further discourage brute-force passcode attacks, there are escalating time delays after the entry of an invalid passcode at the Lock screen. If Settings > Touch ID & Passcode > Erase Data is turned on, the device will automatically wipe after 10 consecutive incorrect attempts to enter the passcode. This setting is also available as an administrative policy through mobile device management (MDM) and Exchange ActiveSync, and can be set to a lower threshold.

On devices with an A7 or later A-series processor, the delays are enforced by the Secure Enclave. If the device is restarted during a timed delay, the delay is still enforced, with the timer starting over for the current period.

## Data Protection classes

When a new file is created on an iOS device, it's assigned a class by the app that creates it. Each class uses different policies to determine when the data is accessible. The basic classes and policies are described in the following sections.

### Complete Protection

(`NSFileProtectionComplete`): The class key is protected with a key derived from the user passcode and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks the device using Touch ID.



**Protected Unless Open**

(`NSFileProtectionCompleteUnlessOpen`): Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background. This behavior is achieved by using asymmetric elliptic curve cryptography (ECDH over Curve25519). The usual per-file key is protected by a key derived using One-Pass Diffie-Hellman Key Agreement as described in NIST SP 800-56A.

The ephemeral public key for the agreement is stored alongside the wrapped per-file key. The KDF is Concatenation Key Derivation Function (Approved Alternative 1) as described in 5.8.1 of NIST SP 800-56A. `AlgorithmID` is omitted. `PartyUInfo` and `PartyVInfo` are the ephemeral and static public keys, respectively. SHA-256 is used as the hashing function. As soon as the file is closed, the per-file key is wiped from memory. To open the file again, the shared secret is re-created using the Protected Unless Open class's private key and the file's ephemeral public key; its hash is used to unwrap the per-file key, which is then used to decrypt the file.

**Protected Until First User Authentication**

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): This class behaves in the same way as Complete Protection, except that the decrypted class key is not removed from memory when the device is locked. The protection in this class has similar properties to desktop full-volume encryption, and protects data from attacks that involve a reboot. This is the default class for all third-party app data not otherwise assigned to a Data Protection class.

**No Protection**

(`NSFileProtectionNone`): This class key is protected only with the UID, and is kept in Effaceable Storage. Since all the keys needed to decrypt files in this class are stored on the device, the encryption only affords the benefit of fast remote wipe. If a file is not assigned a Data Protection class, it is still stored in encrypted form (as is all data on an iOS device).

## Keychain Data Protection

Many apps need to handle passwords and other short but sensitive bits of data, such as keys and login tokens. The iOS keychain provides a secure way to store these items.

The keychain is implemented as a SQLite database stored on the file system. There is only one database; the `securityd` daemon determines which keychain items each process or app can access. Keychain access APIs result in calls to the daemon, which queries the app's "keychain-access-groups," "application-identifier," and "application-group" entitlements. Rather than limiting access to a single process, access groups allow keychain items to be shared between apps.

Keychain items can only be shared between apps from the same developer. This is managed by requiring third-party apps to use access groups with a prefix allocated to them through the iOS Developer Program via application groups. The prefix requirement and application group uniqueness are enforced through code signing, Provisioning Profiles, and the iOS Developer Program.

### Components of a keychain item

Along with the access group, each keychain item contains administrative metadata (such as “created” and “last updated” timestamps).

It also contains SHA-1 hashes of the attributes used to query for the item (such as the account and server name) to allow lookup without decrypting each item. And finally, it contains the encryption data, which includes the following:

- Version number
- Access control list (ACL) data
- Value indicating which protection class the item is in
- Per-item key wrapped with the protection class key
- Dictionary of attributes describing the item (as passed to `SecItemAdd`), encoded as a binary plist and encrypted with the per-item key

The encryption is AES 128 in GCM (Galois/Counter Mode); the access group is included in the attributes and protected by the GMAC tag calculated during encryption.

Keychain data is protected using a class structure similar to the one used in file Data Protection. These classes have behaviors equivalent to file Data Protection classes, but use distinct keys and are part of APIs that are named differently.

Availability	File Data Protection	Keychain Data Protection
When unlocked	<code>NSFileProtectionComplete</code>	<code>kSecAttrAccessibleWhenUnlocked</code>
While locked	<code>NSFileProtectionCompleteUnlessOpen</code>	N/A
After first unlock	<code>NSFileProtectionCompleteUntilFirstUserAuthentication</code>	<code>kSecAttrAccessibleAfterFirstUnlock</code>
Always	<code>NSFileProtectionNone</code>	<code>kSecAttrAccessibleAlways</code>
Passcode enabled	N/A	<code>kSecAttrAccessible-WhenPasscodeSetThisDeviceOnly</code>

Apps that utilize background refresh services can use `kSecAttrAccessibleAfterFirstUnlock` for keychain items that need to be accessed during background updates.

The class `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` behaves the same as `kSecAttrAccessibleWhenUnlocked`, however it is only available when the device is configured with a passcode. This class exists only in the system keybag; they do not sync to iCloud Keychain, are not backed up, and are not included in escrow keybags. If the passcode is removed or reset, the items are rendered useless by discarding the class keys.

Other keychain classes have a “This device only” counterpart, which is always protected with the UID when being copied from the device during a backup, rendering it useless if restored to a different device.

Apple has carefully balanced security and usability by choosing keychain classes that depend on the type of information being secured and when it’s needed by iOS. For example, a VPN certificate must always be available so the device keeps a continuous connection, but it’s classified as “non-migratory,” so it can’t be moved to another device.

For keychain items created by iOS, the following class protections are enforced:

Item	Accessible
Wi-Fi passwords	After first unlock
Mail accounts	After first unlock
Exchange accounts	After first unlock
VPN passwords	After first unlock
LDAP, CalDAV, CardDAV	After first unlock
Social network account tokens	After first unlock
Handoff advertisement encryption keys	After first unlock
iCloud token	After first unlock
Home sharing password	When unlocked
Find My iPhone token	Always
Voicemail	Always
iTunes backup	When unlocked, non-migratory
Safari passwords	When unlocked
Safari bookmarks	When unlocked
VPN certificates	Always, non-migratory
Bluetooth® keys	Always, non-migratory
Apple Push Notification service token	Always, non-migratory

iCloud certificates and private key	Always, non-migratory
iMessage keys	Always, non-migratory
Certificates and private keys installed by Configuration Profile	Always, non-migratory
SIM PIN	Always, non-migratory

### Keychain access control

Keychains can use access control lists (ACLs) to set policies for accessibility and authentication requirements. Items can establish conditions that require user presence by specifying that they can't be accessed unless authenticated using Touch ID or by entering the device's passcode. ACLs are evaluated inside the Secure Enclave and are released to the kernel only if their specified constraints are met.

### Access to Safari saved passwords

iOS apps can interact with keychain items saved by Safari for password autofill using the following two APIs:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Access will be granted only if both the app developer and website administrator have given their approval, and the user has given consent. App developers express their intent to access Safari saved passwords by including an entitlement in their app. The entitlement lists the fully qualified domain names of associated websites. The websites must place a file on their server listing the unique app identifiers of apps they've approved. When an app with the `com.apple.developer.associated-domains` entitlement is installed, iOS makes a TLS request to each listed website, requesting the `file/apple-app-site-association`. If the file lists the app identifier of the app being installed, then iOS marks the website and app as having a trusted relationship. Only with a trusted relationship will calls to these two APIs result in a prompt to the user, who must agree before any passwords are released to the app, or are updated or deleted.

### Keybags

The keys for both file and keychain Data Protection classes are collected and managed in keybags. iOS uses the following four keybags: system, backup, escrow, and iCloud Backup.

**System keybag** is where the wrapped class keys used in normal operation of the device are stored. For example, when a passcode is entered, the `NSFileProtectionComplete` key is loaded from the system keybag and unwrapped. It is a binary plist stored in the No Protection class, but whose contents are encrypted with a key held in Effaceable Storage. In order to give forward security to keybags, this key is wiped and regenerated each time a user changes their passcode. The `AppleKeyStore` kernel extension manages the system keybag, and can be queried regarding a device's lock state. It reports that the device is unlocked only if all the class keys in the system keybag are accessible, and have been unwrapped successfully.

**Backup keybag** is created when an encrypted backup is made by iTunes and stored on the computer to which the device is backed up. A new keybag is created with a new set of keys, and the backed-up data is re-encrypted to these new keys. As explained earlier, non-migratory keychain items remain wrapped with the UID-derived key, allowing them to be restored to the device they were originally backed up from, but rendering them inaccessible on a different device.

The keybag is protected with the password set in iTunes, run through 10,000 iterations of PBKDF2. Despite this large iteration count, there's no tie to a specific device, and therefore a brute-force attack parallelized across many computers could theoretically be attempted on the backup keybag. This threat can be mitigated with a sufficiently strong password.

If a user chooses not to encrypt an iTunes backup, the backup files are not encrypted regardless of their Data Protection class, but the keychain remains protected with a UID-derived key. This is why keychain items migrate to a new device only if a backup password is set.

**Escrow keybag** is used for iTunes syncing and MDM. This keybag allows iTunes to back up and sync without requiring the user to enter a passcode, and it allows an MDM server to remotely clear a user's passcode. It is stored on the computer that's used to sync with iTunes, or on the MDM server that manages the device.

The escrow keybag improves the user experience during device synchronization, which potentially requires access to all classes of data. When a passcode-locked device is first connected to iTunes, the user is prompted to enter a passcode. The device then creates an escrow keybag containing the same class keys used on the device, protected by a newly generated key. The escrow keybag and the key protecting it are split between the device and the host or server, with the data stored on the device in the Protected Until First User Authentication class. This is why the device passcode must be entered before the user backs up with iTunes for the first time after a reboot.

In the case of an OTA software update, the user is prompted for his or her passcode when initiating the update. This is used to securely create a One-time Unlock Token, which unlocks the system keybag after the update. This token cannot be generated without entering the user's passcode, and any previously generated token is invalidated if the user's passcode changed.

One-time Unlock Tokens are either for attended or unattended installation of a software update. They are encrypted with a key derived from the current value of a monotonic counter in the Secure Enclave, the UUID of the keybag, and the Secure Enclave's UID.

Incrementing the One-time Unlock Token counter in the SEP invalidates any existing token. The counter is incremented when a token is used, after the first unlock of a restarted device, when a software update is canceled (by the user or by the system), or when the policy timer for a token has expired.

The One-time Unlock Token for attended software updates expires after 20 minutes. This token is exported from the Secure Enclave and is written to effaceable storage. A policy timer increments the counter if the device has not rebooted within 20 minutes.

For unattended software updates, which is set when the user chooses "Install Later" when notified of the update, the application processor can keep the One-time Unlock Token alive in the Secure Enclave for up to 8 hours. After that time, a policy timer increments the counter.

**iCloud Backup keybag** is similar to the backup keybag. All the class keys in this keybag are asymmetric (using Curve25519, like the Protected Unless Open Data Protection class), so iCloud backups can be performed in the background. For all Data Protection classes except No Protection, the encrypted data is read from the device and sent to iCloud. The corresponding class keys are protected by iCloud keys. The keychain class keys are wrapped with a UID-derived key in the same way as an unencrypted iTunes backup. An asymmetric keybag is also used for the backup in the keychain recovery aspect of iCloud Keychain.

## Security Certifications and programs

### **Cryptographic Validation (FIPS 140-2)**

The cryptographic modules in iOS have been validated for compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1 following each releases since iOS 6. The cryptographic modules in iOS 9 are identical to those in iOS 8, but as with each release, Apple submits the modules for re-validation. This program validates the integrity of cryptographic operations for Apple apps and third-party apps that properly utilize iOS cryptographic services.

### **Common Criteria Certification (ISO 15408)**

Apple has already begun pursuit of iOS certification under the Common Criteria Certification (CCC) program. The first two certifications currently active are against the Mobile Device Fundamental Protection Profile v2.0 (MDFPP2) and the VPN IPSecPP1.4 Client Protection Profile (VPNIPSecPP1.4). Apple has taken an active role within the International Technical Community (ITC) in developing currently unavailable Protection Profiles (PPs) focused on evaluating key mobile security technology. Apple continues to evaluate and pursue certifications against new and updated version of the PPs available today.

### **Commercial Solutions for Classified (CSfC)**

Where applicable, Apple has also submitted the iOS platform and various services for inclusion in the Commercial Solutions for Classified (CSfC) Program Components List. Specifically, iOS for Mobile Platform and the IKEv2 client for the IPSec VPN Client (IKEv2 Always-On VPN only). As Apple platforms and services undergo Common Criteria Certifications, they will be submitted for inclusion under CSfC Program Component List as well.

### **Security Configuration Guides**

Apple has collaborated with governments worldwide to develop guides that give instructions and recommendations for maintaining a more secure environment, also known as “device hardening.” These guides provide defined and vetted information about how to configure and utilize features in iOS for enhanced protection.

For information on iOS security certifications, validations, and guidance, see <https://support.apple.com/kb/HT202739>.

# App Security

Apps are among the most critical elements of a modern mobile security architecture. While apps provide amazing productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly.

Because of this, iOS provides layers of protection to ensure that apps are signed and verified, and are sandboxed to protect user data. These elements provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps on iOS without impacting system integrity. And users can access these apps on their iOS devices without undue fear of viruses, malware, or unauthorized attacks.

## App code signing

Once the iOS kernel has started, it controls which user processes and apps can be run. To ensure that all apps come from a known and approved source and have not been tampered with, iOS requires that all executable code be signed using an Apple-issued certificate. Apps provided with the device, like Mail and Safari, are signed by Apple. Third-party apps must also be validated and signed using an Apple-issued certificate. Mandatory code signing extends the concept of chain of trust from the OS to apps, and prevents third-party apps from loading unsigned code resources or using self-modifying code.

In order to develop and install apps on iOS devices, developers must register with Apple and join the iOS Developer Program. The real-world identity of each developer, whether an individual or a business, is verified by Apple before their certificate is issued. This certificate enables developers to sign apps and submit them to the App Store for distribution. As a result, all apps in the App Store have been submitted by an identifiable person or organization, serving as a deterrent to the creation of malicious apps. They have also been reviewed by Apple to ensure they operate as described and don't contain obvious bugs or other problems. In addition to the technology already discussed, this curation process gives customers confidence in the quality of the apps they buy.

iOS allows developers to embed frameworks inside of their apps, which can be used by the app itself or by extensions embedded within the app. To protect the system and other apps from loading third-party code inside of their address space, the system will perform a code signature validation of all the dynamic libraries that a process links against at launch time. This verification is accomplished through the team identifier (Team ID), which is extracted from an Apple-issued certificate. A team identifier is a 10-character alphanumeric string; for example, 1A2B3C4D5F. A program may link against any platform library that ships with the system or any library with the same team identifier in its code signature as the main executable. Since the executables shipping as part of the system don't have a team identifier, they can only link against libraries that ship with the system itself.

Businesses also have the ability to write in-house apps for use within their organization and distribute them to their employees. Businesses and organizations can apply to the Apple Developer Enterprise Program (ADEP) with a D-U-N-S number. Apple approves applicants after verifying their identity and eligibility. Once an organization becomes a member of ADEP, it can register to obtain a Provisioning Profile that permits in-house apps to run on devices it authorizes. Users must have the Provisioning Profile installed in order to run the in-house apps. This ensures that only the organization's intended users are able to load the apps onto their iOS devices. Apps installed via MDM are implicitly trusted because the relationship between the organization and the device is already established. Otherwise, users have to approve the app's Provisioning Profile in Settings. Organizations can restrict users from approving apps from unknown developers. On first launch of any enterprise app, the device must receive positive confirmation from Apple that the app is allowed to run.

Unlike other mobile platforms, iOS does not allow users to install potentially malicious unsigned apps from websites, or run untrusted code. At runtime, code signature checks of all executable memory pages are made as they are loaded to ensure that an app has not been modified since it was installed or last updated.

## Runtime process security

Once an app is verified to be from an approved source, iOS enforces security measures designed to prevent it from compromising other apps or the rest of the system.

All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using services explicitly provided by iOS.

System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted as read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.

Access by third-party apps to user information and features such as iCloud and extensibility is controlled using declared entitlements. Entitlements are key value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon.

In addition, apps can only perform background processing through system-provided APIs. This enables apps to continue to function without degrading performance or dramatically impacting battery life.

Address space layout randomization (ASLR) protects against the exploitation of memory corruption bugs. Built-in apps use ASLR to ensure that all memory regions are randomized upon launch. Randomly arranging the memory addresses of executable code, system libraries, and related programming constructs reduces the likelihood of many sophisticated exploits. For example, a return-to-libc attack attempts to trick a device into executing malicious code by manipulating memory addresses of the stack and system libraries. Randomizing the placement of these makes the attack far more difficult to execute, especially across multiple devices. Xcode, the iOS development environment, automatically compiles third-party programs with ASLR support turned on.

Further protection is provided by iOS using ARM's Execute Never (XN) feature, which marks memory pages as non-executable. Memory pages marked as both writable and executable can be used only by apps under tightly controlled conditions: The kernel checks for the presence of the Apple-only dynamic code-signing entitlement. Even then, only a single mmap call can be made to request an executable and writable page, which is given a randomized address. Safari uses this functionality for its JavaScript JIT compiler.

## Extensions

iOS allows apps to provide functionality to other apps by providing extensions. Extensions are special-purpose signed executable binaries, packaged within an app. The system automatically detects extensions at install time and makes them available to other apps using a matching system.

A system area that supports extensions is called an extension point. Each extension point provides APIs and enforces policies for that area. The system determines which extensions are available based on extension point-specific matching rules. The system automatically launches extension processes as needed and manages their lifetime. Entitlements can be used to restrict extension availability to particular system applications. For example, a Today view widget appears only in Notification Center, and a sharing extension is available only from the Sharing pane. The extension points are Today widgets, Share, Custom actions, Photo Editing, Document Provider, and Custom Keyboard.

Extensions run in their own address space. Communication between the extension and the app from which it was activated uses interprocess communications mediated by the system framework. They do not have access to each other's files or memory spaces. Extensions are designed to be isolated from each other, from their containing apps, and from the apps that use them. They are sandboxed like any other third-party app and have a container separate from the containing app's container. However, they share the same access to privacy controls as the container app. So if a user grants Contacts access to an app, this grant will be extended to the extensions that are embedded within the app, but not to the extensions activated by the app.

Custom keyboards are a special type of extensions since they are enabled by the user for the entire system. Once enabled, the extension will be used for any text field except the passcode input and any secure text view. For privacy reasons, custom keyboards run by default in a very restrictive sandbox that blocks access to the network, to services that perform network operations on behalf of a process, and to APIs that would allow the extension to exfiltrate typing data. Developers of custom keyboards can request that their extension have Open Access, which will let the system run the extension in the default sandbox after getting consent from the user.



For devices enrolled in mobile device management, document and keyboard extensions obey Managed Open In rules. For example, the MDM server can prevent a user from exporting a document from a managed app to an unmanaged Document Provider, or using an unmanaged keyboard with a managed app. Additionally, app developers can prevent the use of third-party keyboard extensions within their app.

## App Groups

Apps and extensions owned by a given developer account can share content when configured to be part of an App Group. It is up to the developer to create the appropriate groups on the Apple Developer Portal and include the desired set of apps and extensions. Once configured to be part of an App Group, apps have access to the following:

- A shared on-disk container for storage, which will stay on the device as long as at least one app from the group is installed
- Shared preferences
- Shared keychain items

The Apple Developer Portal guarantees that App Group IDs are unique across the app ecosystem.

## Data Protection in apps

The iOS Software Development Kit (SDK) offers a full suite of APIs that make it easy for third-party and in-house developers to adopt Data Protection and help ensure the highest level of protection in their apps. Data Protection is available for file and database APIs, including `NSFileManager`, `CoreData`, `NSData`, and `SQLite`.

The Mail app (including attachments), managed books, Safari bookmarks, app launch images, and location data are also stored encrypted with keys protected by the user's passcode on their device. Calendar (excluding attachments), Contacts, Reminders, Notes, Messages, and Photos implement Protected Until First User Authentication.

User-installed apps that do not opt-in to a specific Data Protection class receive Protected Until First User Authentication by default.

## Accessories

The Made for iPhone, iPod touch, and iPad (MFi) licensing program provides vetted accessory manufacturers access to the iPod Accessories Protocol (iAP) and the necessary supporting hardware components.

When an MFi accessory communicates with an iOS device using a Lightning connector or via Bluetooth, the device asks the accessory to prove it has been authorized by Apple by responding with an Apple-provided certificate, which is verified by the device. The device then sends a challenge, which the accessory must answer with a signed response. This process is entirely handled by a custom integrated circuit that Apple provides to approved accessory manufacturers and is transparent to the accessory itself.

Accessories can request access to different transport methods and functionality; for example, access to digital audio streams over the Lightning cable, or location information provided over Bluetooth. An authentication IC ensures that only approved devices are granted full access to the device. If an accessory does not provide authentication, its access is limited to analog audio and a small subset of serial (UART) audio playback controls.

AirPlay also utilizes the authentication IC to verify that receivers have been approved by Apple. AirPlay audio and CarPlay video streams utilize the MFi-SAP (Secure Association Protocol), which encrypts communication between the accessory and device using AES-128 in CTR mode. Ephemeral keys are exchanged using ECDH key exchange (Curve25519) and signed using the authentication IC's 1024-bit RSA key as part of the Station-to-Station (STS) protocol.

## HomeKit

HomeKit provides a home automation infrastructure that utilizes iCloud and iOS security to protect and synchronize private data without exposing it to Apple.

### HomeKit identity

HomeKit identity and security are based on Ed25519 public-private key pairs. An Ed25519 key pair is generated on the iOS device for each user for HomeKit, which becomes his or her HomeKit identity. It is used to authenticate communication between iOS devices, and between iOS devices and accessories.

The keys are stored in Keychain and are included only in encrypted Keychain backups. The keys are synchronized between devices using iCloud Keychain.

### Communication with HomeKit accessories

HomeKit accessories generate their own Ed25519 key pair for use in communicating with iOS devices. If the accessory is restored to factory settings, a new key pair is generated.

To establish a relationship between an iOS device and a HomeKit accessory, keys are exchanged using Secure Remote Password (3072-bit) protocol, utilizing an 8-digit code provided by the accessory's manufacturer and entered on the iOS device by the user, and then encrypted using ChaCha20-Poly1305 AEAD with HKDF-SHA-512-derived keys. The accessory's MFi certification is also verified during setup.

When the iOS device and the HomeKit accessory communicate during use, each authenticates the other utilizing the keys exchanged in the above process. Each session is established using the Station-to-Station protocol and is encrypted with HKDF-SHA-512 derived keys based on per-session Curve25519 keys. This applies to both IP-based and Bluetooth Low Energy accessories.

### Local data storage

HomeKit stores data about the homes, accessories, scenes, and users on a user's iOS device. This stored data is encrypted using keys derived from the user's HomeKit identity keys, plus a random nonce. Additionally, HomeKit data is stored using Data Protection class Protected Until First User Authentication. HomeKit data is only backed up in encrypted backups, so, for example, unencrypted iTunes backups do not contain HomeKit data.

### Data synchronization between devices and users

HomeKit data can be synchronized between a user's iOS devices using iCloud and iCloud Keychain. The HomeKit data is encrypted during the synchronization using keys derived from the user's HomeKit identity and random nonce. This data is handled as an opaque blob during synchronization. The most recent blob is stored in iCloud to enable synchronization, but it is not used for any other purposes. Because it is encrypted using keys that are available only on the user's iOS devices, its contents are inaccessible during transmission and iCloud storage.

HomeKit data is also synchronized between multiple users of the same home. This process uses authentication and encryption that is the same as that used between an iOS device and a HomeKit accessory. The authentication is based on Ed25519 public keys that are exchanged between the devices when a user is added to a home. After a new user is added to a home, every further communication is authenticated and encrypted using Station-to-Station protocol and per-session keys.

Only the user who initially created the home in HomeKit can add new users. His or her device configures the accessories with the public key of the new user so that the accessory can authenticate and accept commands from the new user. The process for configuring Apple TV for use with HomeKit uses the same authentication and encryption as when adding additional users, but is performed automatically if the user who created the home is signed in to iCloud on the Apple TV, and the Apple TV is in the home.

If a user does not have multiple devices, and does not grant additional users access to his or her home, no HomeKit data is synchronized to iCloud.

### **Home data and apps**

Access to home data by apps is controlled by the user's Privacy settings. Users are asked to grant access when apps request home data, similar to Contacts, Photos, and other iOS data sources. If the user approves, apps have access to the names of rooms, names of accessories, and which room each accessory is in, and other information as detailed in the HomeKit developer documentation.

### **Siri**

Siri can be used to query and control accessories, and to activate scenes. Minimal information about the configuration of the home is provided anonymously to Siri, as described in the Siri section of this paper, to provide names of rooms, accessories, and scenes that are necessary for command recognition.

### **iCloud remote access for HomeKit accessories**

HomeKit accessories can connect directly with iCloud to enable iOS devices to control the accessory when Bluetooth or Wi-Fi communication isn't available.

iCloud Remote access has been carefully designed so that accessories can be controlled and send notifications without revealing to Apple what the accessories are, or what commands and notifications are being sent. HomeKit does not send information about the home over iCloud Remote access.

When a user sends a command using iCloud remote access, the accessory and iOS device are mutually authenticated and data is encrypted using the same procedure described for local connections. The contents of the communications are encrypted and not visible to Apple. The addressing through iCloud is based on the iCloud identifiers registered during the setup process.

Accessories that support iCloud remote access are provisioned during the accessory's setup process. The provisioning process begins with the user signing in to iCloud. Next, the iOS device asks the accessory to sign a challenge using the Apple Authentication Coprocessor that is built into all Built for HomeKit accessories. The accessory also generates prime256v1 elliptic curve keys, and the public key is sent to the iOS device along with the signed challenge and the X.509 certificate of the authentication coprocessor. These are used to request a certificate for the accessory from the iCloud provisioning server. The certificate is stored by the accessory, but it does not contain any identifying information about the accessory, other than it has been granted access to HomeKit iCloud remote access. The iOS device that is conducting the provisioning also sends a bag to the accessory, which contains the URLs and other information needed to connect to the iCloud remote access server. This information is not specific to any user or accessory.

Each accessory registers a list of allowed users with the iCloud remote access server. These users have been granted the ability to control the accessory by the person who added the accessory to the home. Users are granted an identifier by the iCloud server and can be mapped to an iCloud account for the purpose of delivering notification messages and responses from the accessories. Similarly, accessories have iCloud-issued identifiers, but these identifiers are opaque and don't reveal any information about the accessory itself.

When an accessory connects to the HomeKit iCloud remote access server, it presents its certificate and a pass. The pass is obtained from a different iCloud server and it is not unique for each accessory. When an accessory requests a pass, it includes its manufacturer, model, and firmware version in its request. No user-identifying or home-identifying information is sent in this request. The connection to the pass server is not authenticated, in order to help protect privacy.

Accessories connect to the iCloud remote access server using HTTP/2, secured using TLS 1.2 with AES-128-GCM and SHA-256. The accessory keeps its connection to the iCloud remote access server open so that it can receive incoming messages and send responses and outgoing notifications to iOS devices.

## HealthKit

The HealthKit framework provides a common database that apps can use to store and access fitness and health data with permission of the user. HealthKit also works directly with health and fitness devices, such as compatible Bluetooth LE heart rate monitors and the motion coprocessor built into many iOS devices.

### Health data

HealthKit uses a database to store the user's health data, such as height, weight, distance walked, blood pressure, and so on. This database is stored in Data Protection class Complete Protection, which means it is accessible only after a user enters his or her passcode or uses Touch ID to unlock the device.

Another database stores operational data, such as access tables for apps, names of devices connected to HealthKit, and scheduling information used to launch apps when new data is available. This database is stored in Data Protection class Protected Until First User Authentication.

Temporary journal files store health records that are generated when the device is locked, such as when the user is exercising. These are stored in Data Protection class Protected Unless Open. When the device is unlocked, they are imported into the primary health databases, then deleted when the merge is completed.

Health data is not shared via iCloud or synced between devices. Health databases are included in encrypted device backups to iCloud or iTunes. Health data is not included in unencrypted iTunes backups.

### **Data Integrity**

Data stored in the database includes metadata to track the provenance of each data record. This metadata includes an application identifier that identifies which app stored the record. Additionally, an optional metadata item can contain a digitally signed copy of the record. This is intended to provide data integrity for records generated by a trusted device. The format used for the digital signature is the Cryptographic Message Syntax (CMS) specified in IETF RFC 5652.

### **Access by third-party apps**

Access to the HealthKit API is controlled with entitlements, and apps must conform to restrictions about how the data is used. For example, apps are not allowed to utilize health data for advertising. Apps are also required to provide users with a privacy policy that details its use of health data.

Access to health data by apps is controlled by the user's Privacy settings. Users are asked to grant access when apps request access to health data, similar to Contacts, Photos, and other iOS data sources. However, with health data, apps are granted separate access for reading and writing data, as well as separate access for each type of health data. Users can view, and revoke, permissions they've granted for accessing health data in the Sources tab of the Health app.

If granted permission to write data, apps can also read the data they write. If granted the permission to read data, they can read data written by all sources. However, apps can't determine access granted to other apps. In addition, apps can't conclusively tell if they have been granted read access to health data. When an app does not have read access, all queries return no data—the same response as an empty database would return. This prevents apps from inferring the user's health status by learning which types of data the user is tracking.

### **Medical ID**

The Health app gives users the option of filling out a Medical ID form with information that could be important during a medical emergency. The information is entered or updated manually and is not synchronized with the information in the health databases.

The Medical ID information is viewed by tapping the Emergency button on the Lock screen. The information is stored on the device using Data Protection class No Protection so that it is accessible without having to enter the device passcode. Medical ID is an optional feature that enables users to decide how to balance both safety and privacy concerns.

## **Apple Watch**

Apple Watch uses the security features and technology built for iOS to help protect data on the device, as well as communications with its paired iPhone and the Internet. This includes technologies such as Data Protection and keychain access control. The user's passcode is also entangled with the device UID to create encryption keys.

Pairing Apple Watch with iPhone is secured using an out-of-band (OOB) process to exchange public keys, followed by the BTLE link shared secret. Apple Watch displays an animated pattern, which is captured by the camera on iPhone. The pattern contains an encoded secret that is used for BTLE 4.1 out-of-band pairing. Standard BTLE Passkey Entry is used as a fallback pairing method, if necessary.

Once the BTLE session is established, Apple Watch and iPhone exchange keys using a process adapted from IDS, as described in the iMessage section of this paper. Once keys have been exchanged, the Bluetooth session key is discarded, and all communications

between Apple Watch and iPhone are encrypted using IDS, with the encrypted BTLE and Wi-Fi links providing a secondary encryption layer. Key rolling is utilized at 15-minute intervals to limit the exposure window, should traffic be compromised.

To support apps that need streaming data, encryption is provided using methods described in the FaceTime section of this paper, utilizing the IDS service provided by the paired iPhone.

Apple Watch implements hardware-encrypted storage and class-based protection of files and keychain items, as described in the Data Protection section of this paper. Access-controlled keybags for keychain items are also used. Keys used for communication between the watch and iPhone are also secured using class-based protection.

When Apple Watch is not within Bluetooth range, Wi-Fi can be used instead. Apple Watch will not join Wi-Fi networks unless the credentials to do so are present on the paired iPhone, which provides the list of known networks to the watch automatically.

Apple Watch can be manually locked by holding down the side button. Additionally, motion heuristics are used to attempt to automatically lock the device shortly after it's removed from the wrist. When locked, Apple Pay can't be used. If the automatic locking provided by wrist detection is turned off in settings, Apple Pay is disabled. Wrist detection is turned off using the Apple Watch app on iPhone. This setting can also be enforced using mobile device management.

The paired iPhone can also unlock the watch, provided the watch is being worn. This is accomplished by establishing a connection authenticated by the keys established during pairing. iPhone sends the key, which the watch uses to unlock its Data Protection keys. The watch passcode is not known to iPhone nor is it transmitted. This feature can be turned off using the Apple Watch app on iPhone.

Apple Watch can be paired with only one iPhone at a time. Pairing with a new iPhone automatically erases all content and data from Apple Watch.

Enabling Find My Phone on the paired iPhone also enables Activation Lock on Apple Watch. Activation Lock makes it harder for anyone to use or sell an Apple Watch that has been lost or stolen. Activation Lock requires the user's Apple ID and password to unpair, erase, or reactivate an Apple Watch.

# Network Security

In addition to the built-in safeguards Apple uses to protect data stored on iOS devices, there are many network security measures that organizations can take to keep information secure as it travels to and from an iOS device.

Mobile users must be able to access corporate networks from anywhere in the world, so it's important to ensure that they are authorized and their data is protected during transmission. iOS uses—and provides developer access to—standard networking protocols for authenticated, authorized, and encrypted communications. To accomplish these security objectives, iOS integrates proven technologies and the latest standards for both Wi-Fi and cellular data network connections.

On other platforms, firewall software is needed to protect open communication ports against intrusion. Because iOS achieves a reduced attack surface by limiting listening ports and removing unnecessary network utilities such as telnet, shells, or a web server, no additional firewall software is needed on iOS devices.

## TLS

iOS supports Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) and DTLS. Safari, Calendar, Mail, and other Internet apps automatically use these mechanisms to enable an encrypted communication channel between the device and network services. High-level APIs (such as CFNetwork) make it easy for developers to adopt TLS in their apps, while low-level APIs (SecureTransport) provide fine-grained control. By default, CFNetwork disallows SSLv3, and apps that use WebKit (such as Safari) are prohibited from making an SSLv3 connection.

### App Transport Security

App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using `NSURLConnection`, `CFURL`, or `NSURLSession` APIs.

Servers must support a minimum of TLS 1.2, forward secrecy, and certificates must be valid and signed using SHA-256 or better with a minimum of a 2048-bit RSA key or 256-bit elliptic curve key.

Network connections that don't meet these requirements will fail, unless the app overrides App Transport Security. Invalid certificates always result in a hard failure and no connection. App Transport Security is automatically applied to apps that are compiled for iOS 9.

## VPN

Secure network services like virtual private networking typically require minimal setup and configuration to work with iOS devices. iOS devices work with VPN servers that support the following protocols and authentication methods:

- IKEv2/IPSec with authentication by shared secret, RSA Certificates, ECDSA Certificates, EAP-MSCHAPv2, or EAP-TLS.
- Pulse Secure, Cisco, Aruba Networks, SonicWALL, Check Point, Palo Alto Networks, Open VPN, AirWatch, MobileIron, NetMotion Wireless, and F5 Networks SSL-VPN using the appropriate client app from the App Store.
- Cisco IPSec with user authentication by Password, RSA SecurID or CRYPTOCARD, and machine authentication by shared secret and certificates.
- L2TP/IPSec with user authentication by MS-CHAPV2 Password, RSA SecurID or CRYPTOCARD, and machine authentication by shared secret.
- PPTP with user authentication by MS-CHAPV2 Password and RSA SecurID or CRYPTOCARD is supported, but not recommended.

iOS supports VPN On Demand for networks that use certificate-based authentication. IT policies specify which domains require a VPN connection by using a configuration profile.

iOS also supports Per App VPN support, facilitating VPN connections on a much more granular basis. Mobile device management (MDM) can specify a connection for each managed app and/or specific domains in Safari. This helps ensure that secure data always goes to and from the corporate network—and that a user's personal data does not.

iOS supports Always-on VPN, which can be configured for devices managed via MDM and supervised using Apple Configurator or the Device Enrollment Program. This eliminates the need for users to turn on VPN to enable protection when connecting to cellular and Wi-Fi networks. Always-on VPN gives an organization full control over device traffic by tunneling all IP traffic back to the organization. The default tunneling protocol, IKEv2, secures traffic transmission with data encryption. The organization can now monitor and filter traffic to and from its devices, secure data within its network, and restrict device access to the Internet.

## Wi-Fi

iOS supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses 128-bit AES encryption, giving users the highest level of assurance that their data remains protected when sending and receiving communications over a Wi-Fi network connection. With support for 802.1X, iOS devices can be integrated into a broad range of RADIUS authentication environments. 802.1X wireless authentication methods supported on iPhone and iPad include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP.

iOS uses a randomized Media Access Control (MAC) address when conducting Preferred Network Offload (PNO) scans when a device is not associated with a Wi-Fi network and its processor is asleep. A device's processor goes to sleep shortly after the screen is turned off. PNO scans are run to determine if a user can connect to a preferred Wi-Fi network to conduct activity such as wirelessly syncing with iTunes.

iOS also uses a randomized MAC address when conducting enhanced Preferred Network Offload (ePNO) scans when a device is not associated with a Wi-Fi network or its processor is asleep. ePNO scans are run when a device uses Location Services for apps which use geofences, such as location-based reminders that determine whether the device is near a specific location.



Because a device's MAC address now changes when it's not connected to a Wi-Fi network, it can't be used to persistently track a device by passive observers of Wi-Fi traffic, even when the device is connected to a cellular network.

We've worked with Wi-Fi manufacturers to let them know that background scans use a randomized MAC address, and that neither Apple nor manufacturers can predict these randomized MAC addresses.

Wi-Fi MAC address randomization is not supported on iPhone 4s.

## Bluetooth

Bluetooth support in iOS has been designed to provide useful functionality without unnecessary increased access to private data. iOS devices support Encryption Mode 3, Security Mode 4, and Service Level 1 connections. iOS supports the following Bluetooth profiles:

- Hands-Free Profile (HFP 1.5)
- Phone Book Access Profile (PBAP)
- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Personal Area Network Profile (PAN)
- Human Interface Device Profile (HID)

Support for these profiles varies by device. For more information, see <https://support.apple.com/kb/ht3647>.

## Single Sign-on

iOS supports authentication to enterprise networks through Single Sign-on (SSO). SSO works with Kerberos-based networks to authenticate users to services they are authorized to access. SSO can be used for a range of network activities, from secure Safari sessions to third-party apps.

iOS SSO utilizes SPNEGO tokens and the HTTP Negotiate protocol to work with Kerberos-based authentication gateways and Windows Integrated Authentication systems that support Kerberos tickets. Certificate-based authentication is also supported. SSO support is based on the open source Heimdal project.

The following encryption types are supported:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari supports SSO, and third-party apps that use standard iOS networking APIs can also be configured to use it. To configure SSO, iOS supports a configuration profile payload that allows MDM servers to push down the necessary settings. This includes setting the user principal name (that is, the Active Directory user account) and Kerberos realm settings, as well as configuring which apps and/or Safari web URLs should be allowed to use SSO.

## AirDrop security

iOS devices that support AirDrop use Bluetooth Low Energy (BLE) and Apple-created peer-to-peer Wi-Fi technology to send files and information to nearby devices, including AirDrop-capable Mac computers running OS X Yosemite or later. The Wi-Fi radio is used to communicate directly between devices without using any Internet connection or Wi-Fi Access Point.

When a user enables AirDrop, a 2048-bit RSA identity is stored on the device. Additionally, an AirDrop identity hash is created based on the email addresses and phone numbers associated with the user's Apple ID.

When a user chooses AirDrop as the method for sharing an item, the device emits an AirDrop signal over Bluetooth Low Energy. Other devices that are awake, in close proximity, and have AirDrop turned on detect the signal and respond with a shortened version of their owner's identity hash.

AirDrop is set to share with Contacts Only by default. Users can also choose if they want to be able to use AirDrop to share with Everyone or turn off the feature entirely. In Contacts Only mode, the received identity hashes are compared with hashes of people in the initiator's Contacts app. If a match is found, the sending device creates a peer-to-peer Wi-Fi network and advertises an AirDrop connection using Bonjour. Using this connection, the receiving devices send their full identity hashes to the initiator. If the full hash still matches Contacts, the recipient's first name and photo (if present in Contacts) are displayed in the AirDrop sharing sheet.

When using AirDrop, the sending user selects who they want to share with. The sending device initiates an encrypted (TLS) connection with the receiving device, which exchanges their iCloud identity certificates. The identity in the certificates is verified against each user's Contacts app. Then the receiving user is asked to accept the incoming transfer from the identified person or device. If multiple recipients have been selected, this process is repeated for each destination.

In the Everyone mode, the same process is used but if a match in Contacts is not found, the receiving devices are shown in the AirDrop sending sheet with a silhouette and with the device's name, as defined in Settings > General > About > Name.

Organizations can restrict the use of AirDrop for devices or apps being managed by a mobile device management solution.

# Apple Pay

With Apple Pay, users can use supported iOS devices and Apple Watch to pay in an easy, secure, and private way. It's simple for users, and it's built with integrated security in both hardware and software.

Apple Pay is also designed to protect the user's personal information. Apple Pay doesn't collect any transaction information that can be tied back to the user. Payment transactions are between the user, the merchant, and the card issuer.

## Apple Pay components

**Secure Element:** The Secure Element is an industry-standard, certified chip running the Java Card platform, which is compliant with financial industry requirements for electronic payments.

**NFC controller:** The NFC controller handles Near Field Communication protocols and routes communication between the application processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.

**Wallet:** Wallet is used to add and manage credit, debit, rewards, and store cards and to make payments with Apple Pay. Users can view their cards and additional information about their card issuer, their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in Setup Assistant and Settings.

**Secure Enclave:** On iPhone and iPad, the Secure Enclave manages the authentication process and enables a payment transaction to proceed. It stores fingerprint data for Touch ID.

On Apple Watch, the device must be unlocked, and the user must double-click the side button. The double-click is detected and passed to the Secure Element directly without going through the application processor.

**Apple Pay Servers:** The Apple Pay Servers manage the state of credit and debit cards in Wallet and the Device Account Numbers stored in the Secure Element. They communicate both with the device and with the payment network servers. The Apple Pay Servers are also responsible for re-encrypting payment credentials for payments within apps.

## How Apple Pay uses the Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. Credit or debit card data is sent from the payment network or card issuer encrypted to these payment applets using keys that are known only to the payment network and the payment applets' security domain. This data is stored within these payment applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus.

## How Apple Pay uses the NFC controller

As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.

Once payment is authorized by the card holder using Touch ID or passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless transactions are contained to the local NFC field and are never exposed to the application processor. In contrast, payment authorization details for payments within apps are routed to the application processor, but only after encryption by the Secure Element to the Apple Pay Server.

## Credit and debit card provisioning

When a user adds a credit or debit card (including store cards) to Apple Pay, Apple securely sends the card information, along with other information about user's account and device, to the card issuer. Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Apple Pay. These client-server sessions are encrypted using SSL.

Full card numbers are not stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and WatchOS, is never stored on Apple Pay Servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone. Provisioning a card for Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

There are two ways to provision a credit or debit card into Apple Pay:

- Adding a credit or debit card manually to Apple Pay
- Adding credit or debit cards on file from an iTunes Store account to Apple Pay

### **Adding a credit or debit card manually to Apple Pay**

To add a card manually, including store cards, the name, credit card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the iSight camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. Once all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted, as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card will be able to make payments with Apple Pay.

#### **Adding credit or debit cards from an iTunes Store account to Apple Pay**

For a credit or debit card on file with iTunes, the user may be required to re-enter their Apple ID password. The card number is retrieved from iTunes and the Check Card process is initiated. If the card is eligible for Apple Pay, the device will download and display terms and conditions, then send along the term's ID and the card security code to the Link and Provision process. Additional verification may occur for iTunes account cards on file.

#### **Adding credit or debit cards from a card issuer's app**

When the app is registered for use with Apple Pay, keys are established for the app and the merchant's server. These keys are used to encrypt the card information that's sent to the merchant, which prevents the information from being read by the iOS device. The provisioning flow is similar to that used for manually added cards, described above, except that one-time passwords are used in lieu of the CVV.

#### **Additional verification**

A card issuer can decide whether a credit or debit card requires additional verification. Depending on what is offered by the card issuer, the user may be able to choose between different options for additional verification, such as a text message, email, customer service call, or a method in an approved third-party app to complete the verification. For text messages or email, the user selects from contact information the issuer has on file. A code will be sent, which the user will need to enter into Wallet, Settings, or the Apple Watch app. For customer service or verification using an app, the issuer performs their own communication process.

## Payment authorization

The Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave, confirming the user has authenticated with Touch ID or the device passcode. Touch ID is the default method if available but the passcode can be used at any time instead of Touch ID. A passcode is automatically offered after three unsuccessful attempts to match a fingerprint and after five unsuccessful attempts, the passcode is required. A passcode is also required when Touch ID is not configured or not enabled for Apple Pay.

Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the NFC controller, which in turn is connected to the application processor. Even though not directly connected, the Secure Enclave and Secure Element can communicate securely using a shared pairing key that is provisioned during the manufacturing process. The encryption and authentication of the communication is based on AES, with cryptographic nonces used by both sides to protect against replay attacks. The pairing key is generated inside the Secure Enclave from its UID key and the Secure Element's unique identifier. The pairing key is then securely transferred from the Secure Enclave to a hardware security module (HSM) in the factory, which has the key material required to then inject the pairing key into the Secure Element.

When the user authorizes a transaction, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction (contactless or within apps) to the Secure Element, tied to an Authorization Random (AR) value. The AR is generated in the Secure Enclave when a user first provisions a credit card and is persisted while Apple Pay is enabled, protected by the Secure Enclave's encryption and anti-rollback mechanism. It is securely delivered to the Secure Element via the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as deleted.

Credit and debit cards added to the Secure Element can only be used if the Secure Element is presented with authorization using the same pairing key and AR value from when the card was added. This allows iOS to instruct the Secure Enclave to render cards unusable by marking its copy of the AR as invalid under the following scenarios:

When the passcode is disabled.

- The user logs out of iCloud.
- The user selects Erase All Content and Settings.
- The device is restored from recovery mode.

With Apple Watch, cards are marked as invalid when:

- The watch's passcode is disabled.
- The watch is unpaired from iPhone.
- Wrist detection is turned off.

Using the pairing key and its copy of the current AR value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment. This process also applies when retrieving encrypted payment data from a payment applet for transactions within apps.

## Transaction-specific dynamic security code

All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:

- A random number generated by the payment applet
- Another random number generated by the terminal—in the case of an NFC transaction or
- Another random number generated by the server—in the case of transactions within apps

These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

## Contactless payments with Apple Pay

If iPhone is on and detects an NFC field, it will present the user with the relevant credit or debit card, or the default card, which is managed in Settings. The user can also go to the Wallet app and choose a credit or debit card, or when the device is locked, double-click the Home button.

Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. When Apple Watch is unlocked, double-clicking the side button activates the default card for payment. No payment information is sent without user authentication.

Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment. Neither Apple nor a user's device sends the full actual credit or debit card numbers to merchants. Apple may receive anonymous transaction information such as the approximate time and location of the transaction, which helps improve Apple Pay and other Apple products and services.

## Paying with Apple Pay within apps

Apple Pay can also be used to make payments within iOS apps. When users pay in apps using Apple Pay, Apple receives encrypted transaction information and re-encrypts it with a merchant-specific key before it's sent to the merchant. Apple Pay retains anonymous transaction information such as approximate purchase amount. This information can't be tied back to the user and never includes what the user is buying.

When an app initiates an Apple Pay payment transaction, the Apple Pay Servers receive the encrypted transaction from the device prior to the merchant receiving it. The Apple Pay Servers then re-encrypt it with a merchant-specific key before relaying the transaction to the merchant.

When an app requests a payment, it calls an API to determine if the device supports Apple Pay and if the user has credit or debit cards that can make payments on a payment network accepted by the merchant. The app requests any pieces of information it needs to process and fulfill the transaction, such as the billing and shipping address, and contact information. The app then asks iOS to present the Apple Pay sheet, which requests information for the app, as well as other necessary information, such as the card to use.

At this time, the app is presented with city, state, and zip code information to calculate the final shipping cost. The full set of requested information isn't provided to the app until the user authorizes the payment with Touch ID or the device passcode. Once the payment is authorized, the information presented in the Apple Pay sheet will be transferred to the merchant.

When the user authorizes the payment, a call is made to the Apple Pay Servers to obtain a cryptographic nonce, which is similar to the value returned by the NFC terminal used for in-store transactions. The nonce, along with other transaction data, is passed to the Secure Element to generate a payment credential that will be encrypted with an Apple key. When the encrypted payment credential comes out of the Secure Element, it's passed to the Apple Pay Servers, which decrypt the credential, verify the nonce in the credential against the nonce sent by the Secure Element, and re-encrypt the payment credential with the merchant key associated with the Merchant ID. It's then returned to the device, which hands it back to the app via the API. The app then passes it along to the merchant system for processing. The merchant can then decrypt the payment credential with its private key for processing. This, together with the signature from Apple's servers, allows the merchant to verify that the transaction was intended for this particular merchant.

The APIs require an entitlement that specifies the supported merchant IDs. An app can also include additional data to send to the Secure Element to be signed, such as an order number or customer identity, ensuring the transaction can't be diverted to a different customer. This is accomplished by the app developer. The app developer is able to specify `applicationData` on the `PKPaymentRequest`. A hash of this data is included in the encrypted payment data. The merchant is then responsible for verifying that their `applicationData` hash matches what's included in the payment data.

## Rewards cards

As of iOS 9, Apple Pay supports the Value Added Service (VAS) protocol for transmitting merchant rewards cards to compatible NFC terminals. The VAS protocol can be implemented on merchant terminals and uses NFC to communicate with supported Apple devices. The VAS protocol works over a short distance and is used to provide complementary services, such as transmission of rewards card information, as part of an Apple Pay transaction.

The NFC terminal initiates receiving the card information by sending a request for a card. If the user has a card with the store's identifier, the user is asked to authorize its use. If the merchant supports encryption, the card information, a timestamp, and a single-use random ECDH P-256 key is used with the merchant's public key to derive an encryption key for the card data, which is sent to the terminal. If the merchant does not support encryption, the user is asked to re-present the device to the terminal before the rewards card information is sent.



## Suspending, removing, and erasing cards

Users can suspend Apple Pay on iPhone and iPad by placing their devices in Lost Mode using Find My iPhone. Users also have the ability to remove and erase their cards from Apple Pay using Find My iPhone, iCloud Settings, or directly on their devices using Wallet. On Apple Watch, cards can be removed using iCloud settings, the Apple Watch app on iPhone, or directly on the watch. The ability to make payments using cards on the device will be suspended or removed from Apple Pay by the card issuer or respective payment network even if the device is offline and not connected to a cellular or Wi-Fi network. Users can also call their card issuer to suspend or remove cards from Apple Pay.

Additionally, when a user erases the entire device using “Erase All Content and Settings,” using Find My iPhone, or restoring their device using recovery mode, iOS will instruct the Secure Element to mark all cards as deleted. This has the effect of immediately changing the cards to an unusable state until the Apple Pay Servers can be contacted to fully erase the cards from the Secure Element. Independently, the Secure Enclave marks the AR as invalid, so that further payment authorizations for previously enrolled cards aren’t possible. When the device is online, it attempts to contact the Apple Pay Servers to ensure all cards in the Secure Element are erased.

## Internet Services

### Creating strong Apple ID passwords

Apple IDs are used to connect to a number of services including iCloud, FaceTime, and iMessage. To help users create strong passwords, all new accounts must contain the following password attributes:

- At least eight characters
- At least one letter
- At least one uppercase letter
- At least one number
- No more than three consecutive identical characters
- Not the same as the account name

Apple has built a robust set of services to help users get even more utility and productivity out of their devices, including iMessage, FaceTime, Siri, Spotlight Suggestions, iCloud, iCloud Backup, and iCloud Keychain.

These Internet services have been built with the same security goals that iOS promotes throughout the platform. These goals include secure handling of data, whether at rest on the device or in transit over wireless networks; protection of users' personal information; and threat protection against malicious or unauthorized access to information and services. Each service uses its own powerful security architecture without compromising the overall ease of use of iOS.

### Apple ID

An Apple ID is the user name and password that is used to sign in to Apple services such as iCloud, iMessage, FaceTime, the iTunes Store, the iBooks Store, the App Store, and more. It is important for users to keep their Apple IDs secure to prevent unauthorized access to their accounts. To help with this, Apple requires strong passwords that must be at least eight characters in length, contain both letters and numbers, must not contain more than three consecutive identical characters, and cannot be a commonly used password. Users are encouraged to exceed these guidelines by adding extra characters and punctuation marks to make their passwords even stronger. Apple also sends email and push notifications to users when important changes are made to their account; for example, if a password or billing information has been changed, or the Apple ID has been used to sign in on a new device. If anything does not look familiar, users are instructed to change their Apple ID password immediately.

Apple also offers two-step verification for Apple ID, which provides a second layer of security for the user's account. With two-step verification enabled, the user's identity must be verified via a temporary code sent to one of the user's trusted devices before changes are permitted to his or her Apple ID account information, before signing in to iCloud, iMessage, FaceTime, and Game Center, and before making an iTunes Store, iBooks Store, or App Store purchase from a new device. This can prevent anyone from accessing a user's account, even if they know the password. Users are also provided with a 14-character Recovery Key to be stored in a safe place in case they ever forget their password or lose access to their trusted devices.

For more information on two-step verification for Apple ID, visit <https://support.apple.com/kb/ht5570>.

## iMessage

Apple iMessage is a messaging service for iOS devices and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data.

When a user turns on iMessage on a device, the device generates two pairs of keys for use with the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key on the NIST P-256 curve for signing. The private keys for both key pairs are saved in the device's keychain and the public keys are sent to Apple's directory service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

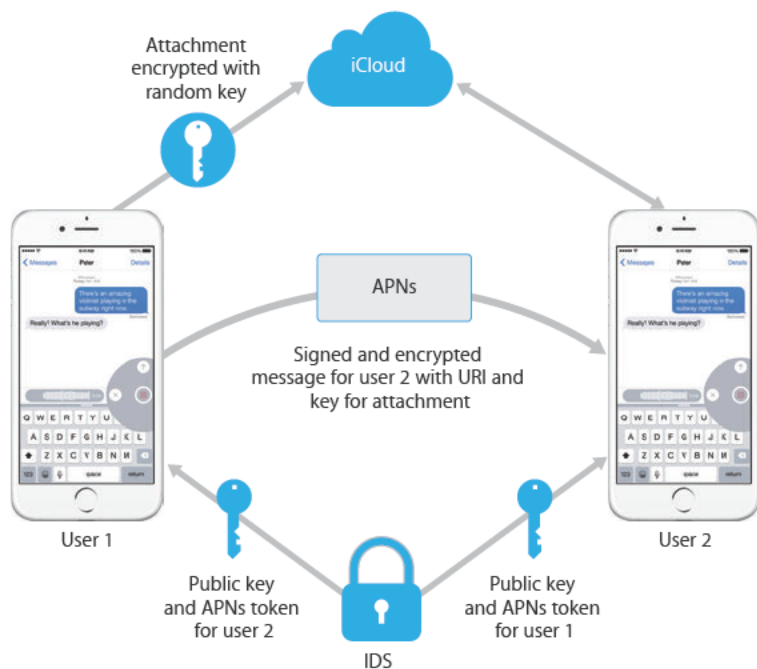
As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which will be verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. Further, all of the user's registered devices display an alert message when a new device, phone number, or email address is added.

### **How iMessage sends and receives messages**

Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the IDS to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. If the user enters a name, the device first utilizes the user's Contacts app to gather the phone numbers and email addresses associated with that name, then gets the public keys and APNs addresses from the IDS.

The user's outgoing message is individually encrypted for each of the receiver's devices. The public RSA encryption keys of the receiving devices are retrieved from IDS. For each receiving device, the sending device generates a random 128-bit key and encrypts the message with it using AES in CTR mode. This per-message AES key is encrypted using RSA-OAEP to the public key of the receiving device. The combination of the encrypted message text and the encrypted message key is then hashed with SHA-1, and the hash is signed with ECDSA using the sending device's private signing key. The resulting messages, one for each receiving device, consist of the encrypted message text, the encrypted message key, and the sender's digital signature. They are then dispatched to the APNs for delivery. Metadata, such as the timestamp and APNs routing information, is not encrypted. Communication with APNs is encrypted using a forward-secret TLS channel.

APNs can only relay messages up to 4 KB or 16 KB in size, depending on iOS version. If the message text is too long, or if an attachment such as a photo is included, the attachment is encrypted using AES in CTR mode with a randomly generated 256-bit key and uploaded to iCloud. The AES key for the attachment, its URI (Uniform Resource Identifier), and a SHA-1 hash of its encrypted form are then sent to the recipient as the contents of an iMessage, with their confidentiality and integrity protected through normal iMessage encryption, as shown below.



For group conversations, this process is repeated for each recipient and their devices.

On the receiving side, each device receives its copy of the message from APNs, and, if necessary, retrieves the attachment from iCloud. The incoming phone number or email address of the sender is matched to the receiver's contacts so that a name can be displayed, if possible.

As with all push notifications, the message is deleted from APNs when it is delivered. Unlike other APNs notifications, however, iMessage messages are queued for delivery to offline devices. Messages are currently stored for up to 30 days.

## FaceTime

FaceTime is Apple's video and audio calling service. Similar to iMessage, FaceTime calls also use the Apple Push Notification service to establish an initial connection to the user's registered devices. The audio/video contents of FaceTime calls are protected by end-to-end encryption, so no one but the sender and receiver can access them. Apple cannot decrypt the data.

FaceTime uses Internet Connectivity Establishment (ICE) to establish a peer-to-peer connection between devices. Using Session Initiation Protocol (SIP) messages, the devices verify their identity certificates and establish a shared secret for each session. The cryptographic nonces supplied by each device are combined to salt keys for each of the media channels, which are streamed via Secure Real Time Protocol (SRTP) using AES-256 encryption.

## iCloud

iCloud stores a user's contacts, calendars, photos, documents, and more and keeps the information up to date across all of his or her devices, automatically. iCloud can also be used by third-party apps to store and sync documents as well as key values for app data as defined by the developer. Users set up iCloud by signing in with an Apple ID and choosing which services they would like to use. iCloud features, including My Photo Stream, iCloud Drive, and Backup, can be disabled by IT administrators via a configuration profile. The service is agnostic about what is being stored and handles all file content the same way, as a collection of bytes.

Each file is broken into chunks and encrypted by iCloud using AES-128 and a key derived from each chunk's contents that utilizes SHA-256. The keys, and the file's metadata, are stored by Apple in the user's iCloud account. The encrypted chunks of the file are stored, without any user-identifying information, using third-party storage services, such as Amazon S3 and Windows Azure.

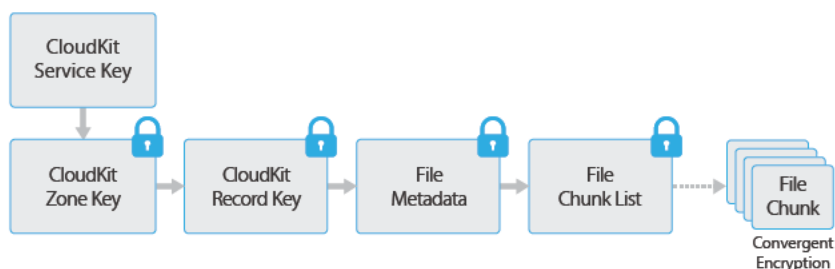
### iCloud Drive

iCloud Drive adds account-based keys to protect documents stored in iCloud. As with existing iCloud services, it chunks and encrypts file contents and stores the encrypted chunks using third-party services. However, the file content keys are wrapped by record keys stored with the iCloud Drive metadata. These record keys are in turn protected by the user's iCloud Drive service key, which is then stored with the user's iCloud account. Users get access to their iCloud documents metadata by having authenticated with iCloud, but must also possess the iCloud Drive service key to expose protected parts of iCloud Drive storage.

### CloudKit

CloudKit allows app developers to store key-value data, structured data, and assets in iCloud. Access to CloudKit is controlled using app entitlements. CloudKit supports both public and private databases. Public databases are used by all copies of the app, typically for general assets, and are not encrypted. Private databases store the user's data.

As with iCloud Drive, CloudKit uses account-based keys to protect the information stored in the user's private database and, similar to other iCloud services, files are chunked, encrypted, and stored using third-party services. CloudKit utilizes a hierarchy of keys, similar to Data Protection. The per-file keys are wrapped by CloudKit Record keys. The Record keys, in turn, are protected by a zone-wide key, which is protected by the user's CloudKit Service key. The CloudKit Service key is stored in the user's iCloud account and is available only after the user has authenticated with iCloud.



## iCloud Backup

iCloud also backs up information—including device settings, app data, photos, and videos in the Camera Roll, and conversations in the Messages app—daily over Wi-Fi. iCloud secures the content by encrypting it when sent over the Internet, storing it in an encrypted format, and using secure tokens for authentication. iCloud Backup occurs only when the device is locked, connected to a power source, and has Wi-Fi access to the Internet. Because of the encryption used in iOS, the system is designed to keep data secure while allowing incremental, unattended backup and restoration to occur.

Here's what iCloud backs up:

- Information about purchased music, movies, TV shows, apps, and books, but not the purchased content itself
- Photos and videos in Camera Roll
- Contacts, calendar events, reminders, and notes
- Device settings
- App data
- PDFs and books added to iBooks but not purchased
- Call history
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Ringtones
- HomeKit data
- HealthKit data
- Visual Voicemail

When files are created in Data Protection classes that are not accessible when the device is locked, their per-file keys are encrypted using the class keys from the iCloud Backup keybag. Files are backed up to iCloud in their original, encrypted state. Files in Data Protection class No Protection are encrypted during transport.

The iCloud Backup keybag contains asymmetric (Curve25519) keys for each Data Protection class, which are used to encrypt the per-file keys. For more information about the contents of the backup keybag and the iCloud Backup keybag, see “Keychain Data Protection” in the Encryption and Data Protection section.

The backup set is stored in the user's iCloud account and consists of a copy of the user's files, and the iCloud Backup keybag. The iCloud Backup keybag is protected by a random key, which is also stored with the backup set. (The user's iCloud password is not utilized for encryption so that changing the iCloud password won't invalidate existing backups.)

While the user's keychain database is backed up to iCloud, it remains protected by a UID-tangled key. This allows the keychain to be restored only to the same device from which it originated, and it means no one else, including Apple, can read the user's keychain items.

On restore, the backed-up files, iCloud Backup keybag, and the key for the keybag are retrieved from the user's iCloud account. The iCloud Backup keybag is decrypted using its key, then the per-file keys in the keybag are used to decrypt the files in the backup set, which are written as new files to the file system, thus re-encrypting them as per their Data Protection class.

**Safari integration with iCloud Keychain**

Safari can automatically generate cryptographically strong random strings for website passwords, which are stored in Keychain and synced to your other devices. Keychain items are transferred from device to device, traveling through Apple servers, but are encrypted in such a way that Apple and other devices cannot read their contents.

**iCloud Keychain**

iCloud Keychain allows users to securely sync his or her passwords between iOS devices and Mac computers without exposing that information to Apple. In addition to strong privacy and security, other goals that heavily influenced the design and architecture of iCloud Keychain were ease of use and the ability to recover a keychain. iCloud Keychain consists of two services: keychain syncing and keychain recovery.

Apple designed iCloud Keychain and keychain recovery so that a user's passwords are still protected under the following conditions:

- A user's iCloud account is compromised.
- iCloud is compromised by an external attacker or employee.
- Third-party access to user accounts.

**Keychain syncing**

When a user enables iCloud Keychain for the first time, the device establishes a circle of trust and creates a syncing identity for itself. A syncing identity consists of a private key and a public key. The public key of the syncing identity is put in the circle, and the circle is signed twice: first by the private key of the syncing identity, then again with an asymmetric elliptical key (using P256) derived from the user's iCloud account password. Also stored with the circle are the parameters (random salt and iterations) used to create the key that is based on the user's iCloud password.

The signed syncing circle is placed in the user's iCloud key value storage area. It cannot be read without knowing the user's iCloud password, and cannot be modified validly without having the private key of the syncing identity of its member.

When the user turns on iCloud Keychain on another device, the new device notices in iCloud that the user has a previously established syncing circle that it is not a member of. The device creates its syncing identity key pair, then creates an application ticket to request membership in the circle. The ticket consists of the device's public key of its syncing identity, and the user is asked to authenticate with his or her iCloud password. The elliptical key generation parameters are retrieved from iCloud and generate a key that is used to sign the application ticket. Finally, the application ticket is placed in iCloud.

When the first device sees that an application ticket has arrived, it displays a notice for the user to acknowledge that a new device is asking to join the syncing circle. The user enters his or her iCloud password, and the application ticket is verified as signed by a matching private key. This establishes that the person who generated the request to join the circle entered the user's iCloud password at the time the request was made.

Upon the user's approval to add the new device to the circle, the first device adds the public key of the new member to the syncing circle, signs it again with both its syncing identity and the key derived from the user's iCloud password. The new syncing circle is placed in iCloud, where it is similarly signed by the new member of the circle.

There are now two members of the signing circle, and each member has the public key of its peer. They now begin to exchange individual keychain items via iCloud key value storage. If both circle members have the same item, the one with the most recent modification date will be synced. Items are skipped if the other member has the item and the modification dates are identical. Each item that is synced is encrypted specifically for the device it is being sent to. It cannot be decrypted by other devices or Apple. Additionally, the encrypted item is ephemeral in iCloud; it's overwritten with each new item that's synced.

This process is repeated as new devices join the syncing circle. For example, when a third device joins, the confirmation appears on both of the other user's devices. The user can approve the new member from either of those devices. As new peers are added, each peer syncs with the new one to ensure that all members have the same keychain items.

However, the entire keychain is not synced. Some items are device-specific, such as VPN identities, and shouldn't leave the device. Only items with the attribute `kSecAttrSynchronizable` are synced. Apple has set this attribute for Safari user data (including user names, passwords, and credit card numbers), as well as Wi-Fi passwords and HomeKit encryption keys.

Additionally, by default, keychain items added by third-party apps do not sync. Developers must set the `kSecAttrSynchronizable` when adding items to the keychain.

### **Keychain recovery**

Keychain recovery provides a way for users to optionally escrow their keychain with Apple, without allowing Apple to read the passwords and other data it contains. Even if the user has only a single device, keychain recovery provides a safety net against data loss. This is particularly important when Safari is used to generate random, strong passwords for web accounts, as the only record of those passwords is in the keychain.

A cornerstone of keychain recovery is secondary authentication and a secure escrow service, created by Apple specifically to support this feature. The user's keychain is encrypted using a strong passcode, and the escrow service will provide a copy of the keychain only if a strict set of conditions are met.

When iCloud Keychain is turned on, the user is asked to create an iCloud Security Code. This code is required to recover an escrowed keychain. By default, the user is asked to provide a simple four-digit value for the security code. However, users can also specify their own, longer code, or let their devices create a cryptographically random code that they can record and keep on their own.

Next, the iOS device exports a copy of the user's keychain, encrypts it wrapped with keys in an asymmetric keybag, and places it in the user's iCloud key value storage area. The keybag is wrapped with the user's iCloud Security Code and the public key of the HSM (hardware security module) cluster that will store the escrow record. This becomes the user's iCloud Escrow Record.

If the user decided to accept a cryptographically random security code, instead of specifying his or her own or using a four-digit value, no escrow record is necessary. Instead, the iCloud Security Code is used to wrap the random key directly.

In addition to establishing a security code, users must register a phone number. This is used to provide a secondary level of authentication during keychain recovery. The user will receive an SMS that must be replied to in order for the recovery to proceed.

### **Escrow security**

iCloud provides a secure infrastructure for keychain escrow that ensures only authorized users and devices can perform a recovery. Topographically positioned behind iCloud are clusters of hardware security modules (HSM). These clusters guard the escrow records. Each has a key that is used to encrypt the escrow records under their watch, as described previously.



To recover a keychain, users must authenticate with their iCloud account and password and respond to an SMS sent to their registered phone number. Once this is done, users must enter their iCloud Security Code. The HSM cluster verifies that a user knows his or her iCloud Security Code using Secure Remote Password protocol (SRP); the code itself is not sent to Apple. Each member of the cluster independently verifies that the user has not exceeded the maximum number of attempts that are allowed to retrieve his or her record, as discussed below. If a majority agree, the cluster unwraps the escrow record and sends it to the user's device.

Next, the device uses the iCloud Security Code to unwrap the random key used to encrypt the user's keychain. With that key, the keychain—retrieved from iCloud key value storage—is decrypted and restored onto the device. Only 10 attempts to authenticate and retrieve an escrow record are allowed. After several failed attempts, the record is locked and the user must call Apple Support to be granted more attempts. After the 10th failed attempt, the HSM cluster destroys the escrow record and the keychain is lost forever. This provides protection against a brute-force attempt to retrieve the record, at the expense of sacrificing the keychain data in response.

These policies are coded in the HSM firmware. The administrative access cards that permit the firmware to be changed have been destroyed. Any attempt to alter the firmware or access the private key will cause the HSM cluster to delete the private key. Should this occur, the owners of all keychains protected by the cluster will receive a message informing them that their escrow record has been lost. They can then choose to re-enroll.

## Siri

By simply talking naturally, users can enlist Siri to send messages, schedule meetings, place phone calls, and more. Siri uses speech recognition, text-to-speech, and a client-server model to respond to a broad range of requests. The tasks that Siri supports have been designed to ensure that only the absolute minimal amount of personal information is utilized and that it is fully protected.

When Siri is turned on, the device creates random identifiers for use with the voice recognition and Siri servers. These identifiers are used only within Siri and are utilized to improve the service. If Siri is subsequently turned off, the device will generate a new random identifier to be used if Siri is turned back on.

In order to facilitate Siri's features, some of the user's information from the device is sent to the server. This includes information about the music library (song titles, artists, and playlists), the names of Reminders lists, and names and relationships that are defined in Contacts. All communication with the server is over HTTPS.

When a Siri session is initiated, the user's first and last name (from Contacts), along with a rough geographic location, is sent to the server. This is so Siri can respond with the name or answer questions that only need an approximate location, such as those about the weather.

If a more precise location is necessary, for example, to determine the location of nearby movie theaters, the server asks the device to provide a more exact location. This is an example of how, by default, information is sent to the server only when it's strictly necessary to process the user's request. In any event, session information is discarded after 10 minutes of inactivity.

When Siri is used from Apple Watch, the watch creates its own random unique identifier, as described above. However, instead of sending the user's information again, its requests also send the Siri identifier of the paired iPhone to provide a reference to that information.

The recording of the user's spoken words is sent to Apple's voice recognition server. If the task involves dictation only, the recognized text is sent back to the device. Otherwise, Siri analyzes the text and, if necessary, combines it with information from the profile associated with the device. For example, if the request is "send a message to my mom," the relationships and names that were uploaded from Contacts are utilized. The command for the identified action is then sent back to the device to be carried out.

Many Siri functions are accomplished by the device under the direction of the server. For example, if the user asks Siri to read an incoming message, the server simply tells the device to speak the contents of its unread messages. The contents and sender of the message are not sent to the server.

User voice recordings are saved for a six-month period so that the recognition system can utilize them to better understand the user's voice. After six months, another copy is saved, without its identifier, for use by Apple in improving and developing Siri for up to two years. Additionally, some recordings that reference music, sports teams and players, and businesses or points of interest are similarly saved for purposes of improving Siri.

Siri can also be invoked hands-free via voice activation. The voice trigger detection is performed locally on the device. In this mode, Siri is activated only when the incoming audio pattern sufficiently matches the acoustics of the specified trigger phrase. When the trigger is detected, the corresponding audio including the subsequent Siri command is sent to Apple's voice recognition server for further processing, which follows the same rules as other user voice recordings made through Siri.

## Continuity

Continuity takes advantage of technologies like iCloud, Bluetooth, and Wi-Fi to enable users to continue an activity from one device to another, make and receive phone calls, send and receive text messages, and share a cellular Internet connection.

### Handoff

With Handoff, when a user's Mac and iOS device are near each other, the user can automatically pass whatever they're working on from one device to the other. Handoff lets the user switch devices and instantly continue working.

When a user signs in to iCloud on a second Handoff capable device, the two devices establish a Bluetooth Low Energy 4.0 pairing out-of-band using the Apple Push Notification service (APNs). The individual messages are encrypted in a similar fashion to iMessage. Once the devices are paired, each will generate a symmetric 256-bit AES key that gets stored in the device's keychain. This key is used to encrypt and authenticate the Bluetooth Low Energy advertisements that communicate the device's current activity to other iCloud paired devices using AES-256 in GCM mode, with replay protection measures. The first time a device receives an advertisement from a new key, it will establish a Bluetooth Low Energy connection to the originating device and perform an advertisement encryption key exchange. This connection is secured using standard Bluetooth Low Energy 4.0 encryption as well as encryption of the individual messages, which is similar to how iMessage is encrypted. In some situations, these messages will go via the Apple Push Notification service instead of Bluetooth Low Energy. The activity payload is protected and transferred in the same way as an iMessage.

### **Handoff between native apps and websites**

Handoff allows an iOS native app to resume webpages in domains legitimately controlled by the app developer. It also allows the native app user activity to be resumed in a web browser.

To prevent native apps from claiming to resume websites not controlled by the developer, the app must demonstrate legitimate control over the web domains it wants to resume. Control over a website domain is established via the mechanism used for shared web credentials. For details, refer to “Access to Safari saved passwords” in the Encryption and Data Protection section. The system must validate an app’s domain name control before the app is permitted to accept user activity Handoff.

The source of a webpage Handoff can be any browser that has adopted the Handoff APIs. When the user views a webpage, the system advertises the domain name of the webpage in the encrypted Handoff advertisement bytes. Only the user’s other devices can decrypt the advertisement bytes (as previously described in the section above).

On a receiving device, the system detects that an installed native app accepts Handoff from the advertised domain name and displays that native app icon as the Handoff option. When launched, the native app receives the full URL and the title of the webpage. No other information is passed from the browser to the native app.

In the opposite direction, a native app may specify a fallback URL when a Handoff-receiving device does not have the same native app installed. In this case, the system displays the user’s default browser as the Handoff app option (if that browser has adopted Handoff APIs). When Handoff is requested, the browser will be launched and given the fallback URL provided by the source app. There is no requirement that the fallback URL be limited to domain names controlled by the native app developer.

### **Handoff of larger data**

In addition to the basic feature of Handoff, some apps may elect to use APIs that support sending larger amounts of data over Apple-created peer-to-peer Wi-Fi technology (in a similar fashion to AirDrop). For example, the Mail app uses these APIs to support Handoff of a mail draft, which may include large attachments.

When an app uses this facility, the exchange between the two devices starts off just as in Handoff (see previous sections). However, after receiving the initial payload using Bluetooth Low Energy, the receiving device initiates a new connection over Wi-Fi. This connection is encrypted (TLS), which exchanges their iCloud identity certificates. The identity in the certificates is verified against the user’s identity. Further payload data is sent over this encrypted connection until the transfer is complete.

### **iPhone Cellular Call Relay**

When your Mac, iPad, or iPod is on the same Wi-Fi network as your iPhone, it can make and receive phone calls using your iPhone cellular connection. Configuration requires your devices to be signed in to both iCloud and FaceTime using the same Apple ID account.

When an incoming call arrives, all configured devices will be notified via the Apple Push Notification service (APNs), with each notification using the same end-to-end encryption as iMessage uses. Devices that are on the same network will present the incoming call notification UI. Upon answering the call, the audio will be seamlessly transmitted from your iPhone using a secure peer-to-peer connection between the two devices.

Outgoing calls will also be relayed to iPhone via the Apple Push Notification service, and audio will be similarly transmitted over the secure peer-to-peer link between devices.

Users can disable phone call relay on a device by turning off iPhone Cellular Calls in FaceTime settings.

### **iPhone Text Message Forwarding**

Text Message Forwarding automatically sends SMS text messages received on iPhone to a user's enrolled iPad, iPod touch, or Mac. Each device must be signed in to the iMessage service using the same Apple ID account. When SMS Message Forwarding is turned on, enrollment is verified on each device by entering a random six-digit numeric code generated by iPhone.

Once devices are linked, iPhone encrypts and forwards incoming SMS text messages to each device, utilizing the methods described in the iMessage section of this document. Replies are sent back to iPhone using the same method, then iPhone sends the reply as a text message using the carrier's SMS transmission mechanism. Text Message Forwarding can be turned on or off in Messages settings.

### **Instant Hotspot**

iOS devices that support Instant Hotspot use Bluetooth Low Energy to discover and communicate to devices that have signed in to the same iCloud account. Compatible Mac computers running OS X Yosemite and later use the same technology to discover and communicate with Instant Hotspot iOS devices.

When a user enters Wi-Fi Settings on the iOS device, the device emits a Bluetooth Low Energy signal containing an identifier that all devices signed in to the same iCloud account agree upon. The identifier is generated from a DSID (Destination Signaling Identifier) tied to the iCloud account, and rotated periodically. When other devices signed in to the same iCloud account are in close proximity and support personal hotspot, they detect the signal and respond, indicating availability.

When a user chooses a device available for personal hotspot, a request to turn on Personal Hotspot is sent to that device. The request is sent across a link that is encrypted using standard Bluetooth Low Energy encryption, and the request is encrypted in a fashion similar to iMessage encryption. The device then responds across the same Bluetooth Low Energy link using the same per-message encryption with personal hotspot connection information.

## **Spotlight Suggestions**

Safari search and Spotlight search include search suggestions from the Internet, apps, iTunes, App Store, movie showtimes, locations nearby, and more.

To make suggestions more relevant to users, user context and search feedback with search query requests are sent to Apple. Context sent with search requests provides Apple with: i) the device's approximate location; ii) the device type (e.g., Mac, iPhone, iPad, or iPod); iii) the client app, which is either Spotlight or Safari; iv) the device's default language and region settings; v) the three most recently used apps on the device; and vi) an anonymous session ID. All communication with the server is encrypted via HTTPS.

To help protect user privacy, Spotlight Suggestions never sends exact location, instead blurring the location on the client before sending. The level of blurring is based on estimated population density at the device's location; for instance, more blurring is used in a rural location versus less blurring in a city center where users will typically be closer together. Further, users can disable the sending of all location information to Apple in Settings, by turning off Location Services for Spotlight Suggestions. If Location Services is disabled, then Apple may use the client's IP address to infer an approximate location.

The anonymous session ID allows Apple to analyze patterns between queries conducted in a 15-minute period. For instance, if users frequently search for "Café phone number" shortly after searching for "Café," Apple may learn to make the phone number more available in results. Unlike most search engines, however, Apple's search service does not use a persistent personal identifier across a user's search history to tie queries to a user or device; instead, Apple devices use a temporary anonymous session ID for at most a 15-minute period before discarding that ID.

Information on the three most recently used apps on the device is included as additional search context. To protect the privacy of users, only apps that are in an Apple-maintained whitelist of popular apps and have been accessed within the last three hours are included.

Search feedback sent to Apple provides Apple with: i) timings between user actions such as key-presses and result selections; ii) Spotlight Suggestions result selected, if any; and iii) type of local result selected (e.g., "Bookmark" or "Contact"). Just as with search context, the search feedback is not tied to any individual person or device.

Apple retains Spotlight Suggestions logs with queries, context, and feedback for up to 18 months. Reduced logs including only query, country, language, date (to the hour), and device-type are retained up to two years. IP addresses are not retained with query logs.

In some cases, Spotlight Suggestions may forward queries for common words and phrases to a qualified partner in order to receive and display the partner's search results. These queries are not stored by the qualified partner and partners do not receive search feedback. Partners also do not receive user IP addresses. Communication with the partner is encrypted via HTTPS. Apple will provide city-level location, device type, and client language as search context to the partner based on which locations, device types, and languages Apple sees repeated queries from.

Spotlight Suggestions can be turned off in Settings for Spotlight, for Safari, or for both. If turned off for Spotlight, then Spotlight is reverted to being a local on-device-only search client that does not transmit information to Apple. If turned off in Safari, the user's search queries, search context, and search feedback are not transmitted to Apple.

Spotlight also includes mechanisms for making local, on-device content searchable:

- The CoreSpotlight API, which allows Apple and third-party apps to pass indexable content to Spotlight.
- The NSUserActivity API, which allows Apple and third-party apps to pass information to Spotlight regarding app pages visited by the user.

Spotlight maintains an on-device index of the information it receives using these two methods, so that results from this data can be shown in response to a user's search, or automatically when Spotlight is launched. There is also an on-device federated search API, only available to Apple-provided apps, which allows Spotlight to pass user search queries to apps for processing, and receive their results.

# Device Controls

iOS supports flexible security policies and configurations that are easy to enforce and manage. This enables organizations to protect corporate information and ensure that employees meet enterprise requirements, even if they are using devices they've provided themselves—for example, as part of a “bring your own device” (BYOD) program.

Organizations can use resources such as passcode protection, configuration profiles, remote wipe, and third-party MDM solutions to manage fleets of devices and help keep corporate data secure, even when employees access this data on their personal iOS devices.

## Passcode protection

By default, the user's passcode can be defined as a numeric PIN. On devices with Touch ID, the minimum passcode length is six digits. On other devices, the minimum length is four digits. Users can specify a longer alphanumeric passcode by selecting Custom Alphanumeric Code in the Passcode Options in Settings > Passcode. Longer and more complex passcodes are harder to guess or attack, and are recommended for enterprise use.

Administrators can enforce complex passcode requirements and other policies using MDM or Exchange ActiveSync, or by requiring users to manually install configuration profiles. The following passcode policies are available:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Auto-lock timeout
- Grace period for device lock
- Maximum number of failed attempts
- Allow Touch ID

For details about each policy, see the Configuration Profile Key Reference documentation at <https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/>.

## iOS pairing model

iOS uses a pairing model to control access to a device from a host computer. Pairing establishes a trust relationship between the device and its connected host, signified by public key exchange. iOS uses this sign of trust to enable additional functionality with the connected host, such as data synchronization. In iOS 9, services that require pairing cannot be started until after the device has been unlocked by the user.

The pairing process requires the user to unlock the device and accept the pairing request from the host. After the user has done this, the host and device exchange and save 2048-bit RSA public keys. The host is then given a 256-bit key that can unlock an escrow keybag stored on the device (see Escrow keybags in the Keybags section). The exchanged keys are used to start an encrypted SSL session, which the device requires before it will send protected data to the host or start a service (iTunes syncing, file transfers, Xcode development, etc.). The device requires connections from a host over Wi-Fi to use this encrypted session for all communication, so it must have been previously paired over USB. Pairing also enables several diagnostic capabilities. In iOS 9, if a pairing record has not been used for more than six months, it expires. For more information, see <https://support.apple.com/kb/HT6331>.

Certain services, including com.apple.pcapd, are restricted to work only over USB. Additionally, the com.apple.file\_relay service requires an Apple-signed configuration profile to be installed.

A user can clear the list of trusted hosts by using the “Reset Network Settings” or “Reset Location & Privacy” options. For more information, see <https://support.apple.com/kb/HT5868>.

## Configuration enforcement

A configuration profile is an XML file that allows an administrator to distribute configuration information to iOS devices. Settings that are defined by an installed configuration profile can't be changed by the user. If the user deletes a configuration profile, all the settings defined by the profile are also removed. In this manner, administrators can enforce settings by tying policies to access. For example, a configuration profile that provides an email configuration can also specify a device passcode policy. Users won't be able to access mail unless their passcodes meet the administrator's requirements.

An iOS configuration profile contains a number of settings that can be specified, including:

- Passcode policies
- Restrictions on device features (disabling the camera, for example)
- Wi-Fi settings
- VPN settings
- Mail server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips
- Credentials and keys
- Advanced cellular network settings

Configuration profiles can be signed and encrypted to validate their origin, ensure their integrity, and protect their contents. Configuration profiles are encrypted using CMS (RFC 3852), supporting 3DES and AES-128.

Configuration profiles can also be locked to a device to completely prevent their removal, or to allow removal only with a passcode. Since many enterprise users own their iOS devices, configuration profiles that bind a device to an MDM server can be removed—but doing so will also remove all managed configuration information, data, and apps.

Users can install configuration profiles directly on their devices using Apple Configurator, or they can be downloaded via Safari, sent via a mail message, or sent over the air using an MDM server.

## Mobile device management (MDM)

iOS support for MDM allows businesses to securely configure and manage scaled iPhone and iPad deployments across their organizations. MDM capabilities are built on existing iOS technologies such as configuration profiles, over-the-air enrollment, and the Apple Push Notification service (APNs). For example, APNs is used to wake the device so it can communicate directly with its MDM server over a secured connection. No confidential or proprietary information is transmitted via APNs.

Using MDM, IT departments can enroll iOS devices in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed devices. For more information on mobile device management, see [www.apple.com/iphone/business/it/management.html](http://www.apple.com/iphone/business/it/management.html).

## Device Enrollment Program

The Device Enrollment Program (DEP) provides a fast, streamlined way to deploy iOS devices that an organization has purchased directly from Apple or through participating Apple Authorized Resellers and carriers. The organization can automatically enroll devices in MDM without having to physically touch or prep the devices before users get them. The setup process for users can be further simplified by removing specific steps in the Setup Assistant, so users are up and running quickly. Administrators can also control whether or not the user can remove the MDM profile from the device and ensure that device restrictions are in place from the very start. For example, they can order the devices from Apple, configure all the management settings, and have the devices shipped directly to the user's home address. Once the device is unboxed and activated, the device enrolls in the organization's MDM—and all management settings, apps, and books are ready for the user.

The process is simple: After enrolling in the program, administrators log in to the program website, link the program to their MDM server, and "claim" the iOS devices purchased through Apple. The devices can then be assigned to users via MDM. Once a user has been assigned, any MDM-specified configurations, restrictions, or controls are automatically installed. For more information, see <https://deploy.apple.com>.

**Note:** The Device Enrollment Program is not available in all countries or regions.



## Apple Configurator

In addition to MDM, Apple Configurator for OS X makes it easy for anyone to deploy iOS devices. Apple Configurator can be used to quickly configure large numbers of devices with apps, data, restrictions, and settings.

### Supervision

During the setup of a device, an organization can configure a device to be supervised. Supervision denotes that a device is institutionally owned, which provides additional control over its configuration and restrictions. Devices can be supervised during setup through the Device Enrollment Program or Apple Configurator.

For more information on configuring and managing devices using MDM or Apple Configurator, see the iOS Deployment Reference at

<https://help.apple.com/deployment/ios>.

For information about the additional controls for supervised devices, see the Configuration Profile Reference: <https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf>.

## Device restrictions

Administrators can restrict device features by installing a configuration profile. Some of the restrictions available include:

- Allow app installs
- Allow trusting enterprise apps
- Allow use of camera
- Allow FaceTime
- Allow screenshots
- Allow voice dialing while locked
- Allow automatic sync while roaming
- Allow in-app purchases
- Allow syncing of recent Mail
- Force user to enter store password for all purchases
- Allow Siri while device is locked
- Allow use of iTunes Store
- Allow documents from managed sources in unmanaged destinations
- Allow documents from unmanaged sources in managed destinations
- Allow iCloud Keychain sync
- Allow updating certificate trust database over the air
- Allow showing notifications on Lock screen
- Force AirPlay connections to use pairing passwords
- Allow Spotlight to show user-generated content from the Internet
- Enable Spotlight Suggestions in Spotlight
- Allow Handoff
- Treat AirDrop as unmanaged destination
- Allow enterprise books to be backed up
- Allow notes and bookmarks in enterprise books to sync across the user's devices
- Allow use of Safari

- Enable Safari autofill
- Force Fraudulent Website Warning
- Enable JavaScript
- Limit ad tracking in Safari
- Block pop-ups
- Accept cookies
- Allow iCloud backup
- Allow iCloud document and key-value sync
- Allow iCloud Photo Sharing
- Allow diagnostics to be sent to Apple
- Allow user to accept untrusted TLS certificates
- Force encrypted backups
- Allow Touch ID
- Allow Control Center access from Lock screen
- Allow Today view from Lock screen
- Require Apple Watch wrist detection

### Supervised-only restrictions

- Allow iMessage
- Allow removal of apps
- Allow manual install of configuration profiles
- Global network proxy for HTTP
- Allow pairing to computers for content sync
- Restrict AirPlay connections with whitelist and optional connection passcodes
- Allow AirDrop
- Allow Find My Friends modification
- Allow autonomous Single App Mode for certain managed apps
- Allow account modification
- Allow cellular data modification
- Allow host pairing (iTunes)
- Allow Activation Lock
- Prevent Erase All Content and Settings
- Prevent enabling restrictions
- Third-party content filter
- Single App mode
- Always-on VPN
- Allow passcode modification
- Allow Apple Watch pairing
- Allow automatic app downloads
- Allow keyboard prediction, autocorrection, spell check, and short cuts

For more information about restrictions, see <https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf>

## Remote wipe

iOS devices can be erased remotely by an administrator or user. Instant remote wipe is achieved by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable. A remote wipe command can be initiated by MDM, Exchange, or iCloud.

When a remote wipe command is triggered by MDM or iCloud, the device sends an acknowledgment and performs the wipe. For remote wipe via Exchange, the device checks in with the Exchange Server before performing the wipe.

Users can also wipe devices in their possession using the Settings app. And as mentioned, devices can be set to automatically wipe after a series of failed passcode attempts.

## Find My iPhone and Activation Lock

If a device is lost or stolen, it's important to deactivate and erase the device. With iOS 7 or later, when Find My iPhone is turned on, the device can't be reactivated without entering the owner's Apple ID credentials. It's a good idea for an organization to either supervise its devices or have a policy in place for users to disable the feature so that Find My iPhone doesn't prevent the organization from assigning the device to another individual.

With iOS 7.1 or later, a compatible MDM solution can enable Activation Lock on supervised devices when a user turns on Find My iPhone. MDM administrators can manage Find My iPhone Activation Lock by supervising devices with Apple Configurator or the Device Enrollment Program. The MDM solution can then store a bypass code when Activation Lock is enabled, and later use this code to clear Activation Lock automatically when the device needs to be erased and assigned to a new user. See your MDM solution documentation for details.

**Important:** By default, supervised devices never have Activation Lock enabled, even if the user turns on Find My iPhone. However, an MDM server may retrieve a bypass code and permit Activation Lock on the device. If Find My iPhone is turned on when the MDM server enables Activation Lock, it is enabled at that point. If Find My iPhone is turned off when the MDM server enables Activation Lock, it's enabled the next time the user activates Find My iPhone.

# Privacy Controls

Apple takes customer privacy seriously and has numerous built-in controls and options that allow iOS users to decide how and when apps utilize their information, as well as what information is being utilized.

## Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine the user's approximate location. Location Services can be turned off using a single switch in Settings, or users can approve access for each app that uses the service. Apps may request to receive location data only while the app is being used or allow it at any time. Users may choose not to allow this access, and may change their choice at any time in Settings. From Settings, access can be set to never allowed, allowed when in use, or always, depending on the app's requested location use. Also, if apps granted access to use location at any time make use of this permission while in background mode, users are reminded of their approval and may change an app's access.

Additionally, users are given fine-grained control over system services' use of location information. This includes being able to turn off the inclusion of location information in information collected by the diagnostic and usage services used by Apple to improve iOS, location-based Siri information, location-based context for Spotlight Suggestions searches, local traffic conditions, and frequently visited locations used to estimate travel times.

## Access to personal data

iOS helps prevent apps from accessing a user's personal information without permission. Additionally, in Settings, users can see which apps they have permitted to access certain information, as well as grant or revoke any future access. This includes access to:

- Contacts
- Calendars
- Reminders
- Photos
- Motion activity on iPhone 5s or later
- Social media accounts, such as Twitter and Facebook
- Microphone
- Camera
- HomeKit
- HealthKit
- Bluetooth sharing

If the user signs in to iCloud, apps are granted access by default to iCloud Drive. Users may control each app's access under iCloud in Settings. Additionally, iOS provides restrictions that prevent data movement between apps and accounts installed by MDM and those installed by the user.

## Privacy policy

Apple's privacy policy is available online at <https://www.apple.com/legal/privacy>.

# Conclusion

## A commitment to security

Apple is committed to helping protect customers with leading privacy and security technologies that are designed to safeguard personal information, as well as comprehensive methods to help protect corporate data in an enterprise environment.

Security is built into iOS. From the platform to the network to the apps, everything a business needs is available in the iOS platform. Together, these components give iOS its industry-leading security without compromising the user experience.

Apple uses a consistent, integrated security infrastructure throughout iOS and the iOS apps ecosystem. Hardware-based storage encryption provides remote wipe capabilities when a device is lost, and enables users to completely remove all corporate and personal information when a device is sold or transferred to another owner. Diagnostic information is also collected anonymously.

iOS apps designed by Apple are built with enhanced security in mind. Safari offers safe browsing with support for Online Certificate Status Protocol (OCSP), EV certificates, and certificate verification warnings. Mail leverages certificates for authenticated and encrypted Mail by supporting S/MIME, which permits per-message S/MIME, so S/MIME users can choose to always sign and encrypt by default, or selectively control how individual messages are protected. iMessage and FaceTime also provide client-to-client encryption.

For third-party apps, the combination of required code signing, sandboxing, and entitlements gives users solid protection against viruses, malware, and other exploits that compromise the security of other platforms. The App Store submission process works to further shield users from these risks by reviewing every iOS app before it's made available for sale.

To make the most of the extensive security features built into iOS, businesses are encouraged to review their IT and security policies to ensure that they are taking full advantage of the layers of security technology offered by this platform.

Apple maintains a dedicated security team to support all Apple products. The team provides security auditing and testing for products under development, as well as for released products. The Apple team also provides security tools and training, and actively monitors for reports of new security issues and threats. Apple is a member of the Forum of Incident Response and Security Teams (FIRST). To learn more about reporting issues to Apple and subscribing to security notifications, go to [apple.com/support/security](http://apple.com/support/security).

# Glossary

<b>Address space layout randomization (ASLR)</b>	A technique employed by iOS to make the successful exploitation of a software bug much more difficult. By ensuring memory addresses and offsets are unpredictable, exploit code can't hard code these values. In iOS 5 and later, the position of all system apps and libraries are randomized, along with all third-party apps compiled as position-independent executables.
<b>Apple Push Notification service (APNs)</b>	A worldwide service provided by Apple that delivers push notifications to iOS devices.
<b>Boot ROM</b>	The very first code executed by a device's processor when it first boots. As an integral part of the processor, it can't be altered by either Apple or an attacker.
<b>Data Protection</b>	File and keychain protection mechanism for iOS. It can also refer to the APIs that apps use to protect files and keychain items.
<b>Device Firmware Upgrade (DFU)</b>	A mode in which a device's Boot ROM code waits to be recovered over USB. The screen is black when in DFU mode, but upon connecting to a computer running iTunes, the following prompt is presented: "iTunes has detected an iPad in recovery mode. You must restore this iPad before it can be used with iTunes."
<b>ECID</b>	A 64-bit identifier that's unique to the processor in each iOS device. Used as part of the personalization process, it's not considered a secret.
<b>Effaceable Storage</b>	A dedicated area of NAND storage, used to store cryptographic keys, that can be addressed directly and wiped securely. While it doesn't provide protection if an attacker has physical possession of a device, keys held in Effaceable Storage can be used as part of a key hierarchy to facilitate fast wipe and forward security.
<b>File system key</b>	The key that encrypts each file's metadata, including its class key. This is kept in Effaceable Storage to facilitate fast wipe, rather than confidentiality.
<b>Group ID (GID)</b>	Like the UID but common to every processor in a class.
<b>Hardware security module (HSM)</b>	A specialized tamper-resistant computer that safeguards and manages digital keys.
<b>iBoot</b>	Code that's loaded by LLB, and in turn loads XNU, as part of the secure boot chain.
<b>Identity Service (IDS)</b>	Apple's directory of iMessage public keys, APNs addresses, and phone numbers and email addresses that are used to look up the keys and device addresses.
<b>Integrated circuit (IC)</b>	Also known as a microchip.
<b>Joint Test Action Group (JTAG)</b>	Standard hardware debugging tool used by programmers and circuit developers.
<b>Keybag</b>	<p>A data structure used to store a collection of class keys. Each type (system, backup, escrow, or iCloud Backup) has the same format:</p> <ul style="list-style-type: none"> <li>• A header containing: <ul style="list-style-type: none"> <li>– Version (set to 3 in iOS 5)</li> <li>– Type (system, backup, escrow, or iCloud Backup)</li> <li>– Keybag UUID</li> <li>– An HMAC if the keybag is signed</li> <li>– The method used for wrapping the class keys: tangling with the UID or PBKDF2, along with the salt and iteration count</li> </ul> </li> <li>• A list of class keys: <ul style="list-style-type: none"> <li>– Key UUID</li> <li>– Class (which file or keychain Data Protection class this is)</li> <li>– Wrapping type (UID-derived key only; UID-derived key and passcode-derived key)</li> <li>– Wrapped class key</li> <li>– Public key for asymmetric classes</li> </ul> </li> </ul>

<b>Keychain</b>	The infrastructure and a set of APIs used by iOS and third-party apps to store and retrieve passwords, keys, and other sensitive credentials.
<b>Key wrapping</b>	Encrypting one key with another. iOS uses NIST AES key wrapping, as per RFC 3394.
<b>Low-Level Bootloader (LLB)</b>	Code that's invoked by the Boot ROM, and in turn loads iBoot, as part of the secure boot chain.
<b>Per-file key</b>	The AES 256-bit key used to encrypt a file on the file system. The per-file key is wrapped by a class key and is stored in the file's metadata.
<b>Provisioning Profile</b>	A plist signed by Apple that contains a set of entities and entitlements allowing apps to be installed and tested on an iOS device. A development Provisioning Profile lists the devices that a developer has chosen for ad hoc distribution, and a distribution Provisioning Profile contains the app ID of an enterprise-developed app.
<b>Ridge flow angle mapping</b>	A mathematical representation of the direction and width of the ridges extracted from a portion of a fingerprint.
<b>Smart card</b>	An integrated, embedded circuit that provides secure identification, authentication, and data storage.
<b>System on a chip (SoC)</b>	An integrated circuit (IC) that incorporates multiple components into a single chip. The Secure Enclave is an SoC within Apple's A7-or-later central processor.
<b>Tangling</b>	The process by which a user's passcode is turned into a cryptographic key and strengthened with the device's UID. This ensures that a brute-force attack must be performed on a given device, and thus is rate limited and cannot be performed in parallel. The tangling algorithm is PBKDF2, which uses AES keyed with the device UID as the pseudorandom function (PRF) for each iteration.
<b>Uniform Resource Identifier (URI)</b>	A string of characters that identifies a web-based resource.
<b>Unique ID (UID)</b>	A 256-bit AES key that's burned into each processor at manufacture. It cannot be read by firmware or software, and is used only by the processor's hardware AES engine. To obtain the actual key, an attacker would have to mount a highly sophisticated and expensive physical attack against the processor's silicon. The UID is not related to any other identifier on the device including, but not limited to, the UDID.
<b>XNU</b>	The kernel at the heart of the iOS and OS X operating systems. It's assumed to be trusted, and enforces security measures such as code signing, sandboxing, entitlement checking, and ASLR.

# Document Revision History

Date	Summary
September 2015	<p data-bbox="829 436 992 457"><b>Updated for iOS 9</b></p> <ul style="list-style-type: none"> <li data-bbox="829 474 1081 495">• Apple Watch activation lock</li> <li data-bbox="829 512 992 533">• Passcode policies</li> <li data-bbox="829 550 1024 571">• Touch ID API support</li> <li data-bbox="829 588 1154 609">• Data Protection on A8 uses AES-XTS</li> <li data-bbox="829 625 1195 646">• Keybags for unattended software update</li> <li data-bbox="829 663 1016 684">• Certification updates</li> <li data-bbox="829 701 1073 722">• Enterprise app trust model</li> <li data-bbox="829 739 1162 760">• Data protection for Safari bookmarks</li> <li data-bbox="829 777 1040 798">• App Transport Security</li> <li data-bbox="829 814 1000 835">• VPN specifications</li> <li data-bbox="829 852 1146 873">• iCloud Remote Access for HomeKit</li> <li data-bbox="829 890 1057 911">• Apple Pay Rewards cards</li> <li data-bbox="829 928 1073 949">• Apple Pay card issuer's app</li> <li data-bbox="829 966 1089 987">• Spotlight on-device indexing</li> <li data-bbox="829 1003 1000 1024">• iOS Pairing Model</li> <li data-bbox="829 1041 1008 1062">• Apple Configurator</li> <li data-bbox="829 1079 943 1100">• Restrictions</li> <li data-bbox="829 1117 1382 1182">• For more information about the security contents of iOS 9 see: <a href="http://support.apple.com/HT205212">support.apple.com/HT205212</a></li> </ul>

© 2015 Apple Inc. All rights reserved. Apple, the Apple logo, AirDrop, AirPlay, Apple TV, Apple Watch, Bonjour, FaceTime, iBooks, iMessage, iPad, iPhone, iPod, iPod touch, iTunes, Keychain, Mac, OS X, Safari, Siri, Spotlight, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Apple Pay, CarPlay Lightning, and Touch ID are trademarks of Apple Inc. iCloud and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. App Store and iBooks Store are service marks of Apple Inc. iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Apple is under license. Java is a registered trademark of Oracle and/or its affiliates. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. September 2015



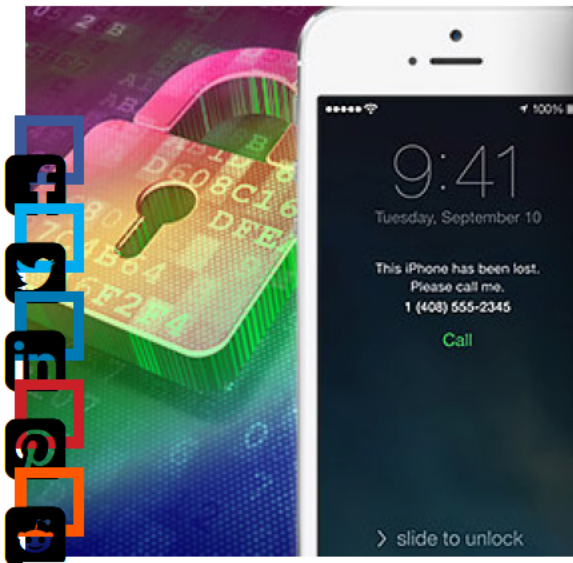
# **Exhibit I**

[Home \(/\)](#) / [Reviews \(http://www.pcmag.com/category2/0,2806,13,00.asp\)](http://www.pcmag.com/category2/0,2806,13,00.asp) / [Cell Phones \(/reviews/cell-phones\)](/reviews/cell-phones/) / **iOS 7 Makes the iPhone More Secure than Ever**

## iOS 7 Makes the iPhone More Secure than Ever

BY [MAX EDDY \(/AUTHOR-BIO/MAX-EDDY\)](/AUTHOR-BIO/MAX-EDDY) SEPTEMBER 13, 2013 [0 COMMENTS](#)

*The latest version of Apple's mobile operating system, and the new iPhone 5S, bring a slew of new security features, making iOS 7 Cupertino's most secure mobile platform ever.*



Apple is notoriously tight-lipped about security, usually letting the glitz of its products do the talking (and also not wanting to invite trouble). But at this week's **[iPhone 5s and iPhone 5c launch event in Cupertino](http://www.pcmag.com/article2/0,2817,2424217,00.asp)** (<http://www.pcmag.com/article2/0,2817,2424217,00.asp>), security was one of the biggest features touted by the notoriously design-driven company. True, a lot of the attention was focused on the **integrated fingerprint reader** (<http://securitywatch.pcmag.com/mobile-security/314872-can-next-gen-phones-deliver-next-gen-security>) in the flagship **iPhone 5s** (<http://www.pcmag.com/article2/0,2817,2424245,00.asp>), but with these new phones and the new iOS 7, Apple has doubled down on mobile security.

### CONTENTS

iOS 7 Makes the iPhone More Secure than Ever

iCloud Keychain & Improved Privacy (<http://www.pcmag.com>)

SMS and Call Blocking, Plus Encryption (<http://www.pcmag.com>)



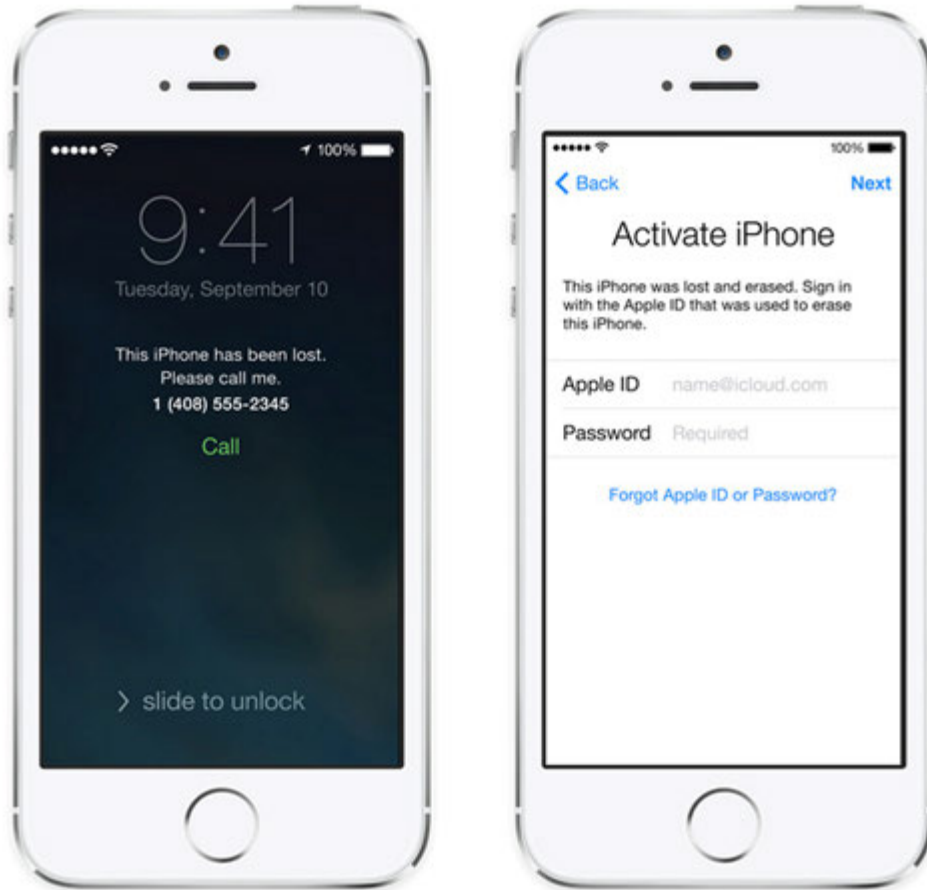
## Touch ID

Though not entirely unexpected, Apple's decision to include a fingerprint reader in the iPhone 5s is generating a lot of discussion. Unlike other fingerprint readers, the iPhone 5s reads your prints from the home button—which every iPhone user presses already. A sapphire lens lets the sensor get a clear image of an inner layer of skin, which Apple says gives it the best view of your loops, arches, and whorls.

In this post-Snowden world, concern about the NSA is rampant but Apple had some soothing words for worry-warts. Apple said fingerprint information would be encrypted and stored on its A7 chip—not on iCloud, and not shared with any third-party apps. Additionally, the *Wall Street Journal* reported (<http://blogs.wsj.com/digits/2013/09/11/apple-new-iphone-not-storing-fingerprints-doesnt-like-sweat/>) that the iPhone 5s wouldn't store images of your fingerprint, but rather "fingerprint data."

A fingerprint reader that people actually use has the potential to change how authentication works in all devices. It's also likely that we'll see other smartphone makers taking an interest in biometric authentication—there's already a device that uses your heart beat (<http://securitywatch.pcmag.com/mobile-security/315428-forget-passwords-nymi-knows-you-by-your-heartbeat>)—which in turn will encourage organizations like banks and retailers to embrace biometrics. If nothing else, it might get that lazy 50 percent of iPhone users to at least lock their phones.

Thankfully, Apple doesn't see fingerprints as the be-all and end-all of authentication on the iPhone 5s. The company told the Wall Street Journal that a special passcode must be used to unlock a rebooted phone or a phone which hasn't been unlocked for 48 hours.

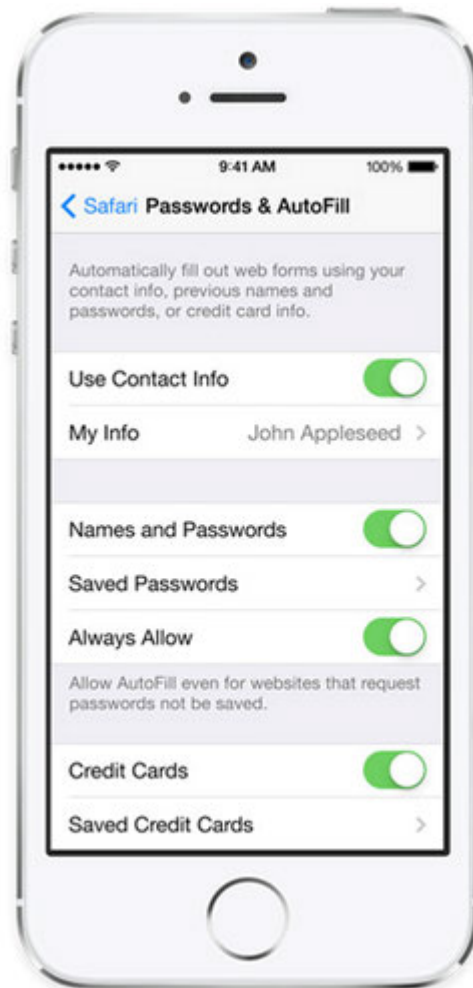


## Find My iPhone Upgraded

Apple beat Android to the punch when it created **Find My iPhone** (<http://www.pcmag.com/article2/0,2817,2422802,00.asp>), a service that can track, lock, and wipe lost or stolen phones. It's an absolutely must-have service for any iPhone user, and Apple is making it even better in iOS 7.

For one thing, deactivating Find My iPhone will require you to enter your Apple ID and password (no word if it will use Fingerprint ID), making it harder for a thief to disconnect you from your device.

But the biggest change is what happens to your iOS device after you wipe it. Right now, wiping your device means ceding it to a thief, sans your data (unless you called your wireless provider first). Not so anymore. "Find My iPhone can also continue to display a custom message," that is, flash on screen a message that you write from another Internet-connected device via your iCloud account, "even after your device is erased," according to Apple's website. "And your Apple ID and password are required before anyone can reactivate it."



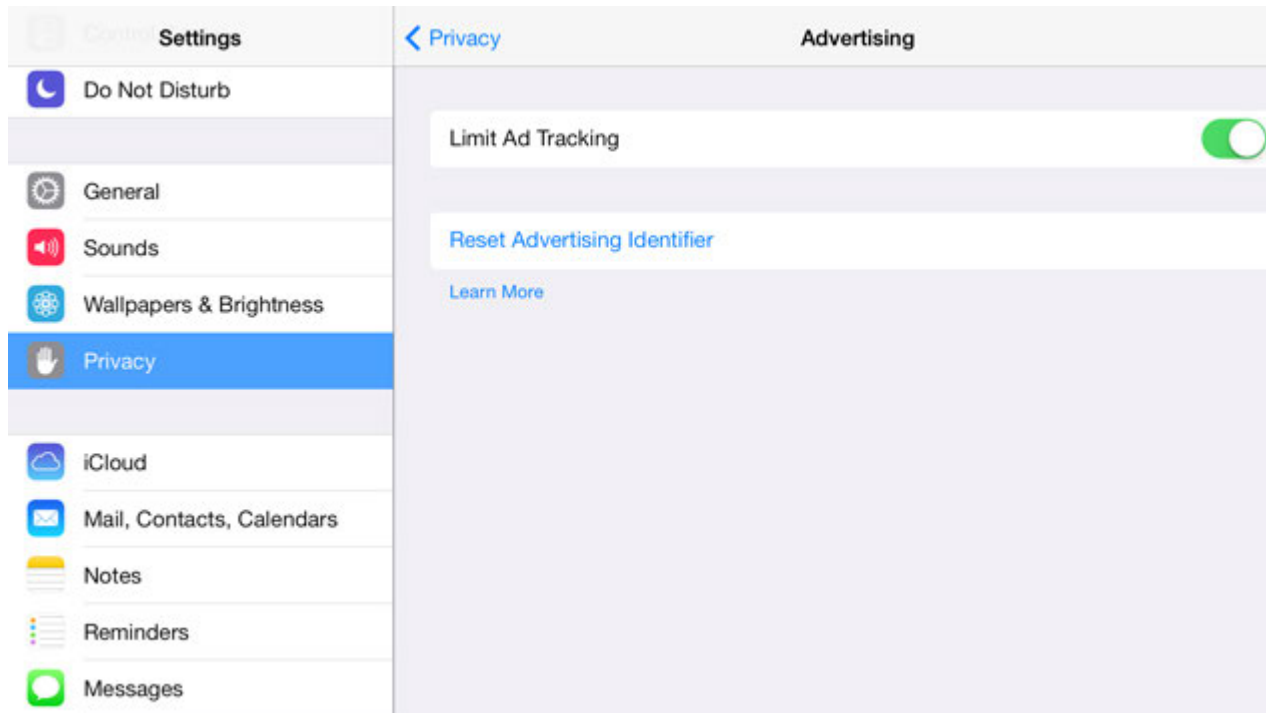
## iCloud Keychain

When we talk about security tips on SecurityWatch, we always tell people to download and use a password manager and call out our Editors' Choice winners LastPass 2.0 and **Dashlane 2.0** (<http://www.pcmag.com/article2/0,2817,2420866,00.asp>). A new feature called iCloud Keychain might mean we have to add one more to that list.

Coming to iOS 7 after the as-yet unannounced launch of the OS X Mavericks, iCloud Keychain is pretty much what the name implies: it stores your Keychain passwords on iCloud, making them accessible to all your iOS and OS X devices. And **not that it matters any more** (<http://securitywatch.pcmag.com/hacking/315668-privacy-is-dead-the-nsa-killed-it-now-what>), but they'll all be secured with 256-bit AES encryption.

Keychain can already capture all your existing passwords, and generate new ones to boot, but they've been locked on whatever device you happen to be using at the time. Now those passwords can be everywhere, and for free. This doesn't quite catch up to the competition since it will be limited to Apple devices but it will be free, (hopefully) seamless, and might encourage Apple users to get smarter about their own password habits.

iCloud Keychain is expected to work with website logins, Wi-Fi passwords, credit cards, and other forms of vital information. We'll see the full extent of the feature once Mavericks launches.

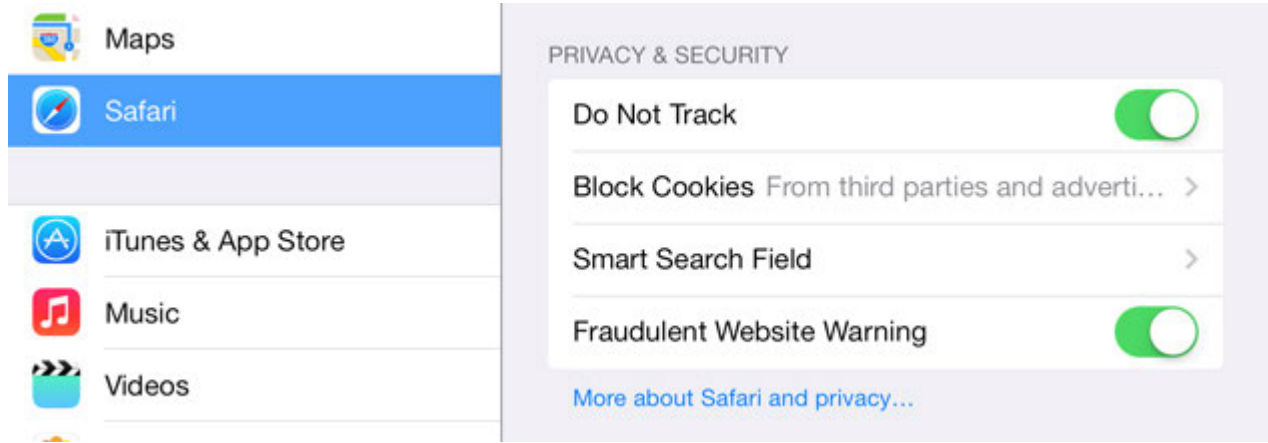


## Privacy on your Phone and on the Web

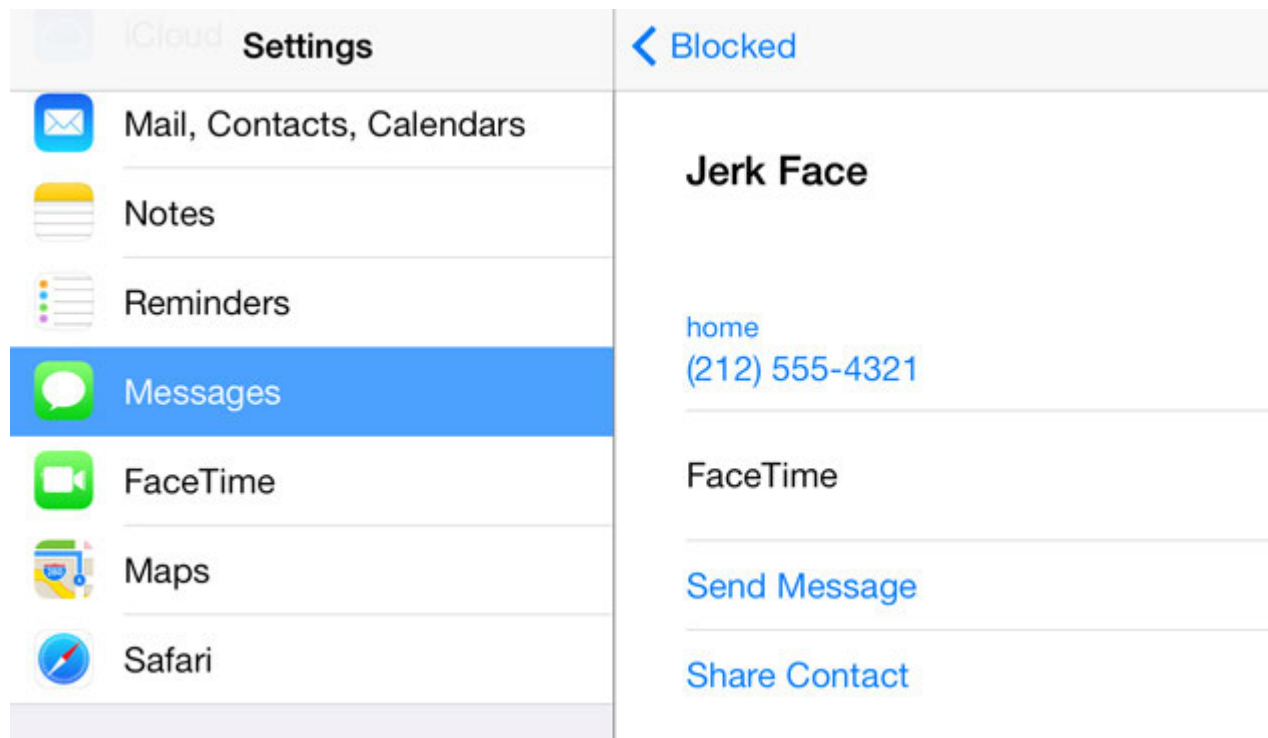
I use both Android and iOS every day, and I much prefer Apple's fine-grained approach to permissions. In iOS 6, you can view the permissions you've granted apps for things like location, and revoke them at any time. In iOS 7, Apple will be giving you even more control, with per-app controls for cellular data usage, microphone access, and camera access.

iOS 7 also comes with a really interesting innovation for how you interact with advertisers. Many free apps are able to make money by including code from ad networks. Sometimes this just puts banner ads in your app, other times the networks might try to **nab your phone number or unique device ID** (<http://securitywatch.pcmag.com/mobile-security/313041-lookout-names-bad-ad-networks-enforces-new-adware-standards>) in order to track your movement between apps.

Apple will soon be introducing an Advertising Identifier, a unique ID assigned to your device that advertisers can query without accessing something more important. And here's the best part: Apple is putting you in control. You'll be able to reset or limit advertisers' access to your ID from you're your iPhone's and iPad's settings.



Beyond your phone, Apple is also adding security and privacy features to mobile Safari as well. In iOS 7, you'll be able to engage a Do Not Track option, which my colleague Jill Duffy believes to be a revamped version of **Private Browsing from iOS 6** (<http://www.pcmag.com/article2/0,2817,2423635,00.asp>). Once engaged, sites which comply with certain standards will not be able to track your movements between websites. It likely wont actively prevent tracking from advertisers who chose not comply, however.



### SMS and Call Blocking, Plus Encryption

Android users have long enjoyed the ability to block calls and SMS using third-party security apps, while only a few iOS developers have tried to work around Apple's tight grip on phone functions. Now, Apple will provide that option in iOS 7.

From the settings, you'll be able to block contacts for calls, messages, and FaceTime interaction. Oddly, Apple hasn't provided a single setting for this feature. Instead, you activate blocking in the settings menu for either Messages or FaceTime and iOS 7 will block interactions in calls, messages, and FaceTime.

iOS 6 users currently enjoy **end-to-end encryption of their text messages** (<http://securitywatch.pcmag.com/security/310015-the-real-reason-the-feds-can-t-read-your-imeessages>) between iOS users, and encrypted FaceTime video chatting as well. iOS 7 will also be adding FaceTime Audio, which lets you make a VoIP call over a data connection. Thankfully, these VoIP calls will also be encrypted, giving you a somewhat more secure way to carry on a conversation.

### Trusted Devices

One of the big revelations at this year's **Black Hat conference** (<http://securitywatch.pcmag.com/security/314586-10-black-hat-hacks-that-will-make-you-put-on-a-tinfoil-hat>) was the Mactans device which could hijack **any iPhone connected via USB** (<http://securitywatch.pcmag.com/hacking/314361-black-hat-don-t-plug-your-phone-into-a-charger-you-don-t-own>). The problem stems from a fundamental issue in



how iOS devices behave when connected to another device via USB. By default, the iOS device would attempt to mount itself as a USB mass storage device, regardless of what was on the other end of the USB cable.

But no more. With iOS 7, you'll be prompted to **authorize whatever computer** (<https://neosmart.net/blog/2013/apple-finally-locks-down-the-usb-port-ios-7/>) you attach to your iPhone. If you don't authorize it, the iPhone treats it like a regular ol' charger and just sucks down some electricity without making itself vulnerable.

Now, clever attackers could get around this with a little bit of social engineering, but it's definitely a step in the right direction.

## **And Beyond**

Apple touted more than 200 new features in iOS 7, and happily it seems that security improvements were among the more noteworthy additions. But there are a lot of small changes that will keep you more secure, too.

For instance, iOS 7 lets you update your apps automatically, so you'll always have the latest and most recently patched version of an app. With more and more attacks going after services, you can bet that this will be critical in the future.

Apple even paid lip service to the issue of malware, acknowledging that mobile malware was a rising problem. However, Apple didn't provide much of a clue as to how it's addressing the issue, saying only, "hardware and firmware features are designed to protect against malware and viruses," whatever that means.

Taken altogether, iOS 7 and the new iPhone 5s are powerful statements from Apple about security. The company is definitely aware of the threats that exist, and seems to have been paying close attention to how threats have developed on the Android operating system. While there are some security issues Apple has yet to address, or address adequately, this is the most we've seen Apple say about mobile security in a long time. iPhone 5s and iOS 7 might just be the most secure offerings from Apple, ever.

# **Exhibit J**



**U.S. Department of Justice**

*United States Attorney  
Eastern District of New York*

F. # 2015R00200

*271 Cadman Plaza East  
Brooklyn, New York 11201*

July 9, 2015

By ECF

The Honorable Sterling Johnson, Jr.  
United States District Judge  
United States District Courthouse  
225 Cadman Plaza East  
Brooklyn, New York 11201

Re: United States v. Adamou Djibo  
Docket No. 15-CR-088 (SJ)

Dear Judge Johnson:

The government respectfully submits this response in opposition to the defendant’s motion to suppress statements and evidence in the above case. As set for more fully below, the defendant’s arguments fail as a matter of law and, accordingly, a suppression hearing is unwarranted. In short, even if the facts alleged in the defendant’s motion are true, there is no basis to suppress either the defendant’s statements or the cellular telephone seized from him on February 3, 2015.

**I. Background**

This is a heroin importation and distribution conspiracy case, in which the defendant was a key member of an international narcotics trafficking organization responsible for importing large amounts of heroin into the United States from Togo. On February 3, 2015, the defendant was arrested at JFK International Airport as he attempted to board a flight out of the United States. The defendant’s flight destination was the United Kingdom, via Amsterdam, although the defendant concedes in his affidavit that his ultimate destination was Togo.

**A. The Border Search**

After checking in for his flight on February 3, 2015 and obtaining his boarding pass, the defendant passed through the TSA security checkpoint and made his way to the boarding gate. At the departure gate, Customs and Boarder Protection (“CBP”) officers selected the defendant for additional screening and conducted an outbound border examination prior to airplane boarding. The CBP officers asked the defendant to step aside from the line of boarding passengers so as not to obstruct the boarding process. The defendant agreed. The CBP officers conducted a border search of the defendant’s carry-on

luggage and other property and located multiple electronic devices and cellular telephones in the defendant's possession, including an Apple iPhone (the "Subject iPhone"). As part of the boarder search, the defendant was asked for and provided the passcode to the Subject iPhone to agents from the Department of Homeland Security, Homeland Security Investigations ("HSI") who were assisting the CBP officers. During this time the defendant was not under arrest and remained in the airport terminal boarding area near the departure gate.

### **B. The Defendant's Arrest**

After CBP officers completed the border search of the defendant's property, the defendant was placed under arrest. He was taken from the boarding gate area to an office elsewhere in the terminal for arrest processing. HSI agents advised the defendant of his Miranda rights, which he invoked. No post-arrest questioning took place.

Due to the late hour, the defendant was taken to the Metropolitan Detention Center in Brooklyn, New York for overnight lodging. He was presented for arraignment the following day in the Eastern District of New York.

On March 5, 2015 a grand jury in the Eastern District of New York returned a four-count indictment charging the defendant with (1) conspiracy to import heroin, in violation of 21 U.S.C. §§ 963 and 960(b)(1)(A); (2) importation of heroin; in violation of 21 U.S.C. §§ 952(a), 960(a)(1) and 960(b)(1)(A); (3) conspiracy to possess heroin with intent to distribute, in violation of 21 U.S.C. §§ 846 and 841(b)(1)(A)(i); and (4) possession of heroin with intent to distribute, in violation of 21 U.S.C. §§ 841(a)(1) and 841(b)(1)(A)(i). See Dkt. No. 6. On July 1, 2015, a grand jury in the Eastern District returned a Superseding Indictment (the "Indictment"), charging the defendant with the same four counts but expanding the date range on the conspiracy counts. See Dkt. No. 22.

On March 3, 2015, the Honorable Ramon E. Reyes, Jr. issued a search warrant for the Subject iPhone.

## **II. There is No Basis to Suppress the Defendant's Statements or his Property because All Were Lawfully Obtained.**

The defendant argues that his border search statements and his physical property seized, including the Subject iPhone and records obtained from it, should be suppressed for three reasons. None are sound.

### **A. The Defendant's Probable Cause Challenges are Unwarranted because Probable Cause is Not Necessary for a Border Search a Grand Jury has Already Returned an Indictment**

First, the defendant argues that his statements and property should be suppressed because "they were the fruits of a warrantless arrest without cause." Mot. at 4. The defendant is wrong. As an initial matter, the defendant's statements and property were obtained pursuant to a border search at the airport boarding gate. "It is well established that

the government has broad powers to conduct searches at the border even where . . . there is no reasonable suspicion that the prospective entrant has committed a crime . . . . Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.” Tabbaa v. Chertoff, 509 F.3d 89, 97-98 (2d Cir. 2007). Accord United States v. Ramsey, 431 U.S. 606, 619 (1977) (routine border searches without a warrant, probable cause or reasonable suspicion deemed “reasonable” in light of government’s interests in protecting its border); United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971) (border searches reasonable because they further the goals of law enforcement). That the defendant was departing the United States rather than arriving into the country is of no matter. The border search exception applies to outbound border searches the same way that it applies to inbound border searches. United States v. Swarovski, 592 F.2d 131, 133 (2d Cir. 1979) (“The warrantless searches of appellant’s luggage as he was about to depart the country did not violate his Fourth Amendment rights.”). As the Second Circuit explained, “that customs officials can make such a search only when the person whose effects are being searched is entering the United States is not the law.” Id. (collecting cases).

Electronic devices, such as Subject iPhone, are equally covered under the border search exception in addition to items like luggage or personal property. See United States v. Irving, 452 F.3d 110, 123-24 (2d Cir. 2006) (“Searches of a person’s luggage or personal belongings are routine searches.”) Searches of computers and other electronic devices such as cellular telephones “are likewise considered routine searches that may be conducted in the absence of reasonable suspicion.” United States v. Young, No. 12-CR-00210-RJA-JJM, 2013 U.S. Dist. LEXIS 33496, at \*5 (W.D.N.Y. Jan. 16, 2013) (citing United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008), cert. denied, 555 U.S. 1176 (2009)). As the Ninth Circuit reasoned, “reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.” Arnold, at 1008. See also United States v. Linarez-Delgado, 259 Fed. Appx. 506, 508, 2007 WL 4525200, \*1 (3d Cir. 2007) (“Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search”).

At the time law enforcement officers conducted the search, the defendant was not under arrest and was lawfully subject to such a search because he had already passed through the TSA security checkpoint and was at the “border” about to board an international flight. Accordingly, probable cause was not needed to stop, question, and search the defendant.

The defendant’s attempt to challenge the basis for his subsequent arrest is also without merit. As set forth more fully in the six-page Complaint, ample probable cause exists for this defendant’s arrest. See Dkt. No. 1. It is not necessary to make a “prima facie showing of criminal activity” or to show that it is more probable than not that a crime occurred. United States v. Cruz, 834 F.2d 47, 50 (2d Cir. 1987). The Complaint more than satisfies this standard. As the Complaint explains, after a drug courier was arrested attempting to enter the United States on a flight from Togo with more than six kilograms of heroin concealed in his suitcase, law enforcement agents seized and searched the courier’s

cellular telephone. Records obtained from that search evidenced this defendant's extensive involvement in the drug smuggling operation and, combined with immigration records, provided overwhelming cause for his arrest. Since then, two different grand juries have agreed there was sufficient probable cause to proceed with this case and returned an indictment and superseding indictment against the defendant. The idea that the sufficiency of the Complaint can be challenged at this stage in proceedings—post-indictment, with overwhelming evidence of the defendant's crimes mounting—is baseless.

The defendant's challenge to the basis for his arrest is no more than a thinly-disguised attempt to preview the government's trial evidence and prematurely obtain § 3500 materials for potential witnesses. These attempts are misguided. The goal of a probable cause standard is not "to finally determine guilt through a weighing of evidence," and the defendant should not be permitted to do so here. Krause v. Bennett, 887 F.2d 362, 372 (2d Cir. 1989). The government has already provided Rule 16 discovery and will provide § 3500 material in a timely fashion before trial. This fishing expedition has no merit and should be rejected.

## **B. The Law Does Not Require Probable Cause for Outbound Border Searches**

Next, the defendant argues that his pre-Miranda statements should be suppressed. Mot. at 5. The law says otherwise. The defendant's pre-Miranda statements were not obtained incident to arrest, but rather in the course of a border search, where the defendant was not "in custody." The over-arching "custody" question for Miranda purposes is whether a reasonable person in a suspect's position would significantly have understood himself to be subjected to restraints comparable to those associated with a formal arrest. United States v. FNU LNU, 653 F.3d 144, 153 (2d Cir. 2011) (denying appeal of motion to suppress statements obtained during border search without Miranda warnings). In FNU LNU, the defendant had been stopped at the border and subjected to an interrogation in a closed room, out of public view, with an armed guard escort, lasting for 90 minutes. Id. The Second Circuit found that even under these circumstances, which are far more severe than even the defendant's own account of his CBP examination, a reasonable defendant could not find what occurred to be "the equivalent of a formal arrest." Id. at 155. The court explained that a reasonable person would consider such an examination "par for the course" when entering the country from abroad. Id.

In the instant case, the defendant was stopped for a routine border examination by CBP officers at the airport boarding gate. He was taken aside from the passenger boarding line, but was not removed from the boarding gate area for the CBP examination. As any reasonable traveler knows, such examinations are "par for the course" when attempting an international departure from a United States airport. See FNU LNU, at 155. There was nothing unusual about questioning the defendant's travel plans, nor was there anything unusual about searching his electronic devices. Young, 2013 U.S. Dist. LEXIS 33496, at \*5 (border searches of electronic devices are "considered routine searches that may be conducted in the absence of reasonable suspicion."). Inquiring about a device's passcode in order to be able to execute that search falls squarely within the routine border search protections and does not violate the defendant's Miranda rights in this case.

### C. The Fruit of the Poisonous Tree Doctrine Does Not Apply to Miranda Violations

The defendant next argues that records obtained from a search of his Subject iPhone should be suppressed as “fruit of the poisonous tree.” Mot. at 6. This ignores well-settled Supreme Court precedent that the Miranda rule “does not require that the statements taken without complying with the rule and their fruits be discarded as inherently tainted.” United States v. Patane, 542 U.S. 630, 639 (2004) (internal citations and quotations omitted) (holding that physical evidence obtained as a result of unwarned statements is not excluded by Miranda). That is because the Fifth Amendment only proscribes “extract[ing] from the person's own lips an admission of guilt, which would thus take the place of other evidence.” Id. at 637. “The Miranda presumption of coercion,” however, “has not barred the use of unwarned, voluntary statements . . . to locate non-testimonial evidence . . .” United States v. Morales, 788 F.2d 883, 886 (2d Cir. 1986). Indeed, “[a]n interrogating officer's failure to advise a suspect of his Miranda rights does not require suppression of the physical fruits of the suspect's unwarned statements.” United States v. Capers, 627 F.3d 470, 493-494 (2d Cir. 2010).

Here, the Subject iPhone’s records were created by the defendant before the involvement of law enforcement and therefore does not contain “compelled testimonial evidence.” Flynn v. James, 513 Fed. Appx. 37, 40 (2d Cir. 2013) (holding statements on a cassette tape seized from the defendant were admissible and did not violate Miranda because they were created voluntarily before police involvement). Moreover, the Subject iPhone search was conducted only after obtaining a search warrant from a magistrate judge, adding an additional layer of protection against unwarranted intrusion into the device’s contents. Accordingly, even if the defendant’s statements, including the Subject iPhone passcode, were obtained in violation of Miranda, the fruits of the Subject iPhone search are not tainted and should not be suppressed.

### III. The Subject iPhone Records Would Have been Inevitably Discovered

The government maintains that the Subject iPhone passcode was lawfully obtained pursuant to a border search and that, even if a Miranda violation did occur, the subsequent search of the device was not tainted. But even if the Court finds otherwise and suppresses the defendant’s statement providing the passcode to unlock the Subject iPhone, the lack of a passcode is not fatal to the government’s ability to obtain the records. That is because HSI is in possession of technology that would allow its forensic technicians to override the passcode security feature on the Subject iPhone and obtain the data contained therein. In other words, even if HSI agents did not have the defendant’s passcode, they would nevertheless have been able to obtain the records stored in the Subject iPhone using specialized software. The software works to bypass the passcode entry requirement and “unlock” the cellular telephone without having to enter the code. Once the device is “unlocked” all records in it can be accessed and copied.

For all of the above reasons, the Court should deny the defendant's motion to suppress statements and physical evidence seized at the airport on February 3, 2015.

Respectfully submitted,

KELLY T. CURRIE  
Acting United States Attorney

By: /s/ Karen L. Koniuszy  
Karen L. Koniuszy  
Assistant U.S. Attorney  
(718) 254-6072

cc: Zachery Margulis-Ohnuma, Esq. (via ECF)  
Clerk of the Court (SJ) (via ECF)



# **Exhibit K**

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA,	:	15-CR-00088(SJ)
	:	
	:	
-against-	:	United States Courthouse
	:	Brooklyn, New York
	:	
	:	Thursday, September 3, 2015
ADAMOU DJIBO,	:	9:30 a.m.
	:	
Defendant.	:	

- - - - - X

TRANSCRIPT OF CRIMINAL CAUSE FOR HEARING  
BEFORE THE HONORABLE STERLING JOHNSON, JR.  
UNITED STATES SENIOR DISTRICT JUDGE

A P P E A R A N C E S:

For the Government: KELLY T. CURRIE, ESQ.  
 United States Attorney  
 Eastern District of New York  
 271 Cadman Plaza East  
 Brooklyn, New York 11201  
 BY: KAREN L. KONIUSZY, ESQ.  
 Assistant United States Attorney

For the Defendant: LAW OFFICE OF ZACHARY MARGULIS-OHNUMA  
 260 Madison Avenue  
 18th Floor  
 New York, New York 10016  
 BY: ZACHARY MARGULIS-OHNUMA, ESQ.

Court Reporter: VICTORIA A. TORRES BUTLER, CRR  
 225 Cadman Plaza East/Brooklyn, NY 11201  
 VButlerRPR@aol.com

Proceedings recorded by mechanical stenography, transcript produced by Computer-Aided Transcription.

1 (In open court.)

2 (Judge STERLING JOHNSON, JR. is in the courtroom.)

3 THE COURTROOM DEPUTY: U.S. versus Djibo.

4 THE COURT: We have your guy on the stand?

5 MS. KONIUSZY: Yes. Last time we were here, one  
6 month ago for the second appearance, the defense expert  
7 testified. His direct exam lasted approximately ten minutes  
8 and defense counsel was unprepared to cross him at that time,  
9 asked for Your Honor to give him another opportunity to come  
10 back, said he needed time to consult with his own witnesses,  
11 and we scheduled today's date specifically for the purposes of  
12 giving him an opportunity to prepare cross and also today was  
13 the date that he was told to bring any witnesses that he had.  
14 They were supposed to testify today.

15 This is our third appearance on this suppression  
16 hearing. This has been going since early July.

17 THE COURT: I am aware. I have been here.

18 MS. KONIUSZY: Thank you.

19 THE COURT: Put your guy on the stand.

20 MS. KONIUSZY: The Government calls Special Agent  
21 David Bauer, B-A-U-E-R.

22 THE COURT: You are still under oath, you remember  
23 that?

24 THE WITNESS: Yes.

25 MR. MARGULIS-OHNUMA: May I inquire?

1 THE COURT: You may.

2 CROSS EXAMINATION

3 BY MR. MARGULIS-OHNUMA:

4 Q Have you and I ever spoken before?

5 A We have not.

6 Q You are -- testified last time that you were an expert  
7 in, I think the field was forensic computers?

8 THE COURT: No, he did not testify as an expert. I  
9 qualified him as an expert.

10 MR. MARGULIS-OHNUMA: Forgive me, Your Honor.

11 Q Let me ask you a little bit about your qualifications as  
12 a forensic computer examiner. Am I saying that right?

13 A Sure.

14 Q You do not have any certifications in that field; is that  
15 correct?

16 A That's not.

17 Q What certifications do you have, sir?

18 A I believe I mentioned on the resume that I provided. I  
19 don't keep them all current, although I've had an IACIS  
20 certification, which is a certification offered by one of the  
21 vendors that manufactures one of the suites we use, very  
22 commonly used.

23 I've also held A plus certification in the past and  
24 still do, which is computer hardware-software. Number other  
25 ones I'm trying to think of. BlackBag Technologies is a

1 company that offers certification in a product called  
2 BlackLight, which is something we commonly use with Apple  
3 devices.

4 Q Sir, am I correct that those are all certifications on  
5 particular software or hardware devices; right?

6 A So far that I've mentioned, yes.

7 Q And those are offered by the manufacturers of those  
8 devices; correct?

9 A With the exception of the A plus certification. There  
10 are others that I am trying to --

11 THE COURT: You talk too fast.

12 THE WITNESS: Okay.

13 Q The A plus certification you ask guy in July of 2003;  
14 correct?

15 A That's correct.

16 Q Have you renewed that since?

17 A That is actually a permanent certification or at least it  
18 was at that time.

19 Q But it's based on the information technology as of that  
20 time in 2003; correct?

21 A Actually, let me correct myself. As part of the program  
22 that I went through in my general forensic training, that  
23 certification is a particular requirement. So although I was  
24 not required to test for it, because I had already gotten the  
25 certification, I actually went through the training again also

1 in 2012.

2 Q Okay. And that is generally on computer hardware and  
3 software; correct?

4 A That's correct.

5 Q Now aside from that, would you agree with me that the  
6 leading certification in this field is offered by, not by a  
7 manufacturer, but by the International Society of Forensic  
8 Computer Examiners?

9 A There are actually a quite a number of credentials out  
10 there so I would not agree to any one in particular. I think  
11 they all offer some benefit, but, no, I would not.

12 Q But you don't have any -- you haven't been recently  
13 certified in any general certification as opposed to one that  
14 is for a particular platform; correct?

15 A Actually, just in July I went through a program which is  
16 called advanced computer evidence recovery training. It was  
17 offered at the Federal Law Enforcement Training Center.

18 THE COURT: In Glynco?

19 THE WITNESS: Exactly.

20 A And that is a program offered about once a year to us, so  
21 that covers a pretty broad base of topics.

22 Q And that's training but that's not a certification;  
23 correct?

24 A That's correct, although there are some practicals  
25 involved, which are pass/fail.

1 Q And, in fact, with respect to the BlackLight  
2 certification you mentioned, there's actually two levels of  
3 BlackLight certification that are available; am I correct  
4 about that?

5 A The only one that I am aware of is the CBE certification  
6 which is Certified BlackLight Examiner.

7 Q Right. Let me hand you, I'll mark it for identification  
8 as Defendant's Exhibit B, and see if that refreshes your  
9 recollection at all.

10 THE COURT: Sustained. Did not say recollection  
11 needed refreshing.

12 MR. MARGULIS-OHNUMA: Okay.

13 Q Is there anything -- withdrawn.

14 As an expert in the field of forensic analysis, you  
15 keep up to date generally on what certifications are  
16 available; correct?

17 A I do.

18 Q Okay. So is there anything that might help reflect your  
19 recollection as to the two different certifications that  
20 BlackBag Technologies offers?

21 A No, not particularly.

22 MR. MARGULIS-OHNUMA: Your Honor, I do not, because  
23 of the situation with our expert, I'm not sure I am going to  
24 have my own witness to offer this. I would like to show it to  
25 him and ask him if it is the sort of thing that he, as on

Bauer - cross - Margulis-Ohnuma

7

1 expert in the field, relies on. It is, and I will proffer  
2 from the BlackBag Technologies's website and reveal that  
3 there's two different certifications, one for certified  
4 BlackLight examiner and one specific to IOS certified  
5 forensic --

6 MS. KONIUSZY: I object to this.

7 THE COURT: I am going sustain and you are  
8 testifying yourself.

9 MR. MARGULIS-OHNUMA: Sorry. I didn't understand  
10 what the objection was to.

11 THE COURT: You are testifying. You were not asking  
12 a question. You have to ask a question of the witness.

13 MR. MARGULIS-OHNUMA: Right. I would like to ask  
14 permission to show him the BlackBag Technologies's website and  
15 see if he can comment on it.

16 THE COURT: Comment on it? Go ahead, show it to  
17 him.

18 MR. MARGULIS-OHNUMA: That's marked for  
19 identification as Defense Exhibit B.

20 MS. KONIUSZY: We never received copies of any of  
21 this in advance. I don't know what this is. We would like a  
22 copy of our own Exhibit --

23 THE COURT: He is showing it to you. It is not in  
24 evidence.

25 (Pause in the proceedings.)



1 A Thank you. Okay.

2 Q Sir, after looking at Defense Exhibit B, does that in any  
3 way help you understand that there's also a more particular,  
4 more advanced, certification for BlackLight on IOS-specific  
5 devices?

6 A Let me just look again, if you would.

7 I can see that there are two certifications offered,  
8 yes. I have the former and not the latter. I'm not sure how  
9 it's relevant to this particular matter because this software  
10 wasn't used in this particular case, but there are a lot of  
11 manufacturers that offer a lot of different certifications and  
12 while --

13 THE COURT: We have a court reporter here, have  
14 mercy.

15 THE WITNESS: Okay. Sorry about that.

16 A There are a lot manufacturers that offer a lot of  
17 different certifications and while I keep tabs on most of  
18 them, or as many as them as possible, I certainly am not aware  
19 of them all.

20 Q Is the reason for that because you're more of a  
21 generalist, you don't -- your expertise is not specific to  
22 IOS, like that particular certification is; is that right?

23 A I wouldn't say that I'm a specialist in any one area, so  
24 that's a fair question, sure.

25 Q So, let's talk about what you relied on and reviewed in

1 preparing for you testimony in this proceeding.

2 What can you -- can you just go over with us, what  
3 did you look at to prepare for this?

4 A I consulted with other examiners that have some  
5 experience with the particular device in question. I read a  
6 technical --

7 Q Let me stop you there. Experience with which device?

8 A Well, I believe the device in question here is the IP-BOX  
9 that was referenced in my earlier testimony.

10 Q So was it -- was your testimony actually based on --  
11 withdrawn.

12 Did you have any experience yourself with IP-BOX  
13 prior to preparing for this proceeding?

14 A I did.

15 Q What else did you rely on?

16 THE COURT: Just a second. How many versions of the  
17 IP-BOX are there?

18 THE WITNESS: Well, it's actually a piece of  
19 hardware and there are different versions of software that you  
20 can update the hardware with. To my knowledge, there's three  
21 different versions and they built on the previous one.

22 THE COURT: Okay.

23 Q What else did you look at or what else did you do to  
24 prepare?

25 A I believe I mentioned consultation with other examiners.

1 There is a single technical paper out there that I am aware  
2 of, which I have also read, and I've also done some my own  
3 testing.

4 Q What's that single technical paper?

5 A I don't recall the exact title off the top of my head,  
6 but it's something to effect of IP-BOX breaking simple pass  
7 codes on IOS devices.

8 THE COURT: Just a second.

9 The phone that you worked on, what was the operating  
10 system for that phone, do you know?

11 THE WITNESS: I do. All Apple iPhones use what they  
12 call IOS.

13 THE COURT: What is the version of the IOS?

14 THE WITNESS: It was 8.1.2.

15 THE COURT: 8.1.2, okay.

16 MR. MARGULIS-OHNUMA: Your Honor, I'll get right to  
17 it. Obviously you're ahead me.

18 Q And according to the published literature, IP-BOX  
19 requires an adapter to work with anything higher than 8.0.0;  
20 correct?

21 A Actually, I believe it's 8.1.1, but there is an adapter;  
22 that's correct.

23 Q Right. And according to the published literature, it  
24 actually does not, is not compatible with 8.1.2; isn't that a  
25 fact?

1 A Actually, no, that is not a fact. The published  
2 literature, and again the only document that I see available,  
3 says that it should, in fact, work.

4 Q And that's a document by a police officer -- withdrawn.

5 Can you produce that? Do you have that?

6 A I don't have it with me, but I can certainly produce it  
7 for you.

8 MR. MARGULIS-OHNUMA: I would ask for production of  
9 that since he relied on it for his opinion.

10 Q You said you did testing of your own; right?

11 A I have.

12 Q And did you test on Mr. Djibo's iPhone?

13 A I did not.

14 Q So, you don't know whether it would actually work on  
15 Mr. Djibo's iPhone or not, because you didn't test it; right?

16 A Well, actually, I would not have had the opportunity to  
17 test it on his iPhone because, as it was presented to me, it  
18 is already unlocked. That is first.

19 Secondly --

20 Q Wait. Can I stop you right there? Let's break that down  
21 a little bit.

22 When you say it was unlocked, you mean the pass code  
23 had been removed by somebody?

24 A I believe that's the case, yes.

25 Q Do you know who removed the pass code?

1 A I don't.

2 Q But you have the pass code for Mr. Djibo's iPhone; right?

3 A Yes. Either it was given to me, or it was presented in  
4 an unlocked form. But either way, I wouldn't modify the phone  
5 in order to test it. I wouldn't change the pass code and  
6 modify evidence. So that was really the other reason I was  
7 getting to.

8 Q But you are saying somebody did before you got the phone,  
9 somebody modified it to remove that pass code, so it was  
10 unlocked when you got it. Is that what --

11 A I understand it --

12 MS. KONIUSZY: Objection.

13 THE COURT: What is the objection?

14 MS. KONIUSZY: It's a compound question.

15 THE COURT: Did you understand the question?

16 THE WITNESS: I did.

17 THE COURT: Overruled.

18 A I'm saying that it was either unlocked when presented to  
19 me, or I was presented the phone with the pass code. In  
20 either case, I could access the contents of the phone.

21 Q Okay. You just don't remember either way?

22 A Correct.

23 Q Okay. So, there's nothing about that that would in any  
24 way have prevented from you testing IP-BOX on that phone;  
25 right?

1 A Well, you wouldn't do that because, for me to do that,  
2 for me to test the phone, I would have to re-enable the  
3 security settings in the device that would require a pass  
4 code, which would modify the contents of that device.

5 You just wouldn't do that. That's just not  
6 forensically sound.

7 Q Okay. But you don't remember if that was the situation;  
8 right?

9 A What I'm saying is, I wouldn't have tested it either way  
10 in that fashion.

11 Q I'm going to ask you -- I am going to have to strike that  
12 answer and ask you not to speculate as to what happened. I  
13 want to just know what you remember or don't remember.

14 Okay. So if you can just let us know if you don't  
15 remember, can you do that?

16 A I'm sorry. I don't understand the question.

17 Q All right. You don't -- what I think you testified to,  
18 tell me if this is correct, is that you don't remember whether  
19 it came to you unlocked with the pass code removed --

20 THE COURT: Asked and answered. Asked and answered.

21 MR. MARGULIS-OHNUMA: Okay.

22 Q Again, I'm trying to understand why you didn't test the  
23 phone. It had nothing to do with whether or not it was  
24 unlocked; correct?

25 A May I explain?

1 Q Sure.

2 A Okay. You would not modify a person's phone in any way,  
3 which you would be doing if you were to re-enable the pass  
4 code on the phone. I wouldn't make changes to a user's  
5 device, because if I were to do that, I would be modifying  
6 evidence. I am not willing to do that.

7 As far as testing a phone in that particular  
8 configuration, you are correct, that I can't do that simple  
9 because I don't have an exemplar phone, i.e, a nonevidentiary  
10 device that is an iPhone 5 running that particular version of  
11 the software.

12 What I can tell you are two things: One, I have  
13 spoken with other examiners who have actually broken pass  
14 codes on phones that have operating systems that are more  
15 recent than this particular version that we are talking about  
16 in your client's phone. Those versions would arguably be more  
17 secure and more difficult to break into. So I have that.

18 The other thing is, there's actually some new  
19 information that's been released since my last testimony that  
20 would have also provided another option to get into this  
21 phone, which we just found out about recently.

22 Q Okay. Sorry, there was a lot there and I want to try to  
23 break it down.

24 A Sure.

25 Q So if I understood your answer, Agent Bauer, directly at

1 the beginning I think you said that you wouldn't have done the  
2 testing because that could have somehow affected the evidence,  
3 it could have spoliated the evidence; is that correct?

4 A I would not have done the testing on this particular  
5 phone; that's correct.

6 Q Because that phone cause evidentiary; right?

7 A Correct.

8 Q And then you said that you spoke to others who have  
9 successively broken into other iPhones; is that correct?

10 A That's correct.

11 Q Who are those people you spoke to?

12 A I don't recall the names offhand, but they are other  
13 examiners like myself.

14 Q Okay. And did they demonstrate -- withdrawn.

15 Did they say that they had used IP-BOX to do that?

16 A Yeah, I can recall specifically that one was able to  
17 access a device running version 8.1.3. I believe that was on  
18 an iPhone 4s.

19 Also, another that was able to access a phone  
20 running the current version 8.4, or the current major version,  
21 at least.

22 Q So, the first person you spoke to, you can't remember  
23 that person's name?

24 A No, I do not, not offhand.

25 Q Was that a Government employee?



1 A Not a Federal Government employee. It was a local law  
2 enforcement person.

3 Q And did they show you that or how did you --

4 A No, this was not a local person.

5 Q Was that person a certified forensic examiner?

6 A I don't know. They were in a computer forensics division  
7 of some sort, but I don't have their exact credentials.

8 Q And -- sorry.

9 As an expert in the field, do you typically rely --  
10 withdrawn.

11 And then someone else told that you they used --  
12 sorry -- that they were able to break into 8.4; is that right?

13 A That's correct.

14 Q And what kind phone was that on?

15 A That was on an iPhone 5s, I believe.

16 Q That's a more advanced phone than the iPhone 5 here;  
17 right?

18 A Correct.

19 Q And the first one you said was actually less advanced  
20 hardware than the 5, right, 4s?

21 A The 4s precedes the 5; that's correct.

22 Q So in both cases they are different configurations from  
23 the phone here; right?

24 A Well, yes, that's correct. And you will find --

25 Q You've answered the question.

1 A Okay.

2 Q So, with the second person, what was that person's name?

3 A I don't have names offhand, I'm sorry.

4 Q Was that person a U.S. Government employee?

5 A Not Federal Government, no. I believe this person worked  
6 for a prosecutor's office. Actually, I know they did.

7 Q Which office was that?

8 A Local, I believe, Bergen County.

9 Q New Jersey?

10 A Correct.

11 Q Now, have you yourself ever broken into a phone with  
12 IP-BOX?

13 A I have.

14 Q What version was that phone running?

15 A I believe an iPhone 4s running 7.0.something. I'm not  
16 sure the exact version. It clearly works on IOS 7 devices.

17 Q In preparing for today's testimony, did you look around a  
18 little for websites regarding IP-BOX?

19 A Sure.

20 Q And did you see any website by the manufacturer of  
21 IP-BOX?

22 A It's not a company that makes the box, so, no.

23 Q Well, if it's not a company, who makes the box?

24 A It's actually made in China by a single individual. It's  
25 not a forensic tool.

1 Q What do you mean it's not a forensic tool?

2 A I mean it's not designed with forensic purposes in mind.  
3 It's, probably my best description of it, honestly, would be  
4 that it's a hacking tool.

5 Q And, in fact, it sends some of the data back and forth to  
6 China that it obtains; right?

7 A I can't answer that question.

8 Q In order to use it, let's just go through a little bit  
9 about how to use it.

10 You have to take the iPhone and pull off the screen;  
11 right?

12 A That's not correct, no.

13 Q How do you use the version you are familiar with?

14 A Well, there's a couple different ways you can use it, but  
15 basically the way the device works is it connects to the  
16 phone, and as I think I described earlier, it attempts  
17 guesses --

18 Q Let me step you through it.

19 MS. KONIUSZY: Objection.

20 THE COURT: Sustained. You ask him a question then  
21 you interrupt him. Sustained.

22 A Okay. So, the device queries the phone with different  
23 numbers using a simple pass code, i.e., 0000 through 9999, and  
24 what will happen when you successfully enter the pass code on  
25 most iPhones is that you will get a change in the color, or

1 rather the light. The screen contrast will change and you  
2 actually are affixing a small light sensor to the surface of  
3 that phone, not taking the screen off. You're simply affixing  
4 the sensor to the surface of the phone.

5 When correct the guess is made, the sensor detects  
6 the change in light, and basically, that's where the system  
7 stops and the correct pass code is recorded.

8 Q Now, let's go back to the iPhone itself and how it works.  
9 Every time you enter a pass code incorrectly, something  
10 changes on the phone itself; correct?

11 A Ah --

12 Q It's a yes or no answer. I'll try step you through  
13 quickly.

14 A The phone will flicker a bit. In some versions basically  
15 the numbers will shake slightly to let you know you've guessed  
16 incorrectly.

17 Q Right. But the phone itself records the incorrect guess;  
18 correct?

19 A In some cases, yes, and in some, no.

20 Q Okay. On the iPhone -- on an iPhone 5 running 8.1.2, the  
21 to be records the guess as the security password; correct?

22 A That's correct.

23 Q So, I'm only going to talk about 8.1.2 on an iPhone 5; is  
24 that okay?

25 A Sure.

1 Q So, on that particular device, every time you guess, it  
2 records the guess and it then increases the length of time  
3 before it will respond to the next guess as a security  
4 measure; is that correct?

5 A Somewhat, but it's not quite correct.

6 Q Tell me what's not correct.

7 A Basically, you're allowed five guesses, beginning with  
8 8.1.1. Need to tell you.

9 From that point forward, you're correct in that  
10 there's a time penalty that begins to be assessed. It will  
11 lock you out for a temporary period.

12 As you continue up the ladder with the number of  
13 incorrect guesses, that time penalty will increase and  
14 eventually you get to the point where you can be essentially  
15 locked out, although it's not a permanent thing. So I think  
16 that's what you're referring to?

17 Q Yes. It's not a permanent thing, but I think you told us  
18 in your direct testimony you can be locked out for 43 years?

19 A There is a phone on my desk that has that situation or  
20 something similar; correct.

21 Q There's also a setting that the user can set where it  
22 automatically wipes the phone after ten incorrect guesses;  
23 correct?

24 A That's correct.

25 Q And the purpose, the point of IP-BOX is to get around

1 that system you just described; isn't that right?

2 A It gets around one of them.

3 Q How is that? Explain that to me.

4 A Actually, I should probably correct that.

5 The adapter you mentioned, and I'm talking now  
6 specifically about the temporarily getting locked out thing we  
7 just discussed, the adapter will basically connect to the  
8 phone and reboot the phone after a certain number of tries,  
9 essentially wiping the slate clean, so to speak. So, that  
10 that process can continue without the time penalty being  
11 assessed.

12 Q All right. And the adapter I mentioned does that by  
13 killing the power to the battery prior to it writing the  
14 information to the flash memory, which is static; is that  
15 correct?

16 A Essentially that's correct.

17 Q Let me break that down. It's a little confusing.

18 The iPhone has system memory and flash memory.  
19 Those are two different things; correct?

20 A All of the memory on the iPhone is flash memory, to my  
21 knowledge, but there are different partitions of memory;  
22 that's correct.

23 Q Which processor does this phone run?

24 A I don't know offhand.

25 Q Okay. Well, it's the A7 or the A8, I think; isn't that

1 right?

2 A I don't know offhand.

3 Q That processor itself has its own internal memory;  
4 correct?

5 A Yes.

6 Q Okay. And when you put in an incorrect password, the  
7 fact that you did that is written to the processor's memory,  
8 starting in 8.11; is that correct?

9 A That's correct.

10 Q And in that way the device you're talking about can't  
11 defeat that unless it somehow cuts the power, because the  
12 phone remembers that you have put in that number of password  
13 attempts; isn't that correct?

14 A I'm not quite sure I understand the question. Could you  
15 repeat that, please?

16 Q Yeah.

17 In order for IP-BOX to work it has to interrupt --  
18 I'm not repeating it. I'm trying to rephrase.

19 A That's fine.

20 Q In order for IP-BOX to work, it has to interrupt the  
21 phone's automatic writing of the fact that you entered an  
22 incorrect password; isn't that correct?

23 A I didn't design the box. I do know that the adapter has  
24 to physically be attached to the phone with the cover off. So  
25 you're basically connecting it directly to the battery, and

1 the reason for that is because it is cutting power, and  
2 rebooting the phone essentially wiping that slate clean, as I  
3 just described.

4 So, that's the reason that it's able to circumvent  
5 the penalty you begin to incur after five wrong guesses.

6 Q So, for this particular phone, you do need to take the  
7 cover off to use that adapter, don't you?

8 A Correct.

9 Q And by the cover, you mean the actual screen; right?

10 A No. I mean the back cover.

11 Q But that separates the back from the screen, does it not?

12 A Actually, the back cover comes off quite easily on  
13 iPhones. You remove two screws, slide it off, you have direct  
14 access to the battery. The screen remains intact.

15 Q Okay. But, so you would have had to open it up in order  
16 to attach the adapter; right?

17 A Yes.

18 Q And in opening it up, there is some risk, is there not,  
19 of damaging the hardware?

20 A I've never opened a phone and damaged it, but I'm sure  
21 you could incur some form of risk in anything you do.

22 Q Have you used the IP-BOX with this particular adapter  
23 we've been talking about?

24 A I have not. And again, that's because I don't have a  
25 device that I can test it on.



1 Q And you would agree that the IP-BOX, without the adapter,  
2 wouldn't work for this phone higher than IOS 8; correct?

3 A Actually, I haven't verified this independently, but no,  
4 I would not, because again, in my discussion with other  
5 examiners, I have actually, specifically the one I mentioned  
6 that was able to bypass version 8.4, this person apparently  
7 got into a phone running 8.4 without the adapter.

8 This is not an exact science.

9 Q But you don't remember that person's name; right?

10 A Offhand, I don't.

11 Q Now, what is the, if not the manufacturer, what are the  
12 seller's claim when they sell the adapter?

13 THE COURT: Where are we going with this line of  
14 questioning?

15 MR. MARGULIS-OHNUMA: Whether it was compatible with  
16 8.1.2, with this phone or not.

17 I realize he just said based on some discussions in  
18 his community that he thinks it is, but, I mean, I have a  
19 website right here that says it's not. And I have an expert  
20 prepared to testify it's not.

21 So I want to ask him about that and see if maybe he  
22 can harmonize it.

23 THE COURT: Well, you have an expert who says that  
24 it is and you have a piece of paper that says it is not.

25 MR. MARGULIS-OHNUMA: Right. I'd like to confront

1 him with the piece of paper.

2 THE COURT: You have already done that.

3 MR. MARGULIS-OHNUMA: This is a different piece of  
4 paper.

5 THE COURT: Let's wind it up.

6 MR. MARGULIS-OHNUMA: I have nothing further except  
7 to confront him with this, Your Honor.

8 THE COURT: Have you confronted him with it?

9 MR. MARGULIS-OHNUMA: No, I have not.

10 THE COURT: Confront him then.

11 MR. MARGULIS-OHNUMA: I'll give a copy to the  
12 Government, just so I'm ready.

13 So I've marked as Defendant's Exhibit A for  
14 identification a printout of a website entitled GSM Server  
15 that purports to sell IP-BOX adapter for IOS 8.

16 BY MR. MARGULIS-OHNUMA:

17 Q You want to take a look at that, sir?

18 A Sure. Yes, I have seen it.

19 Q And so you are familiar with this one?

20 A I am.

21 Q Okay. And would you agree with me -- actually, is this  
22 -- these claims by sellers are the kind of thing that you rely  
23 on to form your opinion; isn't it?

24 A No, not necessarily.

25 Q You don't rely on claims by sellers?

1 A I would certainly consider them, but I don't rely on  
2 them. To the best of my ability, I do my own testing.  
3 Obviously, I am limited in that ability here.

4 I'm aware that this paper you're presenting me with  
5 says that it's supported in certain versions and not in  
6 others.

7 I am also aware that only company that I'm aware of  
8 that sells the adapter --

9 THE COURT: Just a second. Have you marked that as  
10 an exhibit?

11 MR. MARGULIS-OHNUMA: Yes, Defendant's Exhibit A.  
12 Since he's familiar with it, I would like to move it into  
13 evidence, Your Honor.

14 THE COURT: And just Defendant's Exhibit A?

15 MR. MARGULIS-OHNUMA: Correct. I'll give a copy to  
16 the Court.

17 THE COURT: Have you seen it, Counsel?

18 MS. KONIUSZY: We're just looking at it now.

19 MR. MARGULIS-OHNUMA: Sorry, did the Court have a  
20 question?

21 THE COURT: No, I am waiting for an objection.  
22 Do you have any objection to it?

23 MS. KONIUSZY: Yes, Your Honor. We don't have a  
24 problem with him questioning the witness on it, but we object  
25 to moving it into evidence. This isn't even a complete

1 document. It's only a fragment of the print-off. It  
2 certainly doesn't encapsulate the full website. Even the page  
3 that --

4 THE COURT: Sustained.

5 MS. KONIUSZY: Thank you.

6 BY MR. MARGULIS-OHNUMA:

7 Q Is this one of the -- this is one of the things that you  
8 reviewed; correct, sir?

9 A In some form, yes. I've seen this in different areas,  
10 but yes, that's correct.

11 Q And when you say this advertisement for the device is  
12 very specific that it is not compatible with anything higher  
13 than 8.1.0; correct?

14 A I understand -- excuse me.

15 That's correct that that's what it said here, yes.

16 Q Okay. And the phone that you examined that you claim you  
17 could have gotten to, was higher than 8.1.1; correct?

18 A Yes.

19 MR. MARGULIS-OHNUMA: Nothing further for this  
20 witness, Judge.

21 THE COURT: Any redirect?

22 MS. KONIUSZY: Very briefly, Your Honor.

23 REDIRECT EXAMINATION

24 BY MS. KONIUSZY:

25 Q Special Agent Bauer, I believe on cross you were asked

1 what the basis was for your conclusions, and you had started  
2 to name a number different sources that you had consulted.

3 Do you recall that?

4 A Yes.

5 Q I think you got cut off before you finished.

6 In addition to the consultation with other examiners  
7 and the paper you mentioned, and your own testing, did you  
8 consult with anyone else about the IP-BOX?

9 A I consulted with the author of the only technical paper  
10 I'm aware of, which is the one I mentioned.

11 Q And did you consult specifically about the iPhone 5  
12 running the IOS 8.1.2 version?

13 A I did.

14 Q And was there anyone else that you discussed the specific  
15 capabilities of the IP-BOX with respect to the defendant's  
16 specific phone?

17 A Other than the two examiners that I mentioned earlier,  
18 no, but those 3 combined, yes.

19 Q And you said you conducted your own testing as well?

20 A I did.

21 Q And that was on an iPhone device; correct?

22 A That's correct. And in terms of real world devices, I've  
23 had success with one. I've also done and had some success  
24 with other exemplar devices. Again, we are pretty limited by  
25 the pool of what we have available. But I've had some varied

1 success in that regard as well.

2 Q And based on the collective results of all of your  
3 research and all of your own testing, in your expert opinion  
4 would this defendant's iPhone be able to be cracked, using the  
5 IP-BOX?

6 A Yes. It could be done and it actually has been done,  
7 apparently, from other examiners.

8 I've also seen videos of it being done online,  
9 although I'm pretty reluctant to cite YouTube video, I have  
10 seen it, and that's about it.

11 MS. KONIUSZY: Thank you.

12 THE WITNESS: Thank you.

13 RECROSS EXAMINATION

14 BY MR. MARGULIS-OHNUMA:

15 Q I think you just testified that you had -- when you were  
16 using IP-BOX yourself, you had quote, unquote, varied success  
17 with earlier versions of the phone; is that correct?

18 A Yes.

19 Q So sometimes it actually did not work; is that right?

20 A Yes.

21 Q How often did it work and how often did it not work?

22 A I couldn't really give you an exact ratio. I can tell  
23 you it's very finicky. For example, the one real world phone  
24 that I did, I was attempting to do, and had it fail in the  
25 first try. The second try it worked just fine.

1           That's attributable to a number different factors.  
2 One, placement of the light sensor seems to make a big  
3 difference.

4           The other is, there is a window in which the phone  
5 can consider potential correct guesses as the password. And  
6 you have to actually set the software of the IP-BOX to time  
7 that accordingly. So you're basically taking a best guess at  
8 when the open window is.

9           Generally, from my understanding, that time period  
10 has been roughly 4500 to 7,000 milliseconds, 4-and-a-half to 7  
11 seconds. And you're obviously not going to be completely  
12 correct in your guess, but you're fairly accurate.

13           What can happen, as this process continues, is if  
14 you're off by a little bit in the beginning and going through  
15 10,000 numbers, you'll be off by quite a bit more towards the  
16 end. Sort of like a drummer, I guess, would be a good analogy  
17 that's off, off beat by a little bit with the band, you know.  
18 Maybe not so noticeable at first, but by the end of that  
19 process, quite a bit so. And if that happens, it's possible  
20 that the box could actually come up with the correct number  
21 and yet not realize it, because it's missed the window.

22 Q    So, how many real world phones have you actually tested  
23 with IP-BOX?

24 A    One, as I mentioned.

25 Q    And how many test phones have you tested with IP-BOX?

1 A We have two exemplar devices in the lab and I have  
2 probably run tests on them five to ten times.

3 Q And were you able, on all three of these, to actually get  
4 in with IP-BOX?

5 A Yes.

6 Q But sometimes the device failed; right?

7 A Yes.

8 Q And if it had been -- withdrawn.

9 And none of those exemplars were running 8.1.2;  
10 correct?

11 A No.

12 THE COURT: You can step down.

13 THE WITNESS: Thank you.

14 (Witness excused.)

15 THE COURT: You have a witness?

16 MR. MARGULIS-OHNUMA: Your Honor, I do. They're not  
17 here. I'd like to be heard at side-bar about that. I did  
18 write a letter to the Court about that. I would like to be  
19 heard at side-bar about that. It refers to CJA resources.

20 THE COURT: That's what we got off the ECF this  
21 morning? Last night you wrote it?

22 MR. MARGULIS-OHNUMA: That's correct.

23 THE COURT: And he's not here. When can he be here?

24 MR. MARGULIS-OHNUMA: I don't know. He was prepared  
25 to come today, but was not willing to, because of the CJA



Proceedings

32

1 issue. Possibly he will be. I could speak to him now.

2 THE COURT: Well, I am not going to wait around for  
3 him to come.

4 MR. MARGULIS-OHNUMA: No, I would suggest that --  
5 well, we have to resolve the CJA issue first, and if it's  
6 resolved, I would suggest that we set it for maybe sometime  
7 early next week and hopefully we can get him here.

8 THE COURT: What is a good day next week?

9 MS. KONIUSZY: Your Honor, next week doesn't work  
10 for me.

11 THE COURT: Whenever is good for you.

12 MS. KONIUSZY: Could I just check my calendar for  
13 one minute, please?

14 THE COURT: Yes.

15 MS. KONIUSZY: We're available any day the week of  
16 September 28th.

17 THE COURT: We will be on trial, but let's get a --  
18 let's put it down, see how we work it out the 28th.

19 THE COURTROOM DEPUTY: Put it down for that Thursday  
20 or Friday, October 1st.

21 THE COURT: Put it on October 1st, Ana.

22 MS. KONIUSZY: Your Honor, I will just note that  
23 this is now going to be our fourth appearance.

24 THE COURT: I understand that.

25 MR. MARGULIS-OHNUMA: Your Honor, I'm not available.

1 I have a Second Circuit oral argument that morning. We can do  
2 it in the afternoon that day.

3 THE COURT: Let's get another day. I want to do it  
4 in the morning and get it over with.

5 The next day?

6 THE COURTROOM DEPUTY: Friday the 7th?

7 MR. MARGULIS-OHNUMA: Yes, that's fine, Judge.

8 THE COURT: Okay.

9 THE COURTROOM DEPUTY: At 9:30.

10 THE COURT: Get a CJA form for him.

11 MR. MARGULIS-OHNUMA: We have one prepared,  
12 Your Honor.

13 THE COURT: Okay. Thank you.

14 ALL: Thank you, Your Honor.

15 (Matter concluded.)

16

17 ooo0ooo

18

19

20

21

22

23

24

25

# **Exhibit L**

FILED

2016 FEB 19 AM 10:06  
CLERK U.S. DISTRICT COURT  
CENTRAL DIST. OF CALIF.  
RIVERSIDE

1 EILEEN M. DECKER  
United States Attorney  
2 PATRICIA A. DONAHUE  
Assistant United States Attorney  
3 Chief, National Security Division  
TRACY L. WILKISON (California Bar No. 184948)  
4 Assistant United States Attorney  
Chief, Cyber and Intellectual Property Crimes Section  
5 ALLEN W. CHIU (California Bar No. 240516)  
Assistant United States Attorney  
6 Terrorism and Export Crimes Section  
1500 United States Courthouse  
7 312 North Spring Street  
Los Angeles, California 90012  
8 Telephone: (213) 894-0622/2435  
Facsimile: (213) 894-8601  
9 Email: Tracy.Wilkison@usdoj.gov  
Allen.Chiu@usdoj.gov

10 Attorneys for Applicant  
11 UNITED STATES OF AMERICA

12 UNITED STATES DISTRICT COURT  
13 FOR THE CENTRAL DISTRICT OF CALIFORNIA

14 IN THE MATTER OF THE SEARCH OF  
AN APPLE IPHONE SEIZED DURING  
15 THE EXECUTION OF A SEARCH  
WARRANT ON A BLACK LEXUS IS300,  
16 CALIFORNIA LICENSE PLATE  
35KGD203

CM 16-10  
ED No. [REDACTED] (SP)

GOVERNMENT'S MOTION TO COMPEL  
APPLE INC. TO COMPLY WITH THIS  
COURT'S FEBRUARY 16, 2016 ORDER  
COMPELLING ASSISTANCE IN SEARCH;  
EXHIBIT

Hearing Date: March 22, 2016  
Hearing Time: 1:00 p.m.  
Location: Courtroom of the Hon.  
Sheri Pym

22 The United States of America, by and through its counsel of  
23 record, the United States Attorney for the Central District of  
24 California, and Assistant United States Attorneys Tracy L. Wilkison  
25 and Allen W. Chiu, hereby files its Motion to Compel Apple Inc.  
26 ("Apple") to Comply with this Court's February 16, 2016 Order  
27 Compelling Apple To Assist Agents In Its Search.  
28

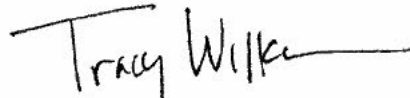
1 This Motion is based upon the attached memorandum of points and  
2 authorities, the attached exhibit, the files and records in this case  
3 including the application and order compelling Apple to assist the  
4 FBI and the underlying search warrant, and such further evidence and  
5 argument as the Court may permit.

6  
7 Dated: February 19, 2016

Respectfully submitted,

8 EILEEN M. DECKER  
United States Attorney

9 PATRICIA A. DONAHUE  
10 Assistant United States Attorney  
11 Chief, National Security Division

12 

13 TRACY L. WILKISON  
14 ALLEN W. CHIU  
Assistant United States Attorneys

15 Attorneys for Applicant  
16 UNITED STATES OF AMERICA  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

TABLE OF CONTENTS

<u>DESCRIPTION</u>	<u>PAGE</u>
TABLE OF AUTHORITIES.....	ii
MEMORANDUM OF POINTS AND AUTHORITIES.....	1
I. INTRODUCTION.....	1
II. STATEMENT OF FACTS.....	3
III. THE COURT SHOULD ISSUE AN ORDER COMPELLING APPLE TO COMPLY WITH ITS ORDER REQUIRING ASSISTANCE WITH THE FBI'S SEARCH OF THE SUBJECT DEVICE PURSUANT TO THE ALL WRITS ACT.....	7
A. This Court's All Writs Act Order is Lawful and Binding....	7
1. The All Writs Act.....	7
2. Apple is not "far removed" from this matter.....	10
3. The Order does not place an unreasonable burden on Apple.....	12
4. Apple's assistance is necessary to effectuate the warrant.....	16
5. Apple's Potential Marketing Concerns Provide Insufficient Grounds to Disregard a Duly Issued Court Order Following a Warrant Based on a Finding of Probable Cause.....	18
6. Public Policy Favors Enforcing of the Order.....	21
B. Congress has Not Limited this Court's Authority to Issue an All Writs Act Order to Apple.....	21
1. No statute addresses data extraction from a passcode-locked cell phone.....	22
2. Congressional inaction does not deprive courts of their authority under the All Writs Act.....	24
IV. CONCLUSION.....	25

**TABLE OF AUTHORITIES**

<u>DESCRIPTION</u>	<u>PAGE</u>
<b><u>FEDERAL CASES</u></b>	
<u>Central Bank of Denver v. First Interstate Bank of Denver,</u> 511 U.S. 164 (1994).....	24
<u>General Construction Company v. Castro,</u> 401 F.3d 963 (9th Cir. 2005).....	24
<u>In re Application of the United States for an Order</u> <u>Directing a Provider of Communication Services to Provide</u> <u>Technical Assistance to the DEA, 2015 WL 5233551, at *4-5</u> (D.P.R. Aug. 27, 2015).....	9
<u>In re Application of United States for an Order Authorizing an</u> <u>In-Progress Trace of Wire Commc'ns over Tel. Facilities</u> <u>(Mountain Bell), 616 F.2d 1122 (9th Cir. 1980).....</u>	<i>passim</i>
<u>In re Application of United States for an Order Directing X to</u> <u>Provide Access to Videotapes (Access to Videotapes),</u> 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (unpublished).....	9, 12
<u>In re Order Requiring [XXX], Inc. to Assist in the Execution</u> <u>of a Search Warrant Issued by This Court by Unlocking a</u> <u>Cellphone (In re XXX), 2014 WL 5510865, at *2 (S.D.N.Y.</u> Oct. 31, 2014).....	9, 15
<u>Konop v. Hawaiian Airlines, Inc.,</u> 302 F.3d 868 (9th Cir. 2002).....	22
<u>Pennsylvania Bureau of Correction v. United States Marshals</u> <u>Service,</u> 474 U.S. 34 (1985).....	7, 22, 24
<u>Plum Creek Lumber Co. v. Hutton,</u> 608 F.2d 1283 (9th Cir. 1979).....	7
<u>Riley v. California,</u> 134 S. Ct. 2473 (2014).....	21
<u>United States v. Catoggio,</u> 698 F.3d 64 (2d Cir. 2012).....	8
<u>United States v. Craft,</u> 535 U.S. 274 (2002).....	24
<u>United States v. Fricosu,</u> 841 F.Supp.2d 1232 (D. Co. 2012).....	17

1 United States v. Hall,  
2 583 F. Supp. 717 (E.D. Va. 1984).....9, 12

3 United States v. Li,  
4 55 F.3d 325, 329 (7th Cir. 1995).....15

5 United States v. Navarro,  
6 No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013).....9

7 United States v. New York Telephone Co.,  
8 434 U.S. 159 (1977).....*passim*

9 **FEDERAL STATUTES**

10 18 U.S.C. § 2510.....22

11 18 U.S.C. § 3103.....21

12 28 U.S.C. § 1651.....7

13 47 U.S.C. § 1001.....22

14 47 U.S.C. § 1002.....22, 23

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



1 MEMORANDUM OF POINTS AND AUTHORITIES

2 I. INTRODUCTION

3 Rather than assist the effort to fully investigate a deadly  
4 terrorist attack by obeying this Court's Order of February 16, 2016,  
5 Apple has responded by publicly repudiating that Order. See Exhibit  
6 1. Apple has attempted to design and market its products to allow  
7 technology, rather than the law, to control access to data which has  
8 been found by this Court to be warranted for an important  
9 investigation. Despite its efforts, Apple nonetheless retains the  
10 technical ability to comply with the Order, and so should be required  
11 to obey it.

12 Before Syed Rizwan Farook ("Farook") and his wife Tafsheen Malik  
13 shot and killed 14 people and injured 22 others at the Inland  
14 Regional Center in San Bernardino, Farook's employer issued him an  
15 iPhone. The Federal Bureau of Investigation ("FBI") recovered that  
16 iPhone during the investigation into the massacre. The government  
17 has reason to believe that Farook used that iPhone to communicate  
18 with some of the very people whom he and Malik murdered. The phone  
19 may contain critical communications and data prior to and around the  
20 time of the shooting that, thus far: (1) has not been accessed; (2)  
21 may reside solely on the phone; and (3) cannot be accessed by any  
22 other means known to either the government or Apple. The FBI  
23 obtained a warrant to search the iPhone, and the owner of the iPhone,  
24 Farook's employer, also gave the FBI its consent to the search.  
25 Because the iPhone was locked, the government subsequently sought  
26 Apple's help in its efforts to execute the lawfully issued search  
27 warrant. Apple refused.

28

1 Apple left the government with no option other than to apply to  
2 this Court for the Order issued on February 16, 2016. The Order  
3 requires Apple to assist the FBI with respect to this single iPhone  
4 used by Farook by providing the FBI with the opportunity to determine  
5 the passcode. The Order does not, as Apple's public statement  
6 alleges, require Apple to create or provide a "back door" to every  
7 iPhone; it does not provide "hackers and criminals" access to  
8 iPhones; it does not require Apple to "hack [its] own users" or to  
9 "decrypt" its own phones; it does not give the government "the power  
10 to reach into anyone's device" without a warrant or court  
11 authorization; and it does not compromise the security of personal  
12 information. See Exhibit 1. To the contrary, the Order allows Apple  
13 to retain custody of its software at all times, and it gives Apple  
14 flexibility in the manner in which it provides assistance. In fact,  
15 the software never has to come into the government's custody.

16 In the past, Apple has consistently complied with a significant  
17 number of orders issued pursuant to the All Writs Act to facilitate  
18 the execution of search warrants on Apple devices running earlier  
19 versions of iOS.<sup>1</sup> The use of the All Writs Act to facilitate a  
20 warrant is therefore not unprecedented; Apple itself has recognized  
21 it for years. Based on Apple's recent public statement and other  
22 statements by Apple, Apple's current refusal to comply with the  
23 Court's Order, despite the technical feasibility of doing so, instead

---

24 <sup>1</sup> Apple's Legal Process Guidelines continue to state that Apple  
25 will provide assistance with unlocking devices running iOS versions  
26 earlier than 8.0, and advises as to what language to include in the  
27 order. See "Extracting Data from Passcode Locked iOS Devices," Apple  
28 Legal Process Guidelines § III(I) (updated September 29, 2015),  
available at <http://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf>. However, Apple has informed another court that it  
now objects to providing such assistance.

1 appears to be based on its concern for its business model and public  
2 brand marketing strategy.<sup>2</sup>

3 Accordingly, the government now brings this motion to compel.  
4 While the Order includes the provision that "to the extent that Apple  
5 believes that compliance with this Order would be unreasonably  
6 burdensome, it may make an application to this Court for relief  
7 within five business days of receipt of the Order," Apple's public  
8 statement makes clear that Apple will not comply with the Court's  
9 Order. The government does not seek to deny Apple its right to be  
10 heard, and expects these issues to be fully briefed before the Court;  
11 however, the urgency of this investigation requires this motion now  
12 that Apple has made its intention not to comply patently clear.<sup>3</sup>  
13 This aspect of the investigation into the December 2, 2015 terrorist  
14 attack must move forward.

15 **II. STATEMENT OF FACTS**

16 As set forth in the government's application for the All Writs  
17 Act Order, and the Declaration of FBI Supervisory Special Agent  
18 ("SSA") Christopher Pluhar, which was attached thereto, both of which  
19 were filed on February 16, 2016, the FBI has been investigating the

---

20 <sup>2</sup> As Apple has stated on its web page, "Our commitment to  
21 customer privacy doesn't stop because of a government information  
22 request. ... Unlike our competitors, Apple cannot bypass your passcode  
23 and therefore cannot access this data. So it's not technically  
24 feasible for us to respond to government warrants for the extraction  
25 of this data from devices in their possession running iOS8."  
([https://web.archive.org/web/20140918023950/http://www.apple.com/priv  
26 acy/government-informaton-requests/](https://web.archive.org/web/20140918023950/http://www.apple.com/privacy/government-informaton-requests/)). Notably, notwithstanding this  
27 previous statement, Apple concedes that it has retained the ability  
28 to do as the Court ordered.

<sup>3</sup> Although a separate order compelling Apple's compliance with  
26 this Court's February 16, 2016, order is not legally necessary, in  
27 light of Apple's publicly stated "[o]pposing [of] this order" and its  
28 stated interest in adversarial testing of the order's legal merits,  
the government files this noticed motion to provide Apple with the  
due process and adversarial testing it seeks.

1 December 2, 2015 mass murder of 14 people, and the shooting and  
2 injuring of 22 others, at the Inland Regional Center ("IRC") in San  
3 Bernardino, California, and the participation by Farook and his wife  
4 Malik in that crime. Farook and Malik died later that day in a  
5 shoot-out after a pursuit with law enforcement.

6 Since that time, the FBI has been tirelessly investigating the  
7 precise role of those who may have been involved in the attack. As  
8 part of this investigation, the FBI obtained search warrants to  
9 search, among other locations and items, the digital devices and  
10 online accounts of Farook and Malik. Through those searches, the FBI  
11 has discovered crucial information about the attack. For example,  
12 the FBI discovered that on December 2, 2015, at approximately 11:14  
13 a.m., a post on a Facebook page associated with Malik stated, "We  
14 pledge allegiance to Khalifa bu bkr al bhaghdadi al quraishi,"  
15 referring to Abu Bakr Al Baghdadi, the leader of Islamic State of  
16 Iraq and the Levant ("ISIL"), also referred to as the Islamic State  
17 ("IS"), or the Islamic State of Iraq and al-sham ("ISIS"), or Daesh.  
18 ISIL is designated as a foreign terrorist organization by the United  
19 States Department of State and has been so designated since December  
20 2004. Moreover, a search warrant executed at Farook's residence  
21 resulted in the discovery of thousands of rounds of ammunition and  
22 over a dozen pipe bombs.

23 In addition, as part of the FBI's investigation, on December 3,  
24 2015, the Honorable David T. Bristow, United States Magistrate Judge,  
25 issued a search warrant in Docket Number ED 15-0451M for a black  
26 Lexus IS300, which was a vehicle that Farook used. The vehicle was  
27 parked outside of his residence where the thousands of rounds of  
28 ammunition and pipe bombs were found. The search warrant for the

1 vehicle also ordered the search of digital devices located within it.  
2 Inside the vehicle the FBI found a cellular telephone of an Apple  
3 make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ,  
4 IMEI:358820052301412, on the Verizon Network (the "SUBJECT DEVICE").  
5 The SUBJECT DEVICE is owned by Farook's employer at the San  
6 Bernardino County Department of Public Health ("SBCDPH"), and was  
7 assigned to, and used by, Farook as part of his employment. The  
8 SBCDPH provided the government its consent to search the SUBJECT  
9 DEVICE and to Apple's assistance with that search.<sup>4</sup>

10 Nonetheless, despite the search warrant ordered by the Court and  
11 the owner's consent to search the SUBJECT DEVICE, the FBI has been  
12 unable to search the SUBJECT DEVICE because it is "locked" or secured  
13 with a user-determined, numeric passcode. More to the point, the FBI  
14 has been unable to make attempts to determine the passcode to access  
15 the SUBJECT DEVICE because Apple has written, or "coded," its  
16 operating systems with a user-enabled "auto-erase function" that  
17 would, if enabled, result in the permanent destruction of the  
18 required encryption key material after 10 failed attempts at the  
19 entering the correct passcode (meaning that, after 10 failed  
20 attempts, the information on the device becomes permanently  
21 inaccessible).

22 The information and data contained on the SUBJECT DEVICE is of  
23 particular concern to the government because, while evidence found on  
24 the iCloud account associated with the SUBJECT DEVICE indicates that  
25 Farook communicated with victims who were later killed during the  
26

---

27 <sup>4</sup> In addition, SBCDPH has a written policy that all digital  
28 devices are subject to search at any time by the SBCDPH, which  
Farook accepted via signature upon employment.

1 shootings on December 2, 2015, the backup iCloud data which the  
2 government has been able to obtain for the account ends on October  
3 19, 2015. In addition, toll records for the SUBJECT DEVICE establish  
4 that Farook communicated with Malik using the SUBJECT DEVICE between  
5 July and November 2015, but this information is not found in the  
6 backup iCloud data. Accordingly, there may be critical  
7 communications and data prior to and around the time of the shooting  
8 that thus far has not been accessed, may reside solely on the SUBJECT  
9 DEVICE; and cannot be accessed by any other means known to either the  
10 government or Apple.

11 When the government first realized that Apple retained the means  
12 to obtain that data from the SUBJECT DEVICE and that due to the way  
13 that Apple created the software Apple was the only means of obtaining  
14 that data, the government sought Apple's voluntary assistance. Apple  
15 rejected the government's request, although it conceded that it had  
16 the technical capability to help. As a result, without any other  
17 alternative, on February 16, 2016, the government applied for – and  
18 this Court subsequently issued – an Order pursuant to the All Writs  
19 Act, compelling Apple to assist the FBI in its search of the SUBJECT  
20 DEVICE.

21 After the government served this Court's Order on Apple, Apple  
22 issued a public statement responding directly to the Order. See  
23 Exhibit 1. In that statement, Apple again did not assert that it  
24 lacks the technical capability to execute the Order, that it is not  
25 essential to gaining access into the iPhone, or that it would be too  
26 time- or labor-intensive. Rather, Apple appears to object based on a  
27 combination of: a perceived negative impact on its reputation and  
28 marketing strategy were it to provide the ordered assistance to the

1 government, numerous mischaracterizations of the requirements of the  
2 Order, and an incorrect understanding of the All Writs Act.

3 **III. THE COURT SHOULD ISSUE AN ORDER COMPELLING APPLE TO COMPLY WITH**  
4 **ITS ORDER REQUIRING ASSISTANCE WITH THE FBI'S SEARCH OF THE**  
5 **SUBJECT DEVICE PURSUANT TO THE ALL WRITS ACT**

6 **A. This Court's All Writs Act Order is Lawful and Binding**

7 To the extent that Apple objects that the Court does not have  
8 authority under the All Writs Act to compel Apple to assist in the  
9 execution of a lawfully obtained search warrant, this objection fails  
10 because the authority to require reasonable third-party assistance  
11 that is necessary to execute a warrant is well-established, and no  
12 provision of any other law or any judicial decision justifies  
13 limitation of that All Writs Act authority. To allow Apple not to  
14 comply with the Order would frustrate the execution of a valid  
15 warrant and thwart the public interest in a full and complete  
16 investigation of a horrific act of terrorism.

17 1. The All Writs Act

18 The All Writs Act provides in relevant part that "all courts  
19 established by Act of Congress may issue all writs necessary or  
20 appropriate in aid of their respective jurisdictions and agreeable to  
21 the usages and principles of law." 28 U.S.C. § 1651(a). As the  
22 Supreme Court explained, "[t]he All Writs Act is a residual source of  
23 authority to issue writs that are not otherwise covered by statute."  
24 Pennsylvania Bureau of Correction v. United States Marshals Service,  
25 474 U.S. 34, 43 (1985). Pursuant to the All Writs Act, the Court has  
26 the power, "in aid of a valid warrant, to order a third party to  
27 provide nonburdensome technical assistance to law enforcement  
28 officers." Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th  
Cir. 1979) (citing United States v. New York Telephone Co., 434 U.S.

1 159 (1977)). The All Writs Act permits a court, in its "sound  
2 judgment," to issue orders necessary "to achieve the rational ends of  
3 law" and "the ends of justice entrusted to it." New York Telephone  
4 Co., 434 U.S. at 172-73 (citations and internal quotation marks  
5 omitted). Courts must apply the All Writs Act "flexibly in  
6 conformity with these principles." Id. at 173; accord United States  
7 v. Catoggio, 698 F.3d 64, 67 (2d Cir. 2012) ("[C]ourts have  
8 significant flexibility in exercising their authority under the  
9 Act.") (citation omitted).

10 In New York Telephone Co., the Supreme Court held that courts  
11 have authority under the All Writs Act to issue supplemental orders  
12 to third parties to facilitate the execution of search warrants. The  
13 Court held that "[t]he power conferred by the Act extends, under  
14 appropriate circumstances, to persons who, though not parties to the  
15 original action or engaged in wrongdoing, are in a position to  
16 frustrate the implementation of a court order or the proper  
17 administration of justice, ... and encompasses even those who have not  
18 taken any affirmative action to hinder justice." Id. at 174. In  
19 particular, the Court upheld an order directing a phone company to  
20 assist in executing a pen register search warrant issued under Rule  
21 41. See id. at 171-76; see also In re Application of United States  
22 for an Order Authorizing an In-Progress Trace of Wire Commc'ns over  
23 Tel. Facilities (Mountain Bell), 616 F.2d 1122, 1132-33 (9th Cir.  
24 1980) (affirming district court's order compelling Mountain Bell to  
25 trace telephone calls, on grounds that "the obligations imposed . . .  
26 were reasonable ones." (citing New York Telephone Co., 434 U.S. at  
27 172)). New York Telephone Co. also held that "Rule 41 is not limited  
28 to tangible items but is sufficiently flexible to include within its



1 scope electronic intrusions authorized upon a finding of probable  
2 cause." 434 U.S. at 169. The Court relied upon the authority of a  
3 search warrant pursuant to Rule 41 to predicate an All Writs Act  
4 order commanding a utility to implement a pen register and trap and  
5 trace device - before Congress had passed a law that specifically  
6 authorized pen registers by court order. Under New York Telephone  
7 Co. and Mountain Bell, the Court had authority pursuant to the All  
8 Writs Act to issue the Order.

9 Further, based on the authority given under the All Writs Act,  
10 courts have issued orders, similar to the one the Court issued here,  
11 that require a manufacturer to attempt to assist in accessing a  
12 cellphone's image files so that a warrant may be executed as  
13 originally contemplated. See, e.g., In re Order Requiring [XXX],  
14 Inc. to Assist in the Execution of a Search Warrant Issued by This  
15 Court by Unlocking a Cellphone (In re XXX), 2014 WL 5510865, at \*2  
16 (S.D.N.Y. Oct. 31, 2014); see also United States v. Navarro, No. 13-  
17 CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013). Courts have also  
18 issued All Writs Act orders in support of warrants in a wide variety  
19 of contexts, including ordering a phone company to assist with a trap  
20 and trace device (Mountain Bell, 616 F.2d at 1129); ordering a credit  
21 card company to produce customer records (United States v. Hall, 583  
22 F. Supp. 717, 722 (E.D. Va. 1984)); ordering a landlord to provide  
23 access to security camera videotapes (In re Application of United  
24 States for an Order Directing X to Provide Access to Videotapes  
25 (Access to Videotapes), 2003 WL 22053105, at \*3 (D. Md. Aug. 22,  
26 2003) (unpublished)); and ordering a phone company to assist with  
27 consensual monitoring of a customer's calls (In re Application of the  
28 United States for an Order Directing a Provider of Communication

1 Services to Provide Technical Assistance to the DEA, 2015 WL 5233551,  
2 at \*4-5 (D.P.R. Aug. 27, 2015)). The government is also aware of  
3 multiple other unpublished orders in this district and across the  
4 country compelling Apple to assist in the execution of a search  
5 warrant by accessing the data on devices running earlier versions of  
6 iOS, orders with which Apple complied.<sup>5</sup> In fact, as noted above,  
7 Apple has long recognized this application, and has complied with  
8 search warrants compelling Apple to extract data from older iOS  
9 devices locked with a passcode. Until last year, Apple did not  
10 dispute any such order.

11 In New York Telephone Co., the Supreme Court considered three  
12 factors in concluding that the issuance of the All Writs Act order to  
13 the phone company was appropriate. First, it found that the phone  
14 company was not "so far removed from the underlying controversy that  
15 its assistance could not be permissibly compelled." Id. at 174.  
16 Second, it concluded that the order did not place an undue burden on  
17 the phone company. See id. at 175. Third, it determined that the  
18 assistance of the company was necessary to achieve the purpose of the  
19 warrant. See id. As set forth below, each of these factors supports  
20 the order issued in this case.

21 2. Apple is not "far removed" from this matter

22 First, Apple is not "so far removed from the underlying  
23 controversy that its assistance could not be permissibly compelled."

24  
25 <sup>5</sup> In litigation pending before a Magistrate Judge in the Eastern  
26 District of New York, that court sua sponte raised the issue of  
27 whether it had authority under the All Writs Act to issue a similar  
28 order. That out-of-district litigation remains pending without any  
issued orders, nor would any such order be binding on this Court. In  
any event, that litigation represents a change in Apple's willingness  
to access iPhones operating prior iOS versions, not a change in  
Apple's technical ability.

1 Apple designed, manufactured and sold the SUBJECT DEVICE, and wrote  
2 and owns the software that runs the phone – which software is  
3 preventing the search for evidence authorized by the warrant.  
4 Indeed, Apple has positioned itself to be essential to gaining access  
5 to the SUBJECT DEVICE or any other Apple device, and has marketed its  
6 products on this basis. See, e.g., Apple’s Security Guide,  
7 [www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](http://www.apple.com/business/docs/iOS_Security_Guide.pdf). Apple designed  
8 and restricts access to the code for the auto-erase function – the  
9 function that makes the data on the phone permanently inaccessible  
10 after multiple failed passcode attempts. This feature effectively  
11 prevents the government from performing the search for evidence  
12 authorized by the warrant without Apple’s assistance. The same  
13 software Apple is uniquely able to modify also controls the delays  
14 Apple implemented between failed passcode attempts – which makes the  
15 process take too long to enable the access ordered by the Court.  
16 Especially but not only because iPhones will only run software  
17 cryptographically signed by Apple, and because Apple restricts access  
18 to the source code of the software that creates these obstacles, no  
19 other party has the ability to assist the government in preventing  
20 these features from obstructing the search ordered by the Court  
21 pursuant to the warrant. Just because Apple has sold the phone to a  
22 customer and that customer has created a passcode does not mean that  
23 the close software connection ceases to exist; Apple has designed the  
24 phone and software updates so that Apple’s continued involvement and  
25 connection is required.

26 Apple is also not made “far removed” by the fact that it is a  
27 non-government third party. While New York Telephone Co. and  
28 Mountain Bell involved public utilities, limiting All Writs Act

1 orders to public utilities is inconsistent with the broad scope of  
2 judicial authority under the All Writs Act. New York Telephone Co.  
3 emphasized that "the Company's facilities were being employed to  
4 facilitate a criminal enterprise on a continuing basis[,] and the  
5 company's noncompliance "threatened obstruction of an investigation  
6 which would determine whether the Company's facilities were being  
7 lawfully used." 434 U.S. at 174. In Mountain Bell, the Ninth  
8 Circuit emphasized that its decision "should not be read to authorize  
9 the wholesale imposition upon private, third parties of duties  
10 pursuant to search warrants," 616 F.2d at 1132, but Apple is not a  
11 random entity summoned off the street to offer assistance, nor is it  
12 the target of the investigation. Where Apple designed its software  
13 and that design interferes with the execution of search warrants,  
14 where it manufactured and sold a phone used by an ISIL-inspired  
15 terrorist, where it owns and licensed the software used to further  
16 the criminal enterprise, where it retains exclusive control over the  
17 source code necessary to modify and install the software, and where  
18 that very software now must be used to enable the search ordered by  
19 the warrant, compulsion of Apple is permissible under New York  
20 Telephone Co.

21 Moreover, other courts have directed All Writs Act orders based  
22 on warrants to entities that are not public utilities. For example,  
23 neither the credit card company in Hall nor the landlord in Access to  
24 Videotapes was a public utility. See Hall, 583 F. Supp. at 722;  
25 Access to Videotapes, 2003 WL 22053105, at \*3. Apple's close  
26 relationship to the iPhone and its software, both legally and  
27 technically – which are the produce of Apple's own design – makes  
28

1 compelling assistance from Apple a permissible and indispensable  
2 means of executing the warrant.

3 3. The Order does not place an unreasonable burden on  
4 Apple

5 The Order has also not placed any unreasonable burden on Apple.  
6 Where, as here, compliance with the order would not require  
7 inordinate effort, no unreasonable burden can be found. See New York  
8 Telephone Co., 434 U.S. at 175 (holding that All Writs Act order was  
9 not burdensome because it required minimal effort by the company and  
10 provided for reimbursement for the company's efforts); Mountain Bell,  
11 616 F.2d at 1132 (rejecting telephone company's argument that  
12 unreasonable burden would be imposed because of a drain on resources  
13 and possibility of system malfunctions because the "Order was  
14 extremely narrow in scope, restricting the operation to [electronic  
15 switching system] facilities, excluding the use of manual tracing,  
16 prohibiting any tracing technique which required active monitoring by  
17 company personnel, and requiring that operations be conducted 'with a  
18 minimum of interference to the telephone service'").

19 While the Order in this case requires Apple to provide or employ  
20 modified software, modifying an operating system - which is  
21 essentially writing software code in discrete and limited manner - is  
22 not an unreasonable burden for a company that writes software code as  
23 part of its regular business.<sup>6</sup> The simple fact of having to create  
24 code that may not now exist in the exact form required does not an  
25 undue burden make. In fact, providers of electronic communications  
26

---

27 <sup>6</sup> Additionally, the Order provides that Apple may request  
28 reasonable reimbursement for expenses incurred in complying with the  
Order.

1 services and remote computing services are sometimes required to  
2 write some amount of code in order to gather information in response  
3 to subpoenas or other process. Additionally, assistance under the  
4 All Writs Act has been compelled to provide something that did not  
5 previously exist - the decryption of the contents of devices seized  
6 pursuant to a search warrant. In United States v. Fricosu, 841  
7 F.Supp.2d 1232, 1237 (D. Co. 2012), a defendant's computer - whose  
8 contents were encrypted - was seized, and the defendant was ordered  
9 pursuant to the All Writs Act to assist the government in producing a  
10 copy of the unencrypted contents of the computer. Here, the type of  
11 assistance does not even require Apple to assist in producing the  
12 unencrypted contents; the assistance is rather to facilitate the  
13 FBI's attempts to test passcodes.

14 As noted above, Apple designs and implements all of the features  
15 discussed, writes and cryptographically signs the iOS, routinely  
16 patches security or functionality issues in its operating system, and  
17 releases new versions of its operating system to address issues. By  
18 comparison, writing a program that turns off non-encryption features  
19 that Apple was responsible for writing to begin with would not be  
20 unduly burdensome. At no point has Apple ever said that it does not  
21 have the technical ability to comply with the Order, or that the  
22 Order asks Apple to undertake an unreasonably challenging software  
23 development task. On this point, Apple's silence speaks volumes.

24 Moreover, contrary to Apple's recent public statement that the  
25 assistance ordered by the Court "could be used over and over again,  
26 on any number of devices" and that "[t]he government is asking Apple  
27 to hack our own users," the Order is tailored for and limited to this  
28 particular phone. And the Order will facilitate only the FBI's

1 efforts to search the phone; it does not require Apple to conduct the  
2 search or access any content on the phone. Nor is compliance with  
3 the Order a threat to other users of Apple products. Apple may  
4 maintain custody of the software, destroy it after its purpose under  
5 the Order has been served, refuse to disseminate it outside of Apple,  
6 and make clear to the world that it does not apply to other devices  
7 or users without lawful court orders. As such, compliance with the  
8 Order presents no danger for any other phone and is not "the  
9 equivalent of a master key, capable of opening hundreds of millions  
10 of locks."

11 To the extent that Apple claims that the Order is unreasonably  
12 burdensome because it undermines Apple's marketing strategies or  
13 because it fears criticism for providing lawful access to the  
14 government, these concerns do not establish an undue burden. The  
15 principle that "private citizens have a duty to provide assistance to  
16 law enforcement officials when it is required is by no means foreign  
17 to our traditions." New York Telephone 434 U.S. at 176 n.24. Apple  
18 is not above the law in that regard, and it is perfectly capable of  
19 advising consumers that compliance with a discrete and limited court  
20 order founded on probable cause is an obligation of a responsible  
21 member of the community. It does not mean the end of privacy. As  
22 discussed above, the Order requires Apple to assist only in  
23 facilitating proper, legal access based on a finding of probable  
24 cause. Further, the government is not seeking to "break" Apple's  
25 encryption infrastructure or unlawfully violate the privacy of its  
26 customers. Instead, through proper legal process through the Court,  
27 the government is seeking to use capabilities that Apple has  
28 purposefully retained in a situation where the former user of the

1 phone is dead and no longer has any expectation of privacy in the  
2 phone, and the owner of the phone consents both to the search of the  
3 phone and to Apple's assistance thereto.

4 More generally, the burden associated with compliance with legal  
5 process is measured based on the direct costs of compliance, not on  
6 other more general considerations about reputations or the  
7 ramifications of compliance. See In re XXX, 2014 WL 5510865, at \*2.  
8 For example, an All Writs Act order may be used to require the  
9 production of a handwriting exemplar, see United States v. Li, 55  
10 F.3d 325, 329 (7th Cir. 1995), even though the subject may face  
11 criminal sanctions as a result of his compliance. Apple's  
12 speculative policy concerns regarding possible consequences from  
13 compliance with the Order in this matter merit little weight,  
14 particularly when complying with a court order based on a warrant  
15 serves the ends of justice and protects public safety in furthering  
16 the investigative aims of a terrorism investigation.

17 4. Apple's assistance is necessary to effectuate the  
18 warrant

19 Apple's assistance is also necessary to effectuate the warrant.  
20 In New York Telephone Co., the Court held that the order met that  
21 standard because "[t]he provision of a leased line by the Company was  
22 essential to the fulfillment of the purpose – to learn the identities  
23 of those connected with the gambling operation – for which the pen  
24 register order had been issued." 434 U.S. at 175. The Order issued  
25 here also meets this standard, as it is essential to ensuring that  
26 the government is able to execute the warrant.

27 In this case, the ability to perform the search ordered by the  
28 warrant on the SUBJECT DEVICE is of critical importance to an ongoing



1 terrorism investigation. The user of the phone, Farook, is a mass  
2 murderer who caused the death of a large number of his coworkers and  
3 the shooting of many others, and who built bombs and hoarded weapons  
4 for this purpose. The FBI has been able to obtain several iCloud  
5 backups for the SUBJECT DEVICE, and executed a warrant to obtain all  
6 saved iCloud data associated with the SUBJECT DEVICE. Evidence in  
7 the iCloud account indicates that Farook was in communication with  
8 victims who were later killed during the shootings perpetrated by  
9 Farook on December 2, 2015, and toll records show that Farook  
10 communicated with Malik using the SUBJECT DEVICE. Importantly,  
11 however, the most recent backup of the iCloud data obtained by the  
12 government was dated October 19, 2015, approximately one and a half  
13 months before the shooting. As such, there may be relevant, critical  
14 communications and data around the time of the shooting that may  
15 reside solely on the SUBJECT DEVICE and can only be obtained if the  
16 government is able to search the phone as directed by the warrant.

17 Moreover, as discussed above, Apple's assistance is necessary  
18 because without the access to Apple's software code and ability to  
19 cryptographically sign code for the SUBJECT DEVICE that only Apple  
20 has, the FBI cannot attempt to determine the passcode without fear of  
21 permanent loss of access to the data or excessive time delay.

22 Indeed, after reviewing a number of other suggestions to obtain the  
23 data from the SUBJECT DEVICE with Apple, technicians from both Apple  
24 and the FBI agreed that they were unable to identify any other  
25 methods - besides that which is now ordered by this Court - that are  
26 feasible for gaining access to the currently inaccessible data on the  
27  
28

1 SUBJECT DEVICE.<sup>7</sup> There can thus be no question that Apple's  
2 assistance is necessary, and that the Order was therefore properly  
3 issued.

4 5. Apple's Potential Marketing Concerns Provide  
5 Insufficient Grounds to Disregard a Duly Issued Court  
6 Order Following a Warrant Based on a Finding of  
7 Probable Cause

8 To the extent that Apple objects on the grounds that it would  
9 undermine its marketing strategy to comply with this Court's Order,  
10 or that it has an overall objection to anything that enables lawful  
11 access by the government to encrypted information, the government  
12 believes these objections are irrelevant and not legally cognizable  
13 before this Court.

14 First, in this case, the government seeks to search the SUBJECT  
15 DEVICE pursuant to a validly-issued search warrant, and a validly-  
16 issued All Writs Act Order. The government shares Apple's stated  
17 concern that "information needs to be protected from hackers and

---

18 <sup>7</sup> The four suggestions that Apple and the FBI discussed (and  
19 their deficiencies) were: (1) to obtain cell phone toll records for  
20 the SUBJECT DEVICE (which, while the government has of course done  
21 so, is insufficient because there is far more information on the  
22 SUBJECT DEVICE than simply toll records); (2) to determine if any  
23 computers were paired with the SUBJECT DEVICE to obtain data (which  
24 the government has determined that none were); (3) to attempt an  
25 auto-backup of the SUBJECT DEVICE with the related iCloud account  
26 (which would not work in this case because neither the owner nor the  
27 government knew the password to the iCloud account, and the owner, in  
28 an attempt to gain access to some information in the hours after the  
attack, was able to reset the password remotely, but that had the  
effect of eliminating the possibility of an auto-backup); and (4)  
obtaining previous back-ups of the SUBJECT DEVICE (which the  
government has done, but is insufficient because these backups end on  
October 19, 2015, nearly one-and-a-half months prior to the IRC  
shooting incident, and also back-ups do not appear to have the same  
amount of information as is on the phone itself). After subsequent  
conversations, though, Apple conceded that none of these suggestions  
would work to execute the search warrant or to sufficiently obtain  
the information sought.

1 criminals who want to access it, steal it, and use it without our  
2 knowledge or permission." See Exhibit 1. The Order at issue does  
3 not compromise that interest. This is not a situation of protecting  
4 the owner and user of this particular device against unauthorized or  
5 unlawful access - here, the owner consented to the government  
6 accessing it. Nor is it about protecting Apple's customers from the  
7 government "intercept[ing] [their] messages, access[ing] [their]  
8 health records or financial data, track[ing] [their] location, or  
9 even access [their] phone's microphone or camera without [their]  
10 knowledge" or from "hackers and criminals who want to access  
11 [personal information], steal it, and use it without our knowledge or  
12 permission." What is at stake are two judicially issued orders: one  
13 based on a finding of probable cause, approved by this Court,  
14 permitting the government to search one telephone of an individual  
15 suspected of being involved in a terrorist attack that killed 14  
16 Americans and wounded 22 others on our own soil, the other directing  
17 Apple to provide limited assistance it is uniquely qualified to  
18 provide to effectuate that order.

19 Second, the assistance ordered is not a "back door" or a "hack"  
20 to all of Apple's encryption software. That is an unwarranted and  
21 inaccurate characterization. As was made plain in the government's  
22 application for the All Writs Act Order, the government asks that  
23 Apple assist in the execution of a search warrant using the  
24 capabilities that Apple has retained along within its encryption  
25 software, such that the government can attempt to determine the  
26 passcode without the additional, non-encryption features that Apple  
27 has coded into its operating system, for the SUBJECT DEVICE only. In  
28 sum, the government seeks the ability to make multiple attempts at

1 determining the passcode without risk that the data subject to search  
2 under the warrant would be rendered permanently inaccessible after 10  
3 wrong attempts. This aspect of the Order is no more or less than  
4 what a user has the ability to do if the auto-erase function is  
5 turned off. Moreover, the software required is no more of a "hack"  
6 or a provision of dangerous malware than any update Apple or other  
7 providers send to a phone. Indeed, it is less so because the  
8 software requested would not reside permanently on the SUBJECT  
9 DEVICE, and Apple can retain control over it entirely. The Order  
10 does nothing regarding the encryption aspect of the operating  
11 software, but instead implicates only the non-encryption additional  
12 features that Apple has programmed.

13 Moreover, to the extent that Apple has concerns about turning  
14 over software to the government so that the government can run the  
15 passcode check program, the Order permits Apple to take possession of  
16 the SUBJECT DEVICE to load the programs in its own secure location,  
17 similar to what Apple has done for years for earlier operating  
18 systems, and permit the government to make its passcode attempts via  
19 remote access. In this fashion, just as with Apple's own already-  
20 existing operating systems and software, no one outside Apple would  
21 have access to the software required by the Order unless Apple itself  
22 chose to share it. This eliminates any danger that the software  
23 required by the Order would go into the "wrong hands" and lead to  
24 criminals' and bad actors' "potential to unlock any iPhone in  
25 someone's physical possession."

26 Third, marketing or general policy concerns are not legally  
27 cognizable objections to the Order. As discussed above, the analysis  
28 of whether a court order presents an unreasonable burden is focused

1 on the direct costs of compliance, not whether the party strongly  
2 disagrees with the concept of complying. This Court should not  
3 entertain an argument that fulfilling basic civic responsibilities of  
4 any American citizen or company - complying with a lawful court order  
5 - could be obviated because that company prefers to market itself as  
6 providing privacy protections that make it infeasible to comply with  
7 court-issued warrants.

8           6. Public Policy Favors Enforcing of the Order

9           Strong public policy interests favor enforcing the All Writs Act  
10 Order in this matter. In New York Telephone Co., the Supreme Court  
11 emphasized "the clear indication by Congress that the pen register is  
12 a permissible law enforcement tool." 434 U.S. at 176. Here, this  
13 matter involves the most fundamental investigative tool of all, the  
14 search warrant. Its use is enshrined in the text of the Constitution  
15 and explicitly endorsed by Congress. See U.S. Const. amend. IV ("no  
16 warrants shall issue, but upon probable cause"); 18 U.S.C. § 3103a(a)  
17 ("a warrant may be issued to search for and seize any property that  
18 constitutes evidence of a criminal offense"). Recently, in Riley v.  
19 California, 134 S. Ct. 2473, 2495 (2014), the Supreme Court set the  
20 standard for what law enforcement must do to search a cell phone  
21 seized incident to arrest: "get a warrant." Here, the government  
22 has obtained a warrant to search the phone of a mass murderer, but  
23 unless this Court enforces the Order requiring Apple's assistance,  
24 the warrant will be meaningless.

25           **B. Congress has Not Limited this Court's Authority to Issue an**  
26           **All Writs Act Order to Apple**

27           Based on the government's discussions with Apple, Apple's public  
28 statement, and the litigation pending in the Eastern District of New

1 York, it appears Apple is arguing that it is justified in refusing to  
2 comply with the Order because the All Writs Act has been limited by  
3 Congress. This argument fails because there is no statute that  
4 specifically addresses the issue of Apple's assistance, and the  
5 absence of such a specific statute cannot be read as a decision to  
6 limit existing authority. Thus, the Order was an appropriate  
7 execution of this court's jurisdiction in this matter.

8 1. No statute addresses data extraction from a passcode-  
9 locked cell phone

10 The Supreme Court has made clear that "[t]he All Writs Act is a  
11 residual source of authority to issue writs that are not otherwise  
12 covered by statute[,] " such that courts may not rely on the All Writs  
13 Act "[w]here a statute specifically addresses the particular issue at  
14 hand[.]" Pennsylvania Bureau of Correction, 474 U.S. at 43. In this  
15 case, no other statute addresses the procedures for requiring Apple  
16 to extract data from a passcode-locked iPhone, so Pennsylvania Bureau  
17 of Correction provides no basis for denying the government's  
18 application for an All Writs Act Order in this case.

19 In particular, neither Federal Rule of Criminal Procedure 41 nor  
20 the Communications Assistance for Law Enforcement Act ("CALEA"), 47  
21 U.S.C. § 1002, "specifically addresses" - or even vaguely addresses -  
22 the duty of Apple to assist in extracting data from a passcode-locked  
23 cell phone in order to permit the government to execute a validly  
24 issued search warrant. CALEA requires telecommunications carriers to  
25 retain the capability to comply with court orders for real-time  
26 interceptions and call-identifying information (data "in motion").<sup>8</sup>

27 \_\_\_\_\_  
28 <sup>8</sup> For example, for the contents of communications, CALEA  
requires telecommunications carriers to be able "to intercept" wire  
(footnote cont'd on next page)

1 Id. By contrast, this case involves evidence already stored on a  
2 cell phone (data "at rest"). Here, Apple is not acting as a  
3 telecommunications carrier, and the Order concerns access to stored  
4 data rather than real-time interceptions and call-identifying  
5 information. Put simply, CALEA is entirely inapplicable to the  
6 present dispute and does not limit this Court's authority under the  
7 All Writs Act to require Apple to assist the government in executing  
8 a search warrant.<sup>9</sup>

9 New York Telephone Co. further illustrates that it is  
10 appropriate for a court to rely on the All Writs Act unless a statute  
11 specifically addresses the particular issue at hand. When the Court  
12 decided New York Telephone Co. in 1977, Congress had enacted Title  
13 III for intercepting the contents of communications, but it had not  
14 yet enacted the closely-related pen register statute for acquiring  
15 non-content information. See Electronic Communications Privacy Act  
16 of 1986 § 301, 100 Stat. 1848 (enacting pen register statute).  
17 Despite the existence of a statute regulating government access to  
18 information closely related to pen registers, but not specifically

19 \_\_\_\_\_  
20 and electronic communications carried by the carrier. 47 U.S.C.  
21 § 1002(a)(1). CALEA incorporates the definition of "intercept" from  
22 the Wiretap Act, see 47 U.S.C. § 1001(1) & 18 U.S.C. § 2510(4), and  
that definition encompasses only information acquired during  
transmission, not while it is in storage. Konop v. Hawaiian  
Airlines, Inc., 302 F.3d 868, 877-878 (9th Cir. 2002).

23 <sup>9</sup> Furthermore, nothing in CALEA prevents a court from ordering a  
24 telecommunications carrier to decrypt communications that the carrier  
25 is capable of decrypting. See 47 U.S.C. § 1002(b)(3). When Congress  
26 enacted CALEA, it understood that existing provider-assistance  
27 provisions required a provider to decrypt communications when it was  
28 able to do so. Both the House and Senate reports for CALEA stated  
that "telecommunications carriers have no responsibility to decrypt  
encrypted communications that are the subject of court-ordered  
wiretaps, unless the carrier provided the encryption and can decrypt  
it." H.R. Rep. No. 103-827(I), at 24 (1994); S. Rep. No. 103-402, at  
24 (1994).

1 addressing pen registers, the Supreme Court held that an All Writs  
2 Act order could be issued in support of a warrant for a pen register.  
3 Under this reasoning, CALEA is no barrier to the Order in this case.

4 2. Congressional inaction does not deprive courts of  
5 their authority under the All Writs Act

6 The current lack of congressional action regarding encryption-  
7 related issues does not deprive this Court of its authority to issue  
8 the Order in this case. Under Pennsylvania Bureau of Correction,  
9 courts may not rely on the All Writs Act where "a statute  
10 specifically addresses" an issue. But the opposite is not true.  
11 Courts may not categorically refuse to rely on the All Writs Act - as  
12 Apple would seemingly want the Court to do - where Congress has  
13 declined to legislate. Court authority to issue All Writs Act orders  
14 in support of warrants has been clearly established since the Supreme  
15 Court decided New York Telephone Co. in 1977. Congress may choose to  
16 expand or limit this authority, but it must do so through enactment  
17 of legislation.

18 The Supreme Court and the Ninth Circuit have repeatedly  
19 cautioned that "Congressional inaction lacks persuasive significance  
20 because several equally tenable inferences may be drawn from such  
21 inaction[.]" General Construction Company v. Castro, 401 F.3d 963,  
22 970-71 (9th Cir. 2005) (quoting Central Bank of Denver v. First  
23 Interstate Bank of Denver, 511 U.S. 164, 187 (1994)); see also United  
24 States v. Craft, 535 U.S. 274, 287 (2002).

25 Here, there are many possible explanations for congressional  
26 inaction on encryption, including that Congress is satisfied with  
27 existing authorities, or that Congress has not yet reached agreement  
28 on whether or how much to expand existing authorities. These



1 possibilities provide no basis for restricting legal authorities that  
2 existed before the beginning of the debate.<sup>10</sup> Because courts do not  
3 lose an authority to issue orders under the All Writs Act merely  
4 because Congress does not subsequently enact legislation endorsing or  
5 expanding that authority, this Court retains authority to issue an  
6 All Writs Act Order consistent with New York Telephone Co.

7 **IV. CONCLUSION**

8 This Court issued a valid Order pursuant to the All Writs Act  
9 requiring Apple to assist the United States in enabling the search  
10 for evidence pursuant to a lawful search warrant. Apple has publicly  
11 stated that it will oppose this Order, and has not agreed to comply.  
12 For the foregoing reasons, the government respectfully requests that  
13 this Court issue an Order compelling Apple to comply.

14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25 <sup>10</sup> Granting legal force to statements or proposals by individual  
26 members of Congress during the course of congressional debate risks  
27 absurd results. Congress routinely debates and fails to act on  
28 important issues, but the mere debate does not restrict existing  
legal authority. Under the Constitution, Congress speaks with legal  
force only when it speaks as one body, through bicameralism and  
presentment - i.e. when it passes a bill.

# EXHIBIT 1

February 16, 2016

# A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

## The Need for Encryption

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going.

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.

## The San Bernardino Case

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

## The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

## A Dangerous Precedent

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.

The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.

We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.

While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.

Tim Cook

**Shop and Learn**

- Mac
- iPad
- iPhone
- Watch
- TV
- Music
- iTunes
- iPod
- Accessories
- Gift Cards

**Apple Store**

- Find a Store
- Genius Bar
- Workshops and Learning
- Youth Programs
- Apple Store App
- Refurbished
- Financing
- Reuse and Recycling
- Order Status
- Shipping Help

**For Education**

- Apple and Education
- Shop for College

**For Business**

- iPhone in Business
- iPad in Business
- Mac in Business
- Shop for Your Business

**Account**

- Manage Your Apple ID
- Apple Store Account
- iCloud.com

**Apple Values**

- Environment
- Supplier Responsibility
- Accessibility
- Privacy
- Inclusion and Diversity
- Education

**About Apple**

- Apple Info
- Job Opportunities
- Press Info
- Investors
- Events
- Hot News
- Legal
- Contact Apple

More ways to shop: visit [Apple Store](#), call 1-800-MY-APPLE, or find a reseller.

Copyright © 2015 Apple Inc. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Sales and Refunds](#) [Site Map](#)

United States

**CERTIFICATE OF SERVICE**

I, **REBECCA EVANS**, declare:

That I am a citizen of the United States and resident or employed in Riverside County, California; that my business address is the Office of United States Attorney, 3403 Tenth Street, Suite 200, Riverside, CA 92501; that I am over the age of eighteen years, and am not a party to the above-entitled action; That I am employed by the United States Attorney for the Central District of California who is a member of the Bar of the United States District Court for the Central District of California, at whose direction I served a copy:

**GOVERNMENT'S MOTION TO COMPEL APPLE INC. TO COMPLY WITH THIS COURT'S FEBRUARY 16, 2016 ORDER COMPELLING ASSISTANCE IN SEARCH; EXHIBIT**

By electronic mail as follows:

Mr. Theodore B. Olson Gibson, Dunn & Crutcher LLP <a href="mailto:tolson@gibsondunn.com">tolson@gibsondunn.com</a>	Mr. Theodore J. Boutrous Jr. Gibson, Dunn & Crutcher LLP <a href="mailto:tboutrous@gibsondunn.com">tboutrous@gibsondunn.com</a>
Ms. Nicola T. Hanna Gibson, Dunn & Crutcher LLP <a href="mailto:nhanna@gibsondunn.com">nhanna@gibsondunn.com</a>	Mr. Eric D. Vandeveld Gibson, Dunn & Crutcher LLP <a href="mailto:evandeveld@gibsondunn.com">evandeveld@gibsondunn.com</a>

This Certificate is executed on **February 19, 2016**, in Riverside, California. I certify under penalty of perjury that the foregoing is true and correct.

  
**REBECCA EVANS**

# **Exhibit M**

# The Washington Post

National Security

## Proposal seeks to fine tech companies for noncompliance with wiretap orders

By **Ellen Nakashima** April 28, 2013

A government task force is preparing legislation that would pressure companies such as Facebook and Google to enable law enforcement officials to intercept online communications as they occur, according to current and former U.S. officials familiar with the effort.

Driven by FBI concerns that it is unable to tap the Internet communications of terrorists and other criminals, the task force's proposal would penalize companies that failed to heed wiretap orders — court authorizations for the government to intercept suspects' communications.

Rather than antagonizing companies whose cooperation they need, federal officials typically back off when a company is resistant, industry and former officials said. But law enforcement officials say the cloak drawn on suspects' online activities — what the FBI calls the “[going dark](#)” problem — means that critical evidence can be missed.

“The importance to us is pretty clear,” Andrew Weissmann, the FBI's general counsel, said last month at an [American Bar Association discussion on legal challenges posed by new technologies](#). “We don't have the ability to go to court and say, ‘We need a court order to effectuate the intercept.’ Other countries have that. Most people assume that's what you're getting when you go to a court.”

There is currently no way to wiretap some of these communications methods easily, and companies effectively have been able to avoid complying with court orders. While the companies argue that they have no means to facilitate the wiretap, the government, in turn, has no desire to enter into what could be a drawn-out contempt proceeding.

Under the draft proposal, a court could levy a series of escalating fines, starting at tens of thousands of dollars, on firms that fail to comply with wiretap orders, according to persons who spoke on the condition of anonymity to discuss internal deliberations. A company that does not comply with an order within a certain period would face an automatic judicial inquiry, which could lead to fines. After 90 days, fines that remain unpaid would double daily.



Instead of setting rules that dictate how the wiretap capability must be built, the proposal would let companies develop the solutions as long as those solutions yielded the needed data. That flexibility was seen as inevitable by those crafting the proposal, given the range of technology companies that might receive wiretap orders. Smaller companies would be exempt from the fines.

The proposal, however, is likely to encounter resistance, said industry officials and privacy advocates.

“This proposal is a non-starter that would drive innovators overseas and cost American jobs,” said Greg Nojeim, a senior counsel at the Center for Democracy and Technology, which focuses on issues of privacy and security. “They might as well call it the Cyber Insecurity and Anti-Employment Act.”

The Obama administration has not yet signed off on the proposal. Justice Department, FBI and White House officials declined to comment. Still, Weissmann said at the ABA discussion that the issue is the bureau’s top legislative priority this year, but he declined to provide details about the proposal.

### **Increased urgency**

The issue of online surveillance has taken on added urgency with the explosion of social media and chat services and the proliferation of different types of online communication. Technology firms are seen as critical sources of information about crime and terrorism suspects.

“Today, if you’re a tech company that’s created a new and popular way to communicate, it’s only a matter of time before the FBI shows up with a court order to read or hear some conversation,” said Michael Sussmann, a former federal prosecutor and a partner at the law firm Perkins Coie’s Washington office who represents technology firms. “If the data can help solve crimes, the government will be interested.”

Some technology companies have developed a wiretap capability for some of their services. But a range of communications companies and services are not required to do so under what is known as CALEA, the 1994 Communications Assistance for Law Enforcement Act. Among those services are social media networks and the chat features on online gaming sites.

Former officials say the challenge for investigators was exacerbated in 2010, when Google began end-to-end encryption of its e-mail and text messages after its networks were hacked. Facebook followed suit. That made it more difficult for the FBI to intercept e-mail by serving a court order on the Internet service provider, whose pipes would carry the encrypted traffic.

The proposal would make clear that CALEA extends to Internet phone calls conducted between two computer users without going through a central company server — what is sometimes called “peer-to-peer” communication. But the heart of the proposal would add a provision to the 1968 Wiretap Act that would allow a court to levy fines.

## **Challenges abound**

One former senior Justice Department official, who is not privy to details of the draft proposal, said law enforcement officials are not seeking to expand their surveillance authorities. Rather, said Kenneth L. Wainstein, assistant attorney general for national security from 2006 to 2008, officials are seeking “to make sure their existing authorities can be applied across the full range of communications technologies.”

Proponents say adding an enforcement provision to the 1968 Wiretap Act is a more politically palatable way of achieving that goal than by amending CALEA to redefine what types of companies should be covered. Industry and privacy experts, including some former government officials, are skeptical.

“There will be widespread disagreement over what the law requires,” said Albert Gidari Jr., a partner at Perkins Coie’s flagship Seattle office who represents telecommunications companies. “It takes companies into a court process over issues that don’t belong in court but rather in standards bodies with technical expertise.”

Some experts said a few companies will resist because they believe they might lose customers who have privacy concerns. Google, for instance, prides itself on protecting its search service from law enforcement surveillance, though it might comply in other areas, such as e-mail. And Skype has [lost some of its cachet as a secure communications](#) alternative now that it has been bought by Microsoft and is reportedly complying with wiretap orders.

Susan Landau, a former Sun Microsystems distinguished engineer, has argued that wiring in an intercept capability will increase the likelihood that a company’s servers will be hacked. “What you’ve done is created a way for someone to silently go in and activate a wiretap,” she said. Traditional phone communications were susceptible to illicit surveillance as a result of the 1994 law, she said, but the problem “becomes much worse when you move to an Internet or computer-based network.”

Marcus Thomas, former assistant director of the FBI’s Operational Technology Division, said good software coders can create an intercept capability that is secure. “But to do so costs money,” he said, noting the extra time and expertise needed to develop, test and operate such a service.

A huge challenge, officials agree, is how to gain access to peer-to-peer communications. Another challenge is making sense of encrypted communications.

Thomas said officials need to strike a balance between the needs of law enforcement and those of the technology companies.

“You want to give law enforcement the ability to have the data they’re legally entitled to get, at the same time not burdening industry and not opening up security holes,” he said.

---

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

---

---

# **Exhibit N**

**National Security**

# Obama faces growing momentum to support widespread encryption

By **Ellen Nakashima** and **Andrea Peterson** September 16, 2015

White House officials have backed away from seeking a legislative fix to deal with the rise of encryption on communication devices, and they are even weighing whether to publicly reject a law requiring firms to be able to unlock their customers' smartphones and apps under court order.

For the past year, law enforcement and the intelligence community have warned that an inability to obtain decrypted data is putting public safety and national security at risk, arguing it will allow criminals and terrorists to communicate securely. They have appealed to tech companies to voluntarily come up with solutions for their own products, and they don't want to rule out legislation entirely.

But over the summer, momentum has grown among officials in the commerce, diplomatic, trade and technology agencies for a statement from the president "strongly disavowing" a legislative mandate and supporting widespread encryption, according to senior officials and documents obtained by The Washington Post.

Their argument: Ruling out a law and supporting encryption would counter the narrative that the United States is seeking to expand its surveillance capability at the expense of cybersecurity. They say the statement from the president also would help repair global trust in the U.S. government and U.S. tech companies, whose public images have taken a beating in the wake of disclosures about widespread National Security Agency surveillance.

And, they argue, it would undercut foreign competitors' claims that U.S. firms are instruments of mass surveillance.

Strong pushback has come from national security officials who think that they ought to be able to retrieve text messages, photos and other material when they have a warrant and who think that their inability to do so is hampering criminal and counterterrorism investigations. If they can't gain access to decrypted data, they warn, there will be a tragedy that could have been averted.

"The encryption issue . . . both in this country and abroad is going to have a major impact on how law enforcement and intelligence do their jobs," said a senior administration official, who was given permission to be interviewed, but on the condition of anonymity because of the topic's sensitivity. "It's not surprising that they want to make sure that the public discourse includes a healthy debate about their issues as well."

The official said that the White House's goal is "driving towards a consensus where we can get an administration position out there." But "there are people that have very strong opinions on both sides of this issue."

Privately, law enforcement officials have acknowledged that prospects for congressional action this year are remote. Although "the legislative environment is very hostile today," the intelligence community's top lawyer, Robert S. Litt, said to colleagues in an August e-mail, which was obtained by The Post, "it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."

There is value, he said, in "keeping our options open for such a situation."

Litt was commenting on a draft paper prepared by National Security Council staff members in July, which also was obtained by The Post, that analyzed several options. They included explicitly rejecting a legislative mandate, deferring legislation and remaining undecided while discussions continue.

None mentioned calling for legislation.

In October, FBI Director James B. Comey, in a speech at the Brookings Institution, said he was "focused on trying to get the law changed" so that companies would be required to unlock data and devices for law enforcement, when it has a warrant. "I'm hoping we can now start a dialogue with Congress on updating" the law, he said.

By July, the tone of law enforcement officials had softened. "We do believe that it's important now, rather than seeking a legislative fix across the board, that we try to work with the individual companies" to achieve solutions, Deputy Attorney General Sally Quillian Yates testified before Congress. Each company knows its systems best, she said. "What works for Apple might not be the best solution for another of the communications providers," she said.

Some White House aides had hoped to have a report on the issue to give to the president months ago. But "the complexity of this issue really makes it a very challenging area to arrive at any sort of policy on," the senior official said. A Cabinet meeting to be chaired by National Security Adviser Susan Rice, ostensibly to make a decision, initially was scheduled for Wednesday, but it has been postponed.

The senior official said that the delays are due primarily to scheduling issues — "there are a lot of other things going on in the world" — that are pressing on officials' time.

What is clear, though, is that the law enforcement argument is "just not carrying the day," said a second senior official, who, like several others, was not authorized to speak on the record. "People are still not persuaded this is a problem. People think we have not made the case. We do not have the perfect example where you have the dead child or a terrorist act to point to, and that's what people seem to claim you have to have."

The draft paper was a “snapshot at a point in time” and does not reflect recent updates, the first senior official said. Nonetheless, other officials said, they capture themes heard in the current debate.

Notably, in drawing up the paper, aides had removed an option included in an earlier draft that would have encouraged legislation or other “compulsory” actions. No one, including law enforcement, officials said, thinks it is a realistic option today.

The option to “disavow legislation” was added in July at the urging of officials at economic and trade agencies, a third senior official said.

This option, NSC aides said in the paper, “would remove technology companies’ most consistent grievance with the administration,” and it might improve cooperation on the issue of encryption.

“Overall, the benefits to privacy, civil liberties and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption,” the paper stated.

This option also would “clearly differentiate” U.S. policy from moves by China and others to mandate decryption and would bolster the United States’ reputation “as a leading source” of secure products and services, it added.

But, the paper said, the option would “not provide any relief” to law enforcement in the near term.

Litt, in his e-mail, quipped: “I think one could equally or more accurately say that it will not provide ANY relief, ever.”

He also took issue with the assertion that a strong statement from the United States could dissuade authoritarian regimes from seeking compulsory legislation of their own. “Really?” he wrote. “Does anyone seriously believe that if the U.S. says we won’t seek access, the Chinese and Russians will say, ‘OK, you are right. We’ll give up?’ I don’t think so.”

---

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

---

Andrea Peterson covers technology policy for The Washington Post, with an emphasis on cybersecurity, consumer privacy, transparency, surveillance and open government.

---



# **Exhibit O**

1 EILEEN M. DECKER  
 United States Attorney  
 2 PATRICIA A. DONAHUE  
 Assistant United States Attorney  
 3 Chief, National Security Division  
 TRACY L. WILKISON (California Bar No. 184948)  
 4 Chief, Cyber and Intellectual Property Crimes Section  
 Assistant United States Attorney  
 5 1500 United States Courthouse  
 312 North Spring Street  
 6 Los Angeles, California 90012  
 Telephone: (213) 894-2400  
 7 Facsimile: (213) 894-8601  
 Email: Tracy.Wilkison@usdoj.gov

8 Attorneys for Applicant  
 9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT  
 11 FOR THE CENTRAL DISTRICT OF CALIFORNIA

12 IN THE MATTER OF THE SEARCH  
 OF AN APPLE IPHONE SEIZED  
 13 DURING THE EXECUTION OF A  
 SEARCH WARRANT ON A BLACK  
 14 LEXUS IS300, CALIFORNIA  
 LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)  
  
 DECLARATION OF STACEY PERINO  
 IN SUPPORT OF GOVERNMENT’S  
 REPLY IN SUPPORT OF MOTION TO  
 COMPEL AND OPPOSITION TO APPLE  
 INC.’S MOTION TO VACATE ORDER;  
 EXHIBITS 17-30

Hearing Date: March 22, 2016  
 Hearing Time: 1:00 p.m.  
 Location: Courtroom of the  
 Hon. Sheri Pym

20  
 21  
 22  
 23  
 24  
 25  
 26  
 27  
 28



1 10 in the Central District of California, and the Court’s Order in the same case calling for  
2 a software image file or “SIF” to be prepared by Apple (the “Order”).

3 b. The Declaration of Erik Neuenschwander dated February 25, 2016  
4 (“Neuenschwander Declaration”).

5 c. Apple’s “iOS Security” for iOS 9.0 or later dated September 2015  
6 (“iOS Security”), attached to the Declaration of Nicola T. Hanna as Exhibit K.

7 d. Documentation from the website of the information technology  
8 company Sogeti, attached hereto as Exhibit 17, available at [http://esec-](http://esec-lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf)  
9 [lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf](http://esec-lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf).

10 e. The repository of code stored at  
11 <https://code.google.com/archive/p/iphone-dataprotection>, described as “ios forensics  
12 tools,” and “Tools and information on iOS 3/4/5/6/7 data protection features.”

13 f. Cellebrite Physical Extraction Manual for iPhone & iPad (Rev 1.3),  
14 attached hereto as Exhibit 18.

15 g. Apple’s “Cryptographic Services,” attached hereto as Exhibit 19,  
16 available at [https://developer.apple.com/library/mac/documentation/Security/  
17 Conceptual/Security\\_Overview/CryptographicServices/CryptographicServices.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/Security_Overview/CryptographicServices/CryptographicServices.html).

18 h. Materials from Apple’s “Code Signing Guide”:

19 i. Exhibit 20, “About Code Signing,” available at  
20 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
21 CodeSigningGuide/Introduction/Introduction.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/Introduction/Introduction.html).

22 ii. Exhibit 21, “Code Signing Overview,” available at  
23 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
24 CodeSigningGuide/AboutCS/AboutCS.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/AboutCS/AboutCS.html).

25 iii. Exhibit 22, “Code Signing Tasks,” available at  
26 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
27 CodeSigningGuide/Procedures/Procedures.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/Procedures/Procedures.html).

28

1                   iv.     Exhibit 23, “Code Signing Requirement Language,” available  
2 at [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
3 CodeSigningGuide/RequirementLang/RequirementLang.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/RequirementLang/RequirementLang.html).

4                   i.     Materials from Apple’s “Cryptographic Services Guide”:

5                   i.     Exhibit 24, “About Cryptographic Services,” available at  
6 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
7 cryptoservices/Introduction/Introduction.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Introduction/Introduction.html).

8                   ii.    Exhibit 25, “Cryptography Concepts In Depth,” available at  
9 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
10 cryptoservices/CryptographyConcepts/CryptographyConcepts.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/CryptographyConcepts/CryptographyConcepts.html).

11                   iii.   Exhibit 26, “Encrypting and Hashing Data,” available at  
12 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
13 cryptoservices/GeneralPurposeCrypto/GeneralPurposeCrypto.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/GeneralPurposeCrypto/GeneralPurposeCrypto.html).

14                   iv.    Exhibit 27, “Managing Keys, Certificates, and Passwords,”  
15 available at [https://developer.apple.com/library/mac/documentation/Security/  
16 Conceptual/cryptoservices/KeyManagementAPIs/KeyManagementAPIs.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/KeyManagementAPIs/KeyManagementAPIs.html).

17                   v.     Exhibit 28, “Glossary,” available at  
18 [https://developer.apple.com/library/mac/documentation/Security/Conceptual/  
19 cryptoservices/Glossary/Glossary.html](https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Glossary/Glossary.html).

20                   j.     Apple’s “Unauthorized Modification of iOS Can Cause Security  
21 Vulnerabilities, Instability, Shortened Battery Life, and Other Issues,” attached hereto as  
22 Exhibit 29, and available at <https://support.apple.com/en-us/HT201954>.

23                   k.     Apple’s “Code Signing,” attached hereto as Exhibit 30, and available  
24 at <https://developer.apple.com/support/code-signing/>.

25                   5.     This Declaration relies on Apple’s publicly disseminated descriptions of  
26 how its own devices, operating system, security features, and software operate. Apple’s  
27 source code is not, however, publicly available. Therefore the descriptions below do not  
28

1 rely on my having reviewed Apple’s source code, rather they rely upon Apple’s own  
2 description of its devices, operating system, security features, and software, as well as on  
3 my training and experience in both observing and/or conducting the tests described in  
4 this document, directing the CEAU embedded engineering analysis of Apple devices and  
5 software, and reviewing other open source materials describing Apple mobile device  
6 technologies.

7 **A. Purpose of this Declaration**

8 6. In this declaration, I discuss the following topics:

9 a. The SIF called for in the Order could run *only* on the Subject Device.

10 To explain this, I first provide some background on public key cryptography (Part B.1)  
11 and Apple’s use of it and code signing to prevent the use of unauthorized code on its  
12 products (Part B.2). The Order provides that the SIF would only run on the Subject  
13 Device. Apple already requires that iOS updates include a unique device identifier for  
14 the Subject Device (Part B.3). Because an iPhone requires Apple to have  
15 cryptographically “signed” code before an iPhone will run it, and changing a unique  
16 device identifier within the SIF would invalidate Apple’s signature, the SIF would not  
17 run on other iPhones. (Part B.3.)

18 b. The SIF called for by the Court’s Order would perform functions that  
19 already exist in open source software for older devices and operating systems. In other  
20 words, code already exists that will bypass the auto-erase and time-delay functions and  
21 permit electronic submission of passcodes, but would need to be updated and modified  
22 for newer operating systems. (Part C.) That software, however, cannot run on the  
23 Subject Device without Apple’s “signature.”

24 c. The data contained on the Subject Device can be decrypted *only* on  
25 the Subject Device. This is because the encryption key includes a unique identifier that  
26 exists only on the Subject Device. (Part D.) Because the decryption must occur on the  
27 Subject Device, and because only Apple-signed software can run on the Subject Device  
28

1 (Part B.2), any code or software tools needed to assist in testing passcodes (even code  
2 that includes components that already exist, Part C) must be signed by Apple.

3 d. Because the Subject Device was powered off when it was seized, it  
4 was not possible for it to back itself up to iCloud without the passcode. (Part E.)

5 **B. The SIF Called for by the Order Would Run Only on the Subject**  
6 **Device**

7 **1. General Background on Public Key Cryptography**

8 7. Generally, encryption and decryption are the processes of first converting  
9 intelligible “plaintext” into unintelligible “ciphertext,” and second converting the  
10 ciphertext back into plaintext, respectively.

11 8. While encryption is designed to protect the confidentiality of information, a  
12 separate issue that arises in cryptology is authentication. Public key cryptography  
13 provides a method to both send messages securely, even when using a non-secure  
14 channel, and to validate the messages that are received. A properly implemented  
15 cryptographic signature gives the receiver reason to believe the message was sent by the  
16 person claiming to be the sender. A cryptographic signature also prevents modification  
17 of the original message by anyone other than the signer.

18 9. Public key encryption uses a complex operation that involves two different  
19 keys, a public key and a private key. A public key cryptosystem uses one key to encrypt  
20 (or to sign) a message and a different key to decrypt (or verify) the same message. (For  
21 this reason it is also referred to as asymmetric.) One of the essential properties of a  
22 public key cryptosystem is that it is too difficult—computationally infeasible—to  
23 determine a person’s private key knowing only that person’s public key.

24 10. The public key is made globally available while the private key is kept  
25 confidential. This allows anyone who is a member of the system to use the “phone  
26 book” of public keys to send a private message to any other member using the recipient’s  
27 public key, but it allows only the recipient to open it using that person’s private key.  
28

1 Each key pair is unique to an individual member of a properly implemented  
2 cryptosystem.

3 11. One of the other essential properties of a public key cryptosystem is that the  
4 encryption operation and the decryption operation used in the cryptosystem are inverse  
5 operations.<sup>1</sup> This means that if one started with a message, it would not matter if one  
6 used the encryption operation followed by the decryption operation, or the decryption  
7 operation followed by the encryption operation, either would yield the original message  
8 again.<sup>2</sup>

9 12. A more detailed example of how the public key cryptosystem works to sign  
10 a message is as follows:

- 11 a. Alice generates a public-private key pair, and publishes her public  
12 key.
- 13 b. Alice composes a Message to Bob, and uses her private key to  
14 compute or generate the Signature. (This is represented:  $\text{Signature} = D_{\text{pri}}(\text{Message})$ ,  
15 where D is the decryption operation.)
- 16 c. Alice sends Bob both the Message and the Signature.
- 17 d. Bob then uses Alice's public key to verify that the message was  
18 signed using her private key. Bob does this by running the inverse "encryption"  
19 operation on the Signature. (This is represented:  $E_{\text{pub}}(\text{Signature}) = \text{Message}$ , where E is  
20 the encryption operation.) If the result of that operation is the Message that Alice sent  
21 Bob, then Bob knows the message is not a forgery and came from Alice.

---

25 <sup>1</sup> This is represented as follows, where E() and D() denote the encryption and  
26 decryption operations, and M is the text of the message:  $M = E(D(M)) = D(E(M))$ .

27 <sup>2</sup> (See Ex. 19 at 2, diagram (Apple developer website, Cryptographic Services).  
28 See generally Ex. 25 at 5, 7 (Apple developer website, Cryptographic Concepts in  
Depth).)



1 e. In this example, Alice could also have encrypted the message using  
2 Bob’s public key. Bob could then have decrypted the message using Bob’s own private  
3 key.

4 **2. Apple’s Use of Public Key Encryption to Prevent the Use of**  
5 **Unauthorized Code on Its Products**

6 13. Just as a cryptosystem can be used to “sign” messages, it can be used to  
7 “sign” executable code.<sup>3</sup> Specifically, a vendor can embed a public key into a device  
8 such that the public key cannot be altered. For any and all executable code modules, the  
9 vendor uses its private key to calculate and attach a signature. As the device loads code  
10 modules for execution, the device uses the embedded public key to calculate the  
11 signature and thus verify the module’s integrity and authenticity. As long as the public  
12 key cryptosystem is unbroken and the embedded key cannot be modified within the  
13 device, the scheme guarantees that only code issued by the vendor (that has been  
14 cryptographically signed) will run on the device.

15 14. Apple implements this system to require that its devices use software that  
16 only Apple authorizes. Apple does this by programming the public key into Read Only  
17 Memory (“ROM”). ROM is hardwired during the manufacture of the semiconductor  
18 device and cannot be changed later through any software means. The firmware in ROM  
19 is the first code that executes on the processor when power is applied. According to  
20 Apple’s Security documentation, Apple products have also stored “the Apple Root CA  
21 [certificate authority] public key” within boot ROM.<sup>4</sup> (iOS Security at 5.) The boot  
22 ROM code uses the public key to verify that the next code to load (which is stored in  
23

---

24  
25 <sup>3</sup> In simplified terms, software is generally written by programmers in “source  
26 code.” That source code is converted (or “compiled”) into what is referred to as  
27 “executable code” that is in a format that a computer processor can understand and  
28 “execute.”

<sup>4</sup> Boot ROM is firmware that has been fused or hardwired into the processor during manufacturing. It cannot be changed.

1 memory outside the processor) has also been signed with Apple’s private key. (iOS  
2 Security at 5.)

3 15. This system ensures that Apple controls all code loaded and run on the  
4 device from the initial power-on. Apple describes how it has implemented this process  
5 in what it refers to as its “Chain of Trust” on pages 5-10 of its iOS Security document,  
6 wherein each sequential step needed to boot up the operating system and run application  
7 software relies on—and requires—Apple’s signature. Specific details include the  
8 following:

9 a. “Each step of the startup process contains components that are  
10 cryptographically signed by Apple to ensure integrity and that proceed only after  
11 verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and  
12 baseband firmware.” (*Id.* at 5.)<sup>5</sup>

13 b. “The Boot ROM code contains the Apple Root CA [certificate  
14 authority] public key, which is used to verify that the Low-Level Bootloader (LLB) is  
15 signed by Apple before allowing it to load. This is the first step in the chain of trust  
16 where each step ensures that the next is signed by Apple. When the LLB finishes its  
17 tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and  
18 runs the iOS kernel.” (*Id.*) A certificate authority is the entity that issues digital  
19

---

20 <sup>5</sup> A bootloader is the initial code run on a processor that starts the system’s  
21 hardware components and peripherals and prepares the hardware for the operating  
22 system or higher level code. There may be multiple bootloaders that are executed  
23 sequentially at startup. The kernel is the first part of an operating system that loads and  
24 is responsible for controlling access to the computer’s hardware resources. The kernel  
25 generally runs in protected memory to which other parts of the operating system and  
26 application code cannot directly read or write. Kernel extensions provide a method for  
27 adding or changing functionality of Apple’s kernel without recompiling/relinking the  
28 source code. A mobile device typically has multiple processors; the application  
processor running an operating system, such as iOS 9.02, with which the user interacts  
(via the screen and keyboard), and the baseband processor which handles network  
communications traffic and protocols. The application processor is responsible for  
starting (booting) the baseband processor. Therefore, the application processor provides  
the baseband processor with the code it needs to load and run. Thus, Apple’s chain of  
trust calls for each of these steps to be verified, ensuring that the next steps are  
authorized by Apple before allowing them to run or execute.

1 certificates. Certificate authorities create the public/private key pairs, and are  
2 responsible for ensuring the security of the private key. Apple has built its own  
3 certificate authority and has created its own public/private key pair used in the iPhone.  
4 As noted above, the public key is permanently programmed into the ROM of the iPhone,  
5 while the private key is controlled and protected by Apple. Because only Apple  
6 possesses its private key, only Apple is able to sign software that will be loaded on its  
7 devices. By keeping the private key secret, Apple ensures that only software signed by  
8 Apple using its private key can be loaded on its devices during the boot process.

9 c. “This secure boot chain helps ensure that the lowest levels of  
10 software are not tampered with and allows iOS to run only on validated Apple devices.”  
11 (*Id.*) “From initial boot-up to iOS software updates to third-party apps, each step is  
12 analyzed and vetted to help ensure that the hardware and software are performing  
13 optimally together and using resources properly.” (*Id.*)

14 d. “This architecture is central to security in iOS, and never gets in the  
15 way of device usability. The tight integration of hardware and software on iOS devices  
16 ensures that each component of the system is trusted, and validates the system as a  
17 whole.” (*Id.*)

18 16. “The startup process described above helps ensure that only Apple-signed  
19 code can be installed on a device.” (*Id.* at 6.) If any component can be made to load  
20 code not signed by Apple, the chain of trust is broken. By beginning their chain of trust  
21 with the initial code and public key programmed into the device ROM, Apple has made  
22 it extremely difficult for anyone to defeat the chain of trust.

23 17. As a result of these features, an Apple iPhone is designed to only run code  
24 (the operating system and the many pieces of firmware and software that may operate  
25 within it) that are signed using Apple’s keys.  
26  
27  
28

1                   **3. Apple “Signs” iOS Updates for Its iPhones that Include a Unique**  
2                   **Device Identifier, Ensuring It Only Works on One iPhone**

3                   18. While the features described above permit Apple to ensure that the devices  
4                   it manufactures will use only an operating system or software that Apple has authorized  
5                   (by signing it), Apple also relies on them to ensure that an operating system will work  
6                   only on one specific Apple device. Specifically, during an iOS update, recovery, or  
7                   Device Firmware Update (DFU) process, the device verifies that the code being loaded  
8                   to it was digitally signed specifically for that device, and not for another device. This  
9                   feature, enforced by the hardware-based chain of trust, allows Apple to ensure that any  
10                  code loaded to the phone will only operate on a specific device.

11               19. Apple implements this process in the following manner. First, the device  
12               connects to a computer, for example through iTunes, and provides iTunes with unique  
13               information about itself—both its hardware and software. Second, iTunes sends this  
14               information from the device to an Apple server that builds the package of code needed to  
15               update or recover that device, packages it with the same unique information about the  
16               device, and returns it to the computer running iTunes. Third, upon receiving that  
17               package from the computer running iTunes, the device is required to read and recognize  
18               its own unique information before installing the operating system.

19               20. Details of this process are as follows:

20               a. Apple maintains what it refers to as “the Apple installation  
21               authorization server,” which is referred to herein as the “Installation Server.” (iOS  
22               Security at 6.)

23               b. Whenever a device tries to upgrade its version of iOS, through the  
24               upgrade or recovery process, the device must first send to that server a set of information  
25               from the device. The information sent by the device includes “cryptographic  
26               measurements for each part of the bundle to be installed (for example, LLB, iBoot, the  
27               kernel, and OS image).” (*Id.*) Those measurements are a digest or partial digest of that  
28               component. (A digest can be a cryptographic hash, or the result of a similar algorithm

1 that generates a unique value, akin to a digital fingerprint, after it processes each part of  
2 the bundle.)<sup>6</sup> The device also sends a “nonce,” or a random, one-time-use value.

3 c. Most importantly for ensuring the “personalization” of the software  
4 for use on a specific device, the device also sends “the device’s unique ID (ECID).”  
5 (iOS Security at 6.) The ECID is a unique, device-specific identifier programmed into  
6 the phone hardware during manufacture. (*Id.* at 58 (defining ECID as “[a] 64-bit  
7 identifier that’s unique to the processor in each iOS device. Used as part of the  
8 personalization process, it’s not considered a secret”).) Apple explains the use of these  
9 values in their iOS Security document. “These steps ensure that the authorization is for a  
10 specific device and that an old iOS version from one device can’t be copied to another.”  
11 (*Id.* at 6.)

12 d. Once the Apple Installation Server receives this information from the  
13 device, it builds a software package and digitally signs it using a private key that is not  
14 known to the public. The digital signature includes the ECID, nonce, and other  
15 cryptographic measurements in the signed data. Once the device receives the package,  
16 the device verifies from the signed data that the package is meant for it.

17 e. The device is also able to tell that the installation is current and is not  
18 a repeat of an older installation (which would result in a “downgrade” of the operating  
19 system). The device does so by checking the random, one-time nonce it had sent to the  
20 server was the one returned by the server in the signed package. “The nonce prevents an

---

21 <sup>6</sup> “In cryptography, hashes are used when verifying the authenticity of a piece of  
22 data. Cryptographic hashing algorithms are essentially a form of (extremely) lossy data  
23 compression, but they are specifically designed so that two similar pieces of data are  
24 unlikely to hash to the same value. . . . With good hashing algorithms, collisions  
25 [messages that hash to the same value] are unlikely if you make small changes to a piece  
26 of data. This tamper-resistant nature of good hashes makes them a key component in  
27 code signing, message signing, and various other tamper detection schemes.” (Ex. 19 at  
28 3 (Apple developer website, Cryptographic Services).) By way of background, data  
compression that is “lossy” loses some qualities of the original data, such as when a  
compressed digital image loses resolution or appears “pixelated.” In the cryptography  
context, what is important is that the resulting hash value is unique, not that it be capable  
of reformulating the entire original piece of data, hence it “loses” data by being reduced  
to a small but unique string of letters and numbers.

1 attacker from saving the server’s response and using it to tamper with a device or  
2 otherwise alter the system software.” (*Id.* at 6.)

3 21. The digital signature prevents any part of the returned package from being  
4 changed. If the software in the returned package is altered, the digital signature check  
5 will fail and the device will not load it. If the ECID is changed to that of another device,  
6 the signature check will fail and the device will not load the code.<sup>7</sup> In other words,  
7 unless someone can bypass the digital signature verification, allowing them to load  
8 unsigned code, the software cannot be changed to operate on a different device or  
9 perform a different function.<sup>8</sup>

10 22. The Order provides that the SIF would only run on the Subject Device. As  
11 shown in the preceding description of Apple’s normal code signing process during an  
12 iOS update, Apple already has a mechanism in place to do this by including the ECID  
13 into the digital signature process. If this same or a similar process were used, the SIF  
14 could incorporate the ECID of the Subject Device, and then be signed by Apple. In that  
15 case, if the ECID of the SIF were changed to the ECID of another device, the signature  
16 check would fail and an Apple device would not load the code.<sup>9</sup>

---

17  
18 <sup>7</sup> As described on Apple’s developer website: “When a piece of code has been  
19 signed, it is possible to determine reliably whether the code has been modified by  
20 someone other than the signer.” (Ex. 21 at 1 (Apple developer website, Code Signing  
21 Overview).) Among the purposes of code signing are to “ensure that a piece of code has  
22 not been altered,” and to “identify code as coming from a specific source (a developer or  
23 signer).” (*Id.*)

24 <sup>8</sup> Because of the significance of the ability to digitally sign code and therefore  
25 cryptographically authenticate it, Apple’s developer website explains that a “signing  
26 identity, no matter how obtained, is completely compromised if it is ever out of the  
27 physical control of whoever is authorized to sign code.” (Ex. 22 at 2 (Apple developer  
28 website, Code Signing Tasks).)

<sup>9</sup> An additional measure to ensure the SIF would only run on the Subject Device  
could be to program the Subject Device’s ECID directly into the software running in the  
SIF. In this scenario, the SIF would read the ECID of the device on which it was  
running, and compare that to the ECID of the Subject Device that had been programmed  
into it; if the two did not match, the software would exit. In other words, while the iOS  
update scenario described in this Part relies on the *device’s* refusal to run the code  
without a valid Apple signature (which signature would be invalid by changing the  
ECID), the *SIF* could refuse to fully execute if it did not detect the Subject Device’s

(footnote cont’d on next page)

1           23. For these reasons, the SIF called for by the Order would be permitted to run  
2 only on the Subject Device. In other words, the creation of the SIF, tailored and signed  
3 with the unique identifier of the Subject Device, would not undermine the security of  
4 other iPhones that also require Apple-signed code, because each iPhone has its own  
5 unique identifier. The SIF proposed by the Order would therefore not break Apple’s  
6 chain of trust on its iPhones, or even on the Subject Device; Apple’s assistance will keep  
7 the chain of trust intact.

8           24. Importantly, if somebody were to bypass the Apple digital signature  
9 process, the chain of trust would be broken. Causing an Apple device to allow itself to  
10 run software not signed by Apple is referred to as “jailbreaking” the device. Jailbreaks  
11 result from bugs or errors in different programs that can be exploited to run unsigned  
12 code on a device. To my knowledge, for the iPhone 5C, jailbreaks have been  
13 exclusively performed from a powered-on phone on which the passcode has been  
14 entered and the phone unlocked. Thus there are currently no published jailbreaks for an  
15 iPhone 5C where the passcode has not been entered at least once since powering on, and  
16 hence there are none that could be applied to the Subject Device.

17           **C. Software Already Exists that Performs Similar Functions as the SIF**

18           25. The security features created and implemented by Apple that are described  
19 above were challenged by researchers and hackers as previous iterations of iOS were  
20 released. Apple’s current chain of trust structure has fixed previous issues, but the  
21 methods that have been published and used to test earlier versions of iPhones illustrate  
22 why the components used in the SIF already exist, and why it, like other previous tools,  
23 can be operated from random access memory (“RAM”).

24           26. Paragraph 19 of the Neuenschwander Declaration states that Apple’s  
25 “current iPhone operating systems designed for consumer interaction do not run in  
26

---

27 ECID. This example is designed to illustrate that there is more than one way to cause  
28 the SIF to only load and execute on the Subject Device.

1 RAM, but are installed on the device itself. To make them run in RAM, Apple would  
2 have to make substantial reductions in the size and complexity of the code.” As the  
3 discussion below illustrates, the SIF would not be designed for “consumer interaction.”  
4 Rather, the SIF would be designed only to test passcodes, and other similar tools that  
5 have previously been used for this purpose do run in RAM.

6 27. Those previous tools that are available cannot be used on the Subject  
7 Device because they are not signed by Apple, and the current chain of trust on the  
8 Subject Device requires Apple to have signed any software that will be allowed to run.

9 28. A more detailed description is as follows:

10 a. A previous bug allowed a cold-booted<sup>10</sup> iPhone to load a “minimal”  
11 operating system in memory (RAMdisk) that had not been signed by Apple. Previously,  
12 Apple iPhone versions 3GS and 4 contained a bug in the Apple boot ROM that allowed  
13 unsigned code to be loaded and run through Recovery or DFU mode. This vulnerability  
14 was published as the “limeraln” exploit. Other researchers analyzed the Apple boot  
15 process and published details of it, including the composition of the RAMdisk (*i.e.*,  
16 which software components were bundled into the RAMdisk) used in the Recovery  
17 mode and DFU mode process to update device firmware.

18 b. A passcode-recovery tool has already been developed that uses brute-  
19 force techniques. The information technology company Sogeti<sup>11</sup> analyzed Apple’s  
20 encryption process demonstrating that any passcode “guessing” had to be performed by  
21 code running on the device and could not be done externally (further explained below in  
22 Part D). Other vulnerability researchers used this result to develop software that could  
23 brute force the passcode on a jailbroken device (iphone-dataprotection project<sup>12</sup>).

24 \_\_\_\_\_  
25 <sup>10</sup> Cold-boot refers to a phone that has been powered off and then powered back  
26 on but no passcode has been entered.

27 <sup>11</sup> (Ex. 17 (<http://esec-lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf>.)

28 <sup>12</sup> (<https://code.google.com/archive/p/iphone-dataprotection>, “ios forensics tools,”  
and “Tools and information on iOS 3/4/5/6/7 data protection features.”)



1           c. From this open source research, several forensic tools were  
2 developed that combined (1) the boot ROM code signing defeat, and (2) brute-force  
3 passcode guessing. Examples include the Cellebrite UFED tool and an FBI-developed  
4 tool. Both the Cellebrite<sup>13</sup> and FBI tools utilize the boot ROM exploit, allowing iPhone  
5 3GS and iPhone 4 devices to load and boot an unsigned RAMdisk containing code to  
6 brute force the device passcode. The passcode recovery process operated from RAM,  
7 and did not alter the system or user data area. The passcode recovery software did not  
8 require user interaction, and the entire process ran without use of the “Springboard”  
9 graphical user interface. Because these forensic tools ran from a RAMdisk and did not  
10 use the operating system that was stored on the device, these tools did not incur time  
11 delays or the auto-erase function (which are features implemented by the operating  
12 system installed on the device).

13           d. Apple addressed the bug, and subsequently a jailbreak (i.e., allowing  
14 code unsigned by Apple) could only occur on an iPhone after it had been booted and  
15 unlocked. As described previously, a jailbroken phone is one that has had the chain of  
16 trust broken and can run unsigned code.<sup>14</sup> After Apple corrected the bug present in the

17           <sup>13</sup> Cellebrite is a private company that makes forensic data recovery tools for  
18 mobile devices. While I have not examined the source code for the UFED tool, based on  
19 the Cellebrite Physical Extraction Manual for iPhone and iPad (Rev 1.3) and the fact that  
20 the Cellebrite tool no longer supports iPhone 4S and later devices, I believe the UFED  
21 tool relied on the same ROM exploit. The manual states: “The extraction application  
22 does not load iOS but instead loads a special forensic utility to the device. This utility is  
23 loaded to the device’s memory (RAM) and runs directly from there.” The utility is  
24 loaded from recovery mode.

25           <sup>14</sup> The use of jailbroken phones discussed in this Part occurred in a testing  
26 environment. Outside of a testing environment, some users have jailbroken their phones  
27 to try to use software or services that Apple has not authorized, but Apple cautions that  
28 doing so presents “[s]ecurity vulnerabilities”: “Jailbreaking your device eliminates  
security layers designed to protect your personal information and your iOS device. With  
this security removed from your iOS device, hackers may steal your personal  
information, damage your device, attack your network, or introduce malware, spyware or  
viruses.” (Ex. 29 (<https://support.apple.com/en-us/HT201954>)). Furthermore, the  
jailbreaking process often results in deletion or alteration of data stored on the phone.  
As discussed in this Part, software already exists that performs certain functions that  
could be used in the SIF, and to the extent those software components could be used to  
undermine security, they (like the SIF) would only work on devices that had already  
assumed security vulnerabilities by being jailbroken.

1 iPhone 3GS and 4, all known jailbreaks have been applied from within the iPhone user  
2 interface, instead of during the boot process. There are publicly known jailbreaks for  
3 most recent iPhone OS versions (up to at least version iOS 9.0.2), but they can only be  
4 executed from an unlocked iPhone via the user interface, *i.e.*, after the iPhone had booted  
5 and had been unlocked. After these jailbreaks are applied, software that has not been  
6 signed by Apple may be run.

7 e. The same brute-force source code still works on jailbroken iPhones.

8 A software project named “iphone-dataprotection” includes a passcode recovery  
9 program that can still be compiled, loaded, and run within a jail-broken Apple device.  
10 The FBI tool used essentially the same functionality as this project but executed it from a  
11 RAMdisk. The FBI recently tested the iphone-dataprotection passcode recovery  
12 software on a jailbroken iPhone 6 Plus running iOS 8.4 (in which the passcode had been  
13 entered once). With minor modifications this software still functioned and was able to  
14 recover the passcode without incurring time delays. The FBI also tested this passcode  
15 recovery software on a jailbroken iPad Air 2 running iOS 9.02. In this device the  
16 passcode recovery software functioned, but it did incur the time delays and most likely  
17 would have erased the device.<sup>15</sup> However, this test does verify that the passcode  
18 recovery code works, which has existed for many years and still functions essentially the  
19 same. This specific code would not run on the Subject Device “as is,” because it is not  
20 signed by Apple and also because it would incur time delays and risk causing the device  
21 to erase, which would require further development and modifications to the kernel  
22 software.<sup>16</sup>

23  
24 <sup>15</sup> It should be noted that the iPhone 6 and iPad Air 2 both use the more advanced  
25 A8 processor and the time delay and erase functionality has moved into a separate  
26 security controller called the Secure Enclave.

27 <sup>16</sup> For example, in previous versions of iOS the time delay and password try count  
28 resided in the “springboard” user interface, which is in part what allowed the passcode  
recovery software to work and to bypass the time-delay and auto-wipe features. In  
approximately iOS 8.4, that functionality moved from the Springboard and would  
require further modification to bypass the delay and wipe functions.

1           f.     Only Apple can produce and sign the RAMdisk needed to run the  
2 passcode guessing code without first unlocking the iPhone. Beginning with the release  
3 of the iPhone 4S in 2011, Apple fixed the bug in the boot ROM. Since that time, the  
4 Apple chain of trust—which governs the boot process on an iPhone—has remained  
5 intact, preventing loading of unsigned RAMdisks. (The jailbreaks that have occurred on  
6 iPhones 5C or later have occurred after the boot-up process has occurred, and after a  
7 passcode has been entered; the chain of trust through the boot-up process remains intact  
8 on those phones.) However, the steps used in the Apple Recovery and DFU mode boot  
9 processes have not changed substantially since that time, and Apple’s use of a RAMdisk  
10 to perform the updates and device recovery processes appear consistent with the  
11 methodology of the earlier devices. Without assistance from Apple to digitally sign the  
12 code, however, it has not been possible to continue development of these tools for newer  
13 devices. The passcode-guessing software employed by these tools has been tested within  
14 jailbroken devices running an iOS that has already been booted and unlocked; neither the  
15 FBI, nor others to my knowledge, however, have been able to integrate the software into  
16 a RAMdisk to test passcodes from a cold-booted iPhone device since the iPhone 4.

17           29. As set forth above in the previous paragraph, there are already software  
18 components available that perform some of the functions of the SIF called for by the  
19 Court’s Order. Although code similar to what would be in the SIF already exists, it  
20 cannot be used on the Subject Device without Apple’s signature because of Apple’s  
21 robust security and code-signing practices.

22           **D. The Encrypted Data on the Subject Device Must Be Decrypted on the**  
23 **Subject Device Itself**

24           30. As described in paragraph 12 of the Initial Pluhar Declaration, an iPhone 5C  
25 running iOS 9 is encrypted using a combination of two components: one user-  
26 determined passcode, and one unique 256-bit key (referred to as a “UID”) fused into the  
27  
28

1 phone itself during manufacture. (iOS Security at 12; *id.* 11 (diagram); Neuenschwander  
2 Decl. ¶ 13.) These two different components are discussed below.

3 31. According to Apple’s documentation, the UID is unique to each device, is  
4 fused into the hardware, and is not known to Apple or anyone else, as described on page  
5 10 of iOS Security:

6 The device’s unique ID (UID) . . . [is] fused . . . into the application  
7 processor and Secure Enclave during manufacturing. No software or  
8 firmware can read them directly . . . . The UIDs are unique to each device  
9 and are not recorded by Apple or any of its suppliers. . . . The UID allows  
10 data to be cryptographically tied to a particular device. For example, the  
11 key hierarchy protecting the file system includes the UID, so if the memory  
12 chips are physically moved from one device to another, the files are  
13 inaccessible. The UID is not related to any other identifier on the device.

14 32. I know from Supervisory Special Agent (“SSA”) Pluhar that the Subject  
15 Device was powered off when the FBI found it. When the Subject Device was powered  
16 on, it displays a numerical keypad (like that on a telephone), and a prompts for four  
17 numbers to be entered.

18 33. With a four-digit numerical pin, there are only 10,000 possible passcodes.  
19 Testing 10,000 passcodes electronically would likely take less than a day, depending on  
20 how the SIF were configured.

21 34. Apple’s iOS Security also explains that because its passcodes are permitted  
22 to be weak in that they can be only four numbers, Apple has included additional features  
23 to discourage brute-force attacks. These features are described in paragraphs 13 and 14  
24 of the Initial Pluhar Declaration, and on page 12 of Apple’s iOS Security (noting that  
25 iOS 9 iPhones (1) escalate time delays between failed passcodes, and can (2) be  
26 configured to wipe their contents after ten failed passcodes, to “discourage brute-force  
27 passcode attacks”).

28 35. The UID is itself a strong encryption key. It is fused into the hardware and  
is both unknowable and unchangeable: it is always used the same way to create the  
encryption key. The only variable is the passcode.

1           36. Because both the UID, which is unique and embedded in the device itself, is  
2 a part of the encryption key (along with the user-generated passcode), the data that is  
3 stored on the Subject Device will need to be decrypted on the Subject Device. Because  
4 only Apple-signed software can run on the iPhone, and the decryption must occur on the  
5 Subject Device, any code or software tools needed to assist in testing passcodes must be  
6 signed using Apple's encryption keys.

7           **E. Apple's iCloud Backup**

8           37. I know from SSA Pluhar that the Subject Device was found in a powered-  
9 off state. Based on Apple's published documentation, open source research relating to  
10 Apple's encryption, and Apple press releases about iOS 8 and later encryption, I believe  
11 that (1) the device would not connect to a WiFi network until the passcode was entered,  
12 and (2) even if the device could be forced to perform an iCloud backup, the user data  
13 would still be encrypted with the encryption key formed from the 256 bit UID and the  
14 user's passcode.

15           38. Subsequent to seizing the Subject Device, the FBI performed several tests  
16 on exemplar phones to test whether a cold-booted iPhone could connect to a trusted  
17 WiFi network and perform a backup. The result of that testing was that cold-booted  
18 iPhones would not connect to a WiFi network.

19           a. To the best of my knowledge, a cold-booted iPhone will not connect  
20 to WiFi networks trusted by the Subject Device such as a home or work network until  
21 the passcode is entered. However, according to Apple and verified by the FBI, there are  
22 some WiFi networks inherently trusted by iOS, such as those operated by iPhone  
23 sponsors (referred to as carrier-sponsored WiFi). For example, an AT&T iPhone can  
24 automatically connect to an AT&T hotspot.

25           b. When the FBI tested a locked AT&T phone on which the passcode  
26 had been entered once by taking it to an area with an AT&T hotspot, the phone  
27 connected automatically to the hotspot, as indicated by the WiFi indicator on the top  
28

1 banner of the lock screen display. Additionally the “Find My iPhone” service was used  
2 and was able to locate the iPhone, verifying that a phone in which the passcode has been  
3 entered will connect, even when screen-locked, to a trusted WiFi network.

4 c. The same test was also done with the phone first powered off and  
5 restarted, but with the passcode not having been entered. In this scenario, the test phone  
6 did not show any indication it was connected to the AT&T hotspot through the banner.  
7 Additionally, the “Find My iPhone” service was unable to locate the device. The results  
8 of these tests show that WiFi is not enabled on the device until after the passcode is  
9 entered.

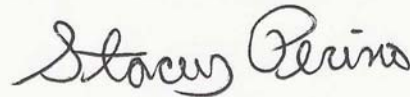
10 d. Further tests were conducted by myself and a colleague in CEAU by  
11 taking an iPhone 5 running iOS 9.02 and an iPhone 6 Plus running iOS 9.2 into a radio-  
12 frequency shielded chamber to test their electronic emissions. Both iPhones were fully  
13 charged, connected to power and had their WiFi enabled. The same series of tests was  
14 done on both phones with identical results. When the iPhone was not protected by a  
15 passcode and was powered on in that chamber, it began to emit signals in the frequency  
16 band of 2.4 gigahertz (GHz), a common band for WiFi connections. This is consistent  
17 with the iPhone trying to detect a WiFi network. When the iPhone *was* protected by a  
18 passcode and was powered on in the same chamber without entering the passcode, no  
19 emissions in the 2.4 GHz frequency band were detected. This indicates that the WiFi  
20 was not active. When the passcode was entered, WiFi 2.4GHz emissions were detected.  
21 The phone was allowed to screen lock after the passcode had been entered. Again,  
22 2.4GHz emissions were detected. Each phone was rebooted, no passcode entered, and  
23 left overnight in the chamber. No 2.4GHz signals were observed. These tests indicate  
24 the WiFi is not active on a cold-booted device until the passcode has been entered at  
25 least once.

1 e. The FBI does not know of any way to force an iPhone that has not  
2 had the passcode entered at least once since being powered on to perform an iCloud  
3 backup.

4 39. This result is consistent with Apple’s security documentation, which states  
5 that data stored on the device is encrypted using a key that is a combination of both the  
6 UID (the device-specific unique identifier) and the passcode generated by the user.  
7 Unless the passcode is entered by the user, the entire encryption key could not be used to  
8 decrypt the data, and the data therefore could not be backed-up to an iCloud—at least in  
9 a state that could be recovered outside the device.

10 I declare under penalty of perjury under the laws of the United States of America  
11 that the foregoing is true and correct and that this declaration is executed at

12 Virginia, on March 9, 2016.



13  
14 STACEY PERINO  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# **Exhibit P**



## Opinions

# Why the fear over ubiquitous data encryption is overblown

**Clarification:** Due to a production error, a version of this column was temporarily posted prematurely before the editing process was complete.

---

By Mike McConnell, Michael Chertoff and William Lynn July 28, 2015

*Mike McConnell is a former director of the National Security Agency and director of national intelligence. Michael Chertoff is a former homeland security secretary and is executive chairman of the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. William Lynn is a former deputy defense secretary and is chief executive of Finmeccanica North America and DRS Technologies.*

More than three years ago, as former national security officials, we penned an [op-ed](#) to raise awareness among the public, the business community and Congress of the serious threat to the nation's well-being posed by the massive theft of intellectual property, technology and business information by the Chinese government through cyberexploitation. Today, we write again to raise the level of thinking and debate about ubiquitous encryption to protect information from exploitation.

In the wake of global controversy over government surveillance, a number of U.S. technology companies have developed and are offering their users what we call ubiquitous encryption — that is, end-to-end encryption of data with only the sender and intended recipient possessing decryption keys. With this technology, the plain text of messages is inaccessible to the companies offering the products or services as well as to the government, even with lawfully authorized access for public safety or law enforcement purposes.

The FBI director and the Justice Department have raised serious and legitimate concerns that ubiquitous encryption without a second decryption key in the hands of a third party would allow criminals to keep their communications secret, even when law enforcement officials have court-approved authorization to access those communications. There also are concerns about such encryption providing secure communications to national security intelligence targets such as terrorist organizations and nations operating counter to U.S. national security interests.

Several other nations are pursuing access to encrypted communications. In Britain, Parliament is considering requiring technology companies to build decryption capabilities for authorized government access into products and services offered in that country. The Chinese have proposed similar approaches to ensure that the government can monitor the content and activities of their citizens. [Pakistan has recently blocked](#) BlackBerry services, which provide

We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.

First, such an encryption system would protect individual privacy and business information from exploitation at a much higher level than exists today. As a recent MIT paper explains, requiring duplicate keys introduces vulnerabilities in encryption that raise the risk of compromise and theft by bad actors. If third-party key holders have less than perfect security, they may be hacked and the duplicate key exposed. This is no theoretical possibility, as evidenced by major cyberintrusions into supposedly secure government databases and the successful [compromise of security tokens](#) held by a major information security firm. Furthermore, requiring a duplicate key rules out security techniques, such as one-time-only private keys.

Second, a requirement that U.S. technology providers create a duplicate key will not prevent malicious actors from finding other technology providers who will furnish ubiquitous encryption. The smart bad guys will find ways and technologies to avoid access, and we can be sure that the "dark Web" marketplace will offer myriad such capabilities. This could lead to a perverse outcome in which law-abiding organizations and individuals lack protected communications but malicious actors have them.

Finally, and most significantly, if the United States can demand that companies make available a duplicate key, other nations such as China will insist on the same. There will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications to a wide spectrum of governmental access regimes with varying degrees of due process.

Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interests. After all, political power and military power are derived from economic strength. If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential. And that imperative may outweigh the tactical benefit of making encrypted communications more easily accessible to Western authorities.

History teaches that the fear that ubiquitous encryption will cause our security to go dark is overblown. There was a great debate about encryption in the early '90s. When the mathematics of "public key" encryption were discovered as a way to provide encryption protection broadly and cheaply to all users, some national security officials were convinced that if the technology were not restricted, law enforcement and intelligence organizations would go dark

As a result, the idea of “escrowed key,” known as Clipper Chip, was introduced. The concept was that unbreakable encryption would be provided to individuals and businesses, but the keys could be obtained from escrow by the government under court authorization for legitimate law enforcement or intelligence purposes.

The Clinton administration and Congress rejected the Clipper Chip based on the reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the '90s and into the new century.

Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.

**Read more on this issue:**

[The Post's View: Putting the digital keys to unlock data out of authorities' reach](#)

[The Post's View: Compromise needed on smartphone encryption](#)

[Cyrus R. Vance Jr.: Apple, Google threaten public safety with default smartphone encryption](#)

---

# Exhibit Q



87 of 206 DOCUMENTS

Copyright 2016 ProQuest Information and Learning  
All Rights Reserved  
Copyright 2016 CNBC/Dow Jones Business Video  
Analyst Wire

March 1, 2016 Tuesday

**ACC-NO:** 28078

**LENGTH:** 3011 words

**HEADLINE:** Loretta Lynch - Interview

**DATELINE:** Lanham

**BODY:**

FULL TEXT

SCARLET FU, BLOOMBERG ANCHOR: "Bloomberg West" anchor Emily Chang is at the RSA Conference, that's the world's largest gathering of security experts, in San Francisco. She is joined right now by U.S. Attorney General Loretta Lynch.

EMILY CHANG, BLOOMBERG ANCHOR: Thank you, guys.

Thank you so much, Madam Attorney General Loretta Lynch, thank you so much for being here.

I also want to welcome our listeners from Bloomberg Radio.

LORETTA LYNCH, ATTORNEY GENERAL: Thank you for having me.

CHANG: So you say there is a middle ground between Apple and the FBI, and I would love some specifics. If there is a middle ground, where is it?

LYNCH: Well, we feel the middle ground between Apple and the FBI, where law enforcement and any company with whom we work, is the courts. That's who we go to to arbitrate these disputes. We have a difference of opinion as to what the law means or as to what compliance means or as to whether or not someone should comply, we go to court.

That's what we did in this case, and that's what we think is the current state of affairs, and that's where we think this dispute is going to play out.

However, as we've discussed, there is also the middle ground of discussing this in the larger forum of ideas in our

Loretta Lynch - Interview Analyst Wire March 1, 2016 Tuesday

country. Having a discussion about what it means to have both privacy and security. We do it all the time. People expect it of us. And we can do it in this case also.

CHANG: Now in the court, a Brooklyn judge just ruled that Apple doesn't have to do this in a separate case. Does that undermine your argument? Does that change your strategy?

LYNCH: No, it doesn't change our strategy or our reliance on the courts. In that case, obviously we were disappointed with that decision, but we will be resubmitting it to a judge in a few days with additional information.

I would also note that that was the case in which we were working very well with Apple. And they, in fact, had agreed to help us with that particular device, an older device. That particular case doesn't involve encryption or anything like it until the issue became public, and then they filed papers in opposition.

So we feel still that there is a path to discussion, to working on all of these issues as they come up.

CHANG: But Tim Cook says there is no middle ground that doesn't put everybody at risk. It's not just about one phone. It's about every phone and it's about the future. How do you respond to that?

LYNCH: Well, I think that in the present we've seen how we do, in fact, balance privacy and security every day. In fact, until recently, Apple was able to comply with our request, and they have some of the strongest security out there. And we haven't seen that parade of horrors ensue in those cases either.

So I think we have seen it done. We have our finance companies, we have our health care companies, all important sectors of the economy depends upon encrypting data to protect all of us, every single one of us.

But they also maintain the ability to manage that data to also keep us safe and secure.

CHANG: The government is asking for the same access in 12 other cases, 14 phones, as we understand it they range from drug dealers to general criminal activity, but not to terrorists. So I wonder where is the middle ground that is not a slippery slope?

LYNCH: Now I think that that particular fact indicates just how important our devices have become and how much data they contain on them. We're in a situation where, in so many cases, frankly, I think, in all cases that we at the DoJ do, we see a electronic evidence becoming paramount.

We still, of course, will get files of papers and boxes of documents, and rely on interviews with people, but electronic evidence is really what we are seeing in every case. That's how we store data, that's maintain data, that's how we access it through our devices.

So the fact that there are other phones just shows that in fact this issue is going to grow, but in every single one of those cases, the same as if we were looking to go into someone's house and look at some documents, we craft a request to court, we narrowly tailor it, we only want to look at what the law will allow us to look at.

And, as in every other case, if there is a third party that can provide assistance, Apple in this case, we go to them and first we ask them to help us voluntarily. Then if they feel that they can't do that, we then say, you know what, let's go to court and let's get some help in deciding that issue.

CHANG: So what does a compromise look like to you? I mean, how does this play out? Because it seems you're admitting it is about more than one phone.

LYNCH: Well, I think that's because phones have become so ubiquitous. But it really is about how do we access evidence anywhere? And we are applying the same principles that if we were trying to go into a home and look at a file full of some certain kinds of papers.

Loretta Lynch - Interview Analyst Wire March 1, 2016 Tuesday

We go to a court and we say, there's a narrow set of evidence that we need, and here's where it's located.

I think in this case it's really important to note that the customer, the actual customer of phone that is an issue in the (INAUDIBLE) case, is the one that has requested Apple's help.

So one way to simply resolve this is for Apple to work with its own customer and work out a way to resolve this issue.

CHANG: Now the premise of the of the government's position is that not having access to encrypted information is a security issue. But aren't companies like Apple that are creating products that can't be hacked into or infiltrated by cyber-terrorists, aren't they making us safer? Is the FBI, in making this request, inadvertently making us less safe?

LYNCH: Well, I think if you think about the current state of business affairs in which we have a situation where companies every day use and protect our data by encrypting it or by a variety of means they keep us safe, but they also retain the ability to respond to warrants, to respond court orders, to respond to their customers when the customer calls the bank and says, I need to get a copy of my last month's statement.

The bank doesn't say, you know what, it's encrypted and even I can't get a hold of it.

So we retain all the time the ability to do both things. And American industry, the greatest industry in the world, can certainly do that. We do it all the time. We can do it in this case.

CHANG: What do you say about the idea around Apple creating an unbreakable operating system? Something that the government cannot get into, do you believe the technology exists to do that? And if so, should the government stop it?

LYNCH: You know, I think you have to the tech people about that. I'm not an engineer and couldn't answer that question. I certainly think that innovation is important. I think that creativity is important. But I think that the reality is we are all in this together.

You know, we all are part of this great experiment called democracy, this great social compact that we have to look out for each other. And we've all agreed that no one is above the law.

And as I said before, were not against strong encryption, our only concern is with warrant-proof encryption. And I think that companies are developing things every day. Technology has changed so much in the last six months, two years, three years, and we don't know what is on the horizon. So I think it's really hard to say.

I do find it curious, though, that a company would say, you know what, when it comes to this issue, we are not going to go any further, we are going to basically lock this data away, throw away the key, and we're not going to give any thought to how we might need to access it for certain needs, we're not going to give any more thought to how we can comply with a court order when they continue to create and innovate in so many other important ways.

CHANG: Speaking of democracy, though, Apple is saying that doing this would infringe on my rights and your rights. Is there something to that argument?

LYNCH: You know, I think that obviously it's in everyone's interests to have strong privacy. But it's also in everyone's interests to have strong security. And the courts are where we have gone to balance those rights since the beginning of our democracy.

And that's why we have gone to court to try and get that neutral third party to give us an answer here, and why we are going to continue to raise the issue there as well continue to have those discussions.

We do this all the time. We balance privacy and security in so many areas. And in fact, part of the government's

Loretta Lynch - Interview Analyst Wire March 1, 2016 Tuesday

role is to support the strong privacy issues as well.

CHANG: Did the U.S. go to the NSA to try to break into this particular phone? And if not, why not?

LYNCH: You know, I can't comment on the specifics of the techniques that we may or may not have used, just because it's an ongoing investigation and we don't do that. In this instance we find ourselves with a situation where we would like to try and obtain information that's on that device.

By the way, we don't want Apple to break into the phone. We don't want Apple to go into the phone and pull data out. What we want them to do is essentially preserve the information on the phone and essentially disable the password blocker that would destroy that data as we try and gain access to it.

CHANG: But they say that that would compromise every phone. That someone could use that to get into my phone and your phone.

LYNCH: You know, I think that it's an interesting argument. And, again, I think that there are some very interesting technical issues here, but this is bigger than a technical issue, in particular when a company has been able to respond to government requests for help until their previous operating system.

So they clearly have the ability to do it. And in many of the devices that are talked about in some of the other cases, those devices predate the current operating system and don't even deal with the issue of encrypted data.

And there are devices where Apple actually has the ability to provide the assistance that they have done for years, but they have chosen not to in this instance.

CHANG: We're speaking with Attorney General Loretta Lynch here on Bloomberg Television and Bloomberg Radio, specifically about this ongoing standoff between Apple and the FBI.

In an interview with FOX News yesterday, you said one of the things that keeps you up at night is threats to our corporate IP and corporate property. You also expressed concerns for U.S. vulnerabilities to Chinese economic espionage.

How is forcing Apple to develop less secure products or a less secure solution to a particular situation not in contradiction to those concerns?

LYNCH: Because in fact the discussion about how we protect corporate IT, intellectual property, how we deal with economic espionage, involves so much more than just one company.

It's a great company. They make beautiful products, but this is so much more than just one company and how they've chosen to build a certain set of devices.

It's about how we track bad actors as they try and infiltrate our systems. It's about how we identify actors as they try and infiltrate our systems. It's about issues that are not tied to a specific device or specific commercial venture or marketing structure, but are about how do we deal with other governments.

That involves diplomacy. It involves law enforcement issues. And it also involves making sure that we keep an eye on what they are doing in processes such as the FBI's investigative efforts.

We work very closely with industries across the board, not just the tech companies, but the financial industries, health care industries, to talk about threats that they are seeing, what are they investigating.

We provide assistance. They provide information to us so that we can all create a profile of what the latest attack may be. These vary from industry to industry, company to company, so that issue is much, much bigger than Apple.



Loretta Lynch - Interview Analyst Wire March 1, 2016 Tuesday

In this instance, as we've said in our court papers, we're asking Apple to do what it has done for years, help us preserve information on a device so that we can try and see if there is relevant data to a terrorist investigation.

CHANG: Now some lawmakers are working to draft legislation that deals with encryption, specifically will the administration seek legislation? And what kind? Have you seen any drafts from senators Burr or Feinstein?

LYNCH: I have not seen drafts at this time. Obviously whenever senators propose legislation, it is something that we look at. And we have not propose that particular fix because we have felt that discussions with companies, and, again, it's more than just one company, more than one issue, we have found that that to be the most effective way to deal with this issue.

Certainly if the debate grows, it may be something that comes up. And, again, we would welcome everyone's participation in the discussion about that.

You know, we have important decisions to make about how we are going to conduct investigations, how we are going to manage the continued balance of privacy and security in here. And the more people are involved in this, the better.

CHANG: Now everybody wants to know about the one thing that you can't speak about, Hillary Clinton's emails. And I wonder why have you been so hesitant to speak about them given that they could have such a huge impact on a really consequential, and some might say scary, election?

LYNCH: Well, I think the answer to that is, why do we not talk about any investigation? We don't talk about open investigations or matters within the Department of Justice. That's a matter -- it's a policy.

It's governed by law. It's governed by policy. It's governed by fundamental fairness to anyone who might be involved in that. And we don't talk about ongoing matters.

What I will say about that matter is what I have said, which is that I understand people's fascination with it, but it is a matter -- it's a review of how classified information was handled by one agency.

It is similar to many others that we have conducted over time. And it's going to be handled like every other investigation in that category, by independent career lawyers. And they're going to look at all the facts and all the evidence, and they're going to come to a conclusion.

CHANG: Donald Trump is getting endorsed by the Ku Klux Klan. And there is some controversy about how he felt about that endorsement, but he has now disavowed it. How do you feel this kind of rhetoric affects America? And are you surprised we're in this situation, in 2016? In 2016, are you surprised that we are talking about this?

LYNCH: Well, you know, I don't have any comment on any of the candidates and the issues that they are facing. I think they've got enough to deal with that.

I think it's unfortunate that the Klan continues to be a force within America. I think, you know, frankly, we've always talked about balancing privacy and security, our First Amendment protects all kinds of speech, even hateful speech.

My concern is when that speech crosses the line into inciting violence. And certainly I think that the Klan as an organization is not consistent with our American values.

CHANG: Your office is responsible for enforcing violations of anti-discrimination legislation. The tech community and many others are currently debating how they can improve gender and racial diversity. Is it something that you're tracking?

Loretta Lynch - Interview Analyst Wire March 1, 2016 Tuesday

LYNCH: Well, we're not tracking it specifically, but I certainly applaud those efforts. Our country has always been better when there has been diversity of thought, diversity of background, diversity of culture participating in the marketplace of ideas.

And certainly the tech industry is founded on those principles of innovation, of creativity, of thinking outside the box. So the more that they can bring different voices and different backgrounds into that debate, the stronger we will all be.

CHANG: With the death of Justice Scalia, the administration is gearing up for a Supreme Court nomination fight. Will the president be submitting a nominee? Will it be you? Are you interested?

(LAUGHTER)

LYNCH: Well, the president has spoken and has stated his intentions as to what he's going to do. He does intend to submit a nominee. I do not know who that nominee will be. I will say that I am very happy in what is the greatest job in the world, in my opinion, as attorney general.

CHANG: And what is the one thing you would like to accomplish before the end of your term that won't be done by a Republican attorney general?

LYNCH: You know, I don't speculate on that because in my view the role of the Department of Justice and law enforcement in general is something that isn't dependent on party affiliation.

All of us who have a concern for the safety and the security of the American people take it very seriously, no matter what letter might be beside our name. And all of us work very hard toward that goal.

CHANG: Attorney General Loretta Lynch, thank you so much for joining us today here on Bloomberg Television and Bloomberg Radio.

LYNCH: Thanks for having me.

CHANG: Nice to have you.

16:20

END

[Copy: Content and programming copyright 2016 CNBC/Dow Jones Business Video, a division of CNBC/Dow Jones Desktop Video, LLC. Copyright 2016 Roll Call, Inc. All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of Roll Call. You may not alter or remove any trademark, copyright or other notice from copies of the content.]

**LOAD-DATE:** March 4, 2016

# **Exhibit R**

CQ CONGRESSIONAL TRANSCRIPTS  
Congressional Hearings  
March 1, 2016 - Final

# House Judiciary Committee Holds Hearing on Encryption Security and Privacy, Panel 2

## LIST OF PANEL MEMBERS AND WITNESSES

PETERS:

So listen, I want to thank you for being here. I wanted to just conclude by saying that I didn't hear very -- did listen carefully to your opening statement. I thought it was very constructive. I think you appreciated the two objectives we have here which is to both preserve privacy and to deal with San Bernardino. You heard that comment hard cases make bad law. They're still hard cases and the problem we see in terrorism now is this, the onesies and the twosies and the notion that we would have invulnerable communications I think is something that we should all be concerned about.

I hope that you and the panel to follow you all be part of the constructed discussion if you got a way to serve both objectives and that the lines won't be too hard drawn on either side so we can do that. And I appreciate Mr. Chairman the chance to thank Director Comey for being here and I look forward to the next panel.

COMEY:

Thank you.

PETERS:

I yield back.

GOODLATTE:

Sure, thanks gentlemen.

Director, you've donated three hours of your time to our efforts today, or more, I'm sure in getting ready so we thank you very much for your participation and for answering a multitude of questions and we are looking for answers so if you have more to add to the record later, we would welcome that as well. Thank you very much.

COMEY:

Thank you, sir.

ISSA:

Chairman, would you entertain a unanimous consent while we're changing panels?

GOODLATTE:

I would.

ISSA:

And I would ask unanimous consent that a letter I received late yesterday from a constituent in the technology business concerning this case be placed in the record. This is Emily Hirsch.

GOODLATTE:

Without objection, we will be made it a part of the record. We ask the witnesses on the second panel to please come forward and be seated.

And now that Mr. Sewell has been afforded similar attention to the attention previously accorded to Director Comey, I'd ask that the press move back so we can begin the second panel.

(UNKNOWN)

Mr. Chairman, I would not assume that was not directed to Miss Landau, this photography.

GOODLATTE:

Thank you. We welcome our distinguished witnesses for today, the second panel. And if you would all, please rise. I'll begin by swearing you in.

Do you and each of you swear that the testimony that you're about to give shall be the truth, the whole truth and nothing but the truth, so help you God?

(UNKNOWN)

I do.

Thank you very much. The record reflect that all the witnesses responded in the affirmative and I'll now introduce the witnesses.

Bruce Sewell is senior vice president and general counsel of Apple. Mr. Sewell serves on Apple's legal team and oversees all legal matters, including global security and privacy. Prior to joining Apple, Mr. Sewell was deputy general counsel and vice president of Intel Corporation. He received his Bachelors Degree from the University of Lancaster and a J.D. from George Washington University.

Dr. Susan Landau is professor of Cyber Security Policy at Worcester Polytechnic Institute. Originally trained as a theoretical computer scientist, Dr. Landau is an expert in cryptographic applications. Within cyber security policy, her work focuses specifically on communication surveillance issues. Dr. Landau earned a Bachelors Degree from Princeton University, a masters from Cornell University and a PhD from the Massachusetts Institute of Technology.

Our final witness, Mr. Cyrus Vance Jr., is the district attorney of New York County. Mr. Vance is currently serving his second term as district attorney after being re-elected in 2013. He also serves as co-chair of the New York State Permanent Commission on Sentencing. Previously, Mr. Vance worked in private practice and taught at Seattle University School of Law. He is a graduate of Yale University and the Georgetown University Law Center.

All of your written statements will be entered into the record in their entirety and we ask that each of you summarize your testimony in five minutes or less. To help you stay within that time, there's a timing light on the table. When the light switches from green to yellow, you have one minute to conclude your testimony. And when the light turns red, that's it, your time is up.

And we'll begin with you, Mr. Sewell. Welcome.

SEWELL:

Thank you very much, Mr. Chairman. Thank you members of the committee and ranking member.

GOODLATTE:

Make sure that microphone is on and pulled close.

SEWELL:

Thank you for that technology. Thank you, Mr. Chairman. It's my pleasure to appear before you and the committee today on behalf of Apple.

We appreciate your invitation and the opportunity to be part of the discussion on this important issue, which centers on the civil liberties that are at the foundation of our country. I want to repeat something that we've said since the beginning that the victims and the families of the San Bernardino attacks have our deepest sympathies. We strongly agree that justice should be served and Apple has no sympathy for terrorists.

We have the utmost respect for law enforcement and share their goal of creating a safer world. We have a team of dedicated professionals that are on call 24 hours a day, seven days a week, 365 days a year to assist law enforcement. When the FBI came to us in the immediate aftermath of the San Bernardino attacks, we gave them all the information we had related to their investigation. And we went beyond that by making Apple engineers available to advise the FBI on a number of investigative alternatives.

But now, we find ourselves at the center of a very extraordinary circumstance. The FBI has asked a court to order us to give them something that we don't have, to create an operating system that does not exist. The reason it doesn't exist is because it would be too dangerous. They are asking for a backdoor into the iPhone, specifically, to build a software tool that can break the encryption system which protects personal information on every iPhone.

As we have told them, and as we told the American public, building that software tool would not affect just one iPhone. It would weaken the security for all of them. In fact, just last week, Director Comey agreed and I think we heard the same here today that the FBI would likely use this as precedent for other cases involving other phones. We've heard from District Attorney Vance who's also said that he absolutely plans to use this tool on over 175 phones that he has in his possession.

We can all agree this is not about access to one iPhone. The FBI is asking Apple to weaken the security of our products. Hackers and cyber criminals could use this to wreak havoc on our privacy and personal safety. It would set a dangerous precedent for government intrusion into the privacy and safety of its citizens. Hundreds of millions of law-abiding citizens trust Apple's products with the most intimate details of their daily lives, photos, private conversations, health data, financial accounts and information about a user's location and the location of that user's family and friends.

Some of you may have an iPhone in your pocket right now and if you think about it, there's probably more information stored on that device than a thief could steal by breaking into your house. The only way we know to protect that data is through strong encryption.

Every day, over a trillion transactions occur safely over the internet as the result of encrypted communications. This range from online banking and credit card transactions to the exchange of health care records, ideas that will change the world for the better and communications between loved ones. The U.S. government has spent tens of millions of dollars through the open technology fund and other U.S. government programs to fund strong encryption. The review groups on intelligence and communications technology convened by President Obama urged the U.S. government to fully support and not, in any way, subvert, weaken or make vulnerable generally available commercial software.

Encryption is a good thing. We need it to keep people safe. We have been using it in our products for over a decade. As attacks on our customer's data become more sophisticated, the tools we need to use to defend against them need to get stronger too. Weakening encryption would only hurt consumers and well-meaning users who rely on companies like Apple to protect their personal information.

Today's hearing is entitled, "Balancing America's Security and Privacy". We believe we can and we must have both. Protecting our data with encryption and other methods preserves our privacy and keeps people safe. The American people deserve an honest conversation around the important questions stemming from the FBI's current demand.

Do we want to put a limit on the technology that protects our data and, therefore, our privacy and safety in the face of -- in the face of increasingly sophisticated cyber attacks? Should the FBI be allowed to stop Apple or any company from offering the American people the safest and most secure products it can make? Should the FBI have the right to compel a company to produce a product it doesn't already make to the FBI's exact specifications and for the FBI's use?

We believe that each of these questions deserves a healthy discussion and any decision should only be made after a thoughtful and honest consideration of the facts. Most importantly, the decision should be made by you and your colleagues as representatives of the people rather than through a warrant request based on a 220-year-old statute.



As Judge Weinstein concluded yesterday, granting the FBI's request would thoroughly undermine fundamental principles of the constitution. At Apple, we are ready to have this conversation. The feedback and support we're hearing indicate to us the American people, too. We feel strongly that our customers, their families, their friends and their neighbors will be better protected from thieves and terrorists if we can offer the best protections for their data at the same time our freedoms and liberties we all cherish will be more secure. Thank you for your time. I look forward to your questions.

GOODLATTE:

Thank you, Mr. Sewell. Ms. Landau, welcome.

LANDAU:

Thank you, Mr. Chairman and members of the committee. Thank you very much for the opportunity to testify today.

The FBI has pitched this battle as one of security versus privacy but a number of the members have already observed it's really about the security versus security. We have a national security threat going on and we haven't solved the problem at all. What the smartphones got to do with it? Absolutely everything. Smartphones hold our photos and music, our notes and calendars, much of that information sensitive, especially the photos.

Smartphones are increasingly wallets and they give us access to all sorts of accounts. Bank accounts, drop box and so on. Many people store proprietary business information on their smartphones even though their personal smartphones even though they know they shouldn't.

Now, NSA will tell you that stealing login credentials is the most effective way into a system. In fact, Rob Joyce of the Tailored Access Operations said so in a public talk a month ago. Here is where smartphones are extremely important. They are poised to become authenticators to a wide variety of systems, the services. In fact, they are already being used that way, including at some high-place government agencies.

Now, District Attorney Vance will tell you that -- has said that large-scale data breaches have nothing to do with smartphone encryption, but that's not true. Look at today's New York Times where there's a story about the attack on the Ukrainian power grid. How did it start? It started by the theft of login credentials, of system operators. We've got to solve the login authentication problem and smartphones are actually our best way forward to do it, but not if it's easy to get into the data of the smartphones.

Now, the committee has already observed that there are many phones that will be -- that will go through the process of being unlocked, not just the one in San Bernardino. And what that means for Apple is that it's going to have to develop a routine to do so. Now, what happens when you have -- when you sign a piece of code to update a phone and you're signing a piece of codes that's an operating system affirm where you do it once? You do it occasionally? It's a whole ritual and there are very senior people involved. But, if you're dealing with phones that are daily being updated in order to solve law enforcements cases, then what happens is you develop a routine. You get a webpage. You get a low-level employee to supervise it. And then it becomes a process that's easy to subvert.

I have lots of respect for Apple's security, but not when it becomes a routine process to build an update for a phone. And what will happen is organized crime or nation-state will do so, using an update to then hack into a phone, maybe the phone of the Secretary of the Chief of the Federal Reserve, maybe a phone of an HVAC employee who's going to go service a power plant. What we're going to do is decrease our security. That's the security risk that's coming from the requests.

Now I get that law enforcement wants data protection that allows them access under legal authorization. But an NSA colleague once remarked to me that while his agency have the right to break into certain systems, no one ever guaranteed that that right would be easy to do so. The problem is when you build a way in for someone who isn't the owner to get us the data, well, you built a way in for somebody else to get in as well.

Let me go to Caliah (ph) for a moment. Caliah (ph) is the security nightmare. I know that Congress has intended it that way but that's what it is. If you'll ask the signal as intelligence people they'll to you. There are many ways for nefarious sorts to take advantage of the opening offered by law enforcement. Instead of embracing the communications and device security we still badly need, law enforcement has been pressing to preserve 20th century investigative techniques. Meanwhile, our enemies are using 21st technologies against us.

The FBI needs to take a page from the NSA. You may recall that in the late 1990s, the NSA was complaining it was going deaf from encrypted calls? Well, they've obviously improved their technology a great deal. According to Mike McConnell, from that time until now, NSA had better sigint than any time in history. What we need is law enforcement to developed 21st century capabilities for conducting electronic surveillance.

Now, the FBI already has some excellent people and expertise but FBI investment and capacity is not at the scale and level necessary. Rather than

asking industry to weaken protections, law enforcement must instead develop a capability for conducting sophisticated investigations themselves.

Congress can help. The FBI needs an investigative center with agents with deep technical understanding of modern telecommunications technology and also because all phones or computer, modern computer -- deep and expertise in computer science, only the teams of researchers, who understand various types of field of devices.

They'll need to know where technology is and where it will be in six months and where it will be in two to five years, communications technology in two to five years so that they can develop the surveillance technologies themselves. Expertise need not be in house. The FBI could pursue a solution where they develop some of their own expertise and closely manage contractors to do some of the work.

But however, the bureau pursues the solution it must develop modern state of the art capabilities. It must do so rather than trying to get industry to weaken security. Your job is to help the FBI build such capabilities, determine the most efficient and effective way that such capabilities could be utilize by state and local law enforcement for they don't have the resources develop that themselves and to also fund that capabilities.

That's the way forward that does not put our national security at risk. It enables law enforcement investigations while encouraging industry to do all it can do to develop better and more effective technologies for securing data and devices. That was a win-win and where we should be going. Thank you.

GOODLATTE:

Thank you, Ms. Landau. Mr. Vance, welcome.

VANCE:

Thank you. Good afternoon, Chairman Goodlatte, Ranking Member Conyers and members of the House Judiciary Committee. Thank you so much for allowing me to participate today.

I'm testifying as a district attorney but on behalf of the National District Attorneys Association. And I'm very grateful for you giving us the opportunity to be here because much of the discussion in the prior panel and in the comments by the other speakers here has been about the federal government and about the issue of security and cyber crime in the federal context. But it's important, I think, for us to recognize that state and local law

enforcement agencies handle 95 percent of the criminal cases each year around the country. So, we have a very deep interest in the subject matter of this hearing today and thank you for allowing us to participate.

Apple and Google's decision to engineer their mobile devices to, in an essence, be warrant-proof has had a real effect on the traditional balance of public safety versus privacy under our Fourth Amendment jurisprudence and I agree with the comments, I think, of everyone here, including the many members of the house that we really need Congress to help solve this problem for us and it's -- why it so important that you are undertaking this effort. But I think in looking at this issue there are some basic facts from the state law perspective that really are very important to this debate but are not in dispute.

And number one, as Tim Cook said in his open letter to his customers of Apple of February 16th of this year, smartphones, led by iPhone, have become an essential part of our lives. Nothing could be more true. We are all using our cell phones for every aspect of our lives.

Number two, is that smartphones are also essential to criminals. Our office investigates and prosecutes a huge variety of cases from homicide to sex crimes, from international financial crime and including terrorism cases. And criminals in each of those cases use smartphones to share information, to plan and to commit crimes, whether it's through text messages, photographs or videos.

Number three, criminals know that the iOS 8 operating system is warrant-proof. Criminals understand that this new operating system provides them with a cloak of secrecy. And they are, ladies and gentlemen, quite literally, laughing at us. And they are astounded that they have a means of communication totally secure from government reach. And I don't ask you to take my word for it. In one lawfully recorded phone conversation from Rikers Island in New York, an inmates talking about the iOS 8 default device encryption called it and I'm quoting, a gift from God.

Number four, the encryption Apple provided on its mobile devices prior to iOS 8, that is before October 2014, was represented to be both secure for its customers and, importantly, was amenable to court authorized searches. We know this because Apple told us this.

Apple characterized its iOS 7 operating system as the ultimate in privacy. It touted its proven encryption methods and assured its users that iOS 7 could be use with confidence in any personal or corporate environment. During the time when iOS 7 was the operating system, Apple also acknowledged that its

responsibility to help, again in Apple's own words, police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease or hoping to prevent the suicide.

So Apples experienced, I believe, with iOS 7 demonstrated that strong encryption and compliance with court orders are not mutually exclusive. Default device encryption has had a profound impact on my office and others like it. In November of 2015 my office published a white paper on public safety and encryption and in that -- and that time, there were 111 iPhones from which we were locked out, having obtained search warrants for those devices.

Now, two and a half months later, when we submitted our written testimony for this committee, the number was 175. Today, it is 205, which represents more than one out of four the approximately 700 Apple devices that have been analyzed by our office's own cyber lab since the introduction of iOS 8. And of course that problem isn't just in Manhattan.

Prosecutors in Houston had been locked out of more than 100 iPhones last year, 46 in Connecticut, 36 in Chicago since January and those are just a few of the thousands of phones taken at evidence each year around the country. So centuries of jurisprudence that have been talked about today have held that no item, not a home, a file cabinet, a safe or even a smartphone just beyond the reach of the court order search warrant. But the warrant-proof encryption today gives two very large companies, we believe, functional control over the path to justice for victims of crime, including who could be prosecuted and, importantly, who may be exonerated.

So, our point, Mr. Chairman, is that we believe this line being drawn which is in public safety in privacy is extremely important. It's affecting our lives. It's affecting our constituent's lives and we believe that you should be drawing it and we ask you to address this problem quickly. Time is not a luxury for state and local law enforcement. Crime victims or communities can afford it. Our laws require speedy trials. Criminals have to be held accountable and victims are, as we speak, and we know in this audience, asking for justice.

GOODLATTE:

Thank you, Mr. Vance. We'll now be proceed with questioning of the witnesses under the five-minute rule and I'll begin by recognizing myself.

Mr. Sewell, Director Comey created a dichotomy between this being a technology problem or a business model problem and said that Apple was addressing this as a business model problem. Is that a fair contrast or is this something else?

SEWELL:

It's by no means a fair contrast, Mr. Chairman. I've heard this raised before. It was raised in New York. It's been raised in San Bernardino and every time I hear this, my blood boils. This is not a marketing issue. That's a way of demeaning the other side of the argument. We don't put out billboards to talk about our security. We don't take out ads that market our encryption. We're doing this because we think that protecting the security and the privacy of hundreds of millions of iPhone users is the right thing to do. That's the reason we're doing this.

And to say that it's a marketing ploy or that it's somehow about P.R., it really diminishes what should be a very serious conversation involving this Congress, the stakeholders, the American people. Just with respect to the New York case, Judge Orenstein last night took on this issue head on and he said, in footnote 14 on page 40, he said, "I reject the government's claim. I find Apple's activities and the position that they are taking conscientious and not with respect to P.R. or marketing."

GOODLATTE:

Director Comey and Mr. Vance seem to suggest that the security provided by encryption on prior devices is fine. But advancing encryption technology is a problem. What do you think about that?

SEWELL:

So, it's important to understand that we haven't started on a path of changing our technology. We haven't suddenly come to the notion that encryption, security and privacy are important. At Apple this began back in 2009 with our encryption of FaceTime and iMessage. We've been on path from generation to generation as the software and the hardware allow us to provide greater security and greater safety in privacy to our customers. What happened between iOS 7 and iOS 8 was that we were able to transform the encryption algorithm that is used within the software and the hardware of the phone to provide a more secure solution.

GOODLATTE:

We are moving to end-to-end the encryption on many devices and apps not just Apple iPhones. Why is that happening?

SEWELL:

I think it's a combination of things. From our perspective at Apple, it's because we see ourselves as being in an arms race, in an arms race with criminals, cyber terrorists, hackers. We're trying to provide a safe and secure place for the users of our devices to be assured that their information cannot be accessed, cannot be hack or stolen. So from our perspective that end-to-end encryption move is an effort to improve the safety and security of our phones.

From the terrorist perspective, I think it's an effort to communicate in ways that cannot be detected. But the terrorists are doing this independently of the issues that we're discussing here today.

GOODLATTE:

Now, if the FBI succeeds in getting the order that is in dispute that Apple has appealed to a final resolution overlying that takes and they then get Apple to develop this device that will allow the 10 times and your -- by the way, all of us here, we can't turn that off, so.

SEWELL:

But we could show you how to do that.

GOODLATTE:

I know but inside our firewall here, we can't do that. So, we understand the reason. But that creates a separate vulnerability, does it not, for people who device falls to be apprehended (ph), they could willfully try 10 times and erase whatever hasn't been backed up on the device. For me that as it may, if they were to get you to develop that code and apply it and then to crack the four-digit code to get into the device, once they get in there, they could find all kinds of other restrictions that Apple has no control over, right, with regard to apps that are on the phone, with regard to various other communications features that the consumer may have chosen to put on there. Is that correct?

SEWELL:

That's absolutely right, Mr. Chairman. One of the most pernicious apps that we've seen in the terrorist space is something called telegraph. Telegraph is an app that can reside on any phone. It has nothing to do with Apple. It can be loaded either over the internet or it could be loaded outside of the country. And this is a method of providing absolutely unencrypt -- uncrackable communications.

What happens here is that Apple is forced to write a new operating system to degrade the safety and security in phones belonging to tens or hundreds of millions of innocent people. It will weaken our safety and security but it will not affect the terrorists in the least.

GOODLATTE:

Thank you very much. My time has expired. The gentleman from Michigan, Mr. Conyers, is recognized for five minutes.

CONYERS:

Thank you, Mr. Chairman, and welcome to the witnesses. Let me start off with Professor Landau. Director Comey has just testified that until the invention of the smartphone, there was no closet, no room, no basement in America that the FBI could enter. Did encryption exist before the invention of the iPhone?

LANDAU:

Encryption has existed for centuries and in particular they've been fights over encryption and the use of encryption in the '70s about publication, in the '80s about, whether NIST or the NSA would control the development of encryption for non-national security agencies, in the '90s about whether there would be export controls on devices with strong encryption.

The White House changed those rules in 2000. We expected to see widespread use of strong encryption on devices and on applications and the technologist's response to Apple is, "What took you guys so long?" How in the face of all the cyber security problems that we've had did it take industry so very long to do this?

CONYERS:

Well, as our technical expert, let me see this. Is there any functional difference between asking Apple to break its own encryption and what FBI has demanded in California?

LANDAU:

I'm sorry. Asking Apple to break -- I don't quite understand the question.

CONYERS:

All right.



LANDAU:

What Apple is being asked to is to subvert the security controls and go around. So it's not breaking the encryption but it's subverting its own security controls.

CONYERS:

Right.

LANDAU:

And is there any functional difference between that end (ph)?

CONYERS:

And what the FBI has demanded in California?

LANDAU:

What has demanded in California is that Apple subverts its own security controls.

CONYERS:

Let me ask Mr. Bruce Sewell the same question. What is the functional difference between ordering Apple to break its encryption and ordering apple to bypass its security so the FBI can break the encryption?

SEWELL:

Thank you, Ranking Member. Functionally, there is no difference. What we're talking about is an operating system in which the passcode is an inherent and integrated part of the encryption algorithm. If you can get access to the passcode, it will affect the encryption process itself. What we're being asked to do in California is to develop a tool, atoll which does not exist at this time that would facilitate and enable the FBI in a very simple process to obtain access to the passcode. That passcode is the cryptographic. So essentially, we are throwing open the doors and we are allowing the very act of decryption to take place.

CONYERS:

I was hoping you'd go in that direction. Let me ask you do this, there's been a suggestion that Apple is working against law enforcement and that you no longer respond to legal process when investigators need your assistance. Is

SEWELL:

It's absolutely false. As I said in my opening statement, we care deeply about the same motivations that motivate law enforcement. The relationship with law enforcement falls within my job at Apple. The people that we have who assist law enforcement everyday are part of my team and I'm incredibly proud of the work they do. We have dedicated individuals who are available around the clock to participate instantly when we get a call. As we discussed a little bit earlier in Director Comey...

CONYERS:

I want to squeeze in one more question before my time runs out.

SEWELL:

All right. I'll try to be very quick. We do everything we can to assist law enforcement and we have a dedicated team of people who are available 24/7 to do that.

CONYERS:

Why is apple taking this stand? What exactly is at stake in the San Bernardino case?

SEWELL:

This is not about the San Bernardino case. This is about the safety and security of every iPhone that is in use today. And I'd like to address one thing that Director Comey raised. This is -- there's no distinction between a 5C and a 6 in this context. The tool that we're being asked to create will work on any iPhone that is in use today. It is extensible. It is common. The principles are the same. So the notion that this is somehow only about opening one lock or that there is some category of locks that can't be open with the tool that they're asking us to create is a misnomer. It's something that we needed to clarify.

CONYERS:

Thank you for your responses.

GOODLATTE:

The chair recognizes the gentleman from Wisconsin, Mr. Sensenbrenner, for five minutes.

SENSENBRENNER:

Thank you very much, Mr. Sewell. And I think you know that I have been one of the privacy hawks on this committee. The whole debate over the USA Freedom Act was whether the NSA should go to court and give them some time of an order or a warrant specifically miming the person or persons whose data is requested. Here, the FBI, you know, has done that. In your prepared testimony, you said the questions about encryption should be decided by Congress rather than through a warrant based on a 220-year-old statute. I point out the Bill of Rights is about the same age. Now, the FBI is attempting to enforce a lawful court order. Apple has every right to challenge that order as you have done but why is Congress and not the court the best venue to decide this issue?

SEWELL:

Congressman, I think that, ultimately, Congress must decide this issue. So I'm completely in support of the decision that you're articulating. I think we find ourselves in an odd situation in our court in California because the FBI chose to pursue in an ex parte fashion a warrant that would compel Apple to do something. We do that not as extension of the debate, not as a way to resolve this issue, we do that as a way to cut off the debate because the court would have grant the release that the FBI is seeking. We would be forced to do the very thing which we think is that issue and should be decided by the American people. We would be forced to create...

SENSENBRENNER:

Hey, now what's your proposal, legislative response? Do you have a bill for us to consider?

SEWELL:

I do not have a bill for you to consider.

SENSENBRENNER:

OK, thank you. That answers that. Now, the FBI has provided some fairly specific policy proposals to ensure that law enforcement can can access encrypted data with a warrant. What policy proposal would Apple support? You don't like what the FBI said. What's your specific response?

SEWELL:

What we're asking for, Congressman, is a debate on this. I don't have a proposal. I don't have a solution for it. But what I think we need to do is to give this an appropriate and fair hearing at this body which exists to convene and deliberate and decide issues of legislative importance. We think that the problem is we need to get the right stakeholders in the room. This is not a security versus privacy issue. This is a security versus security issue and that balance should be struck, we think, by the Congress.

SENSENBRENNER:

Well, you know, let me make this observation. You're having dealt with the fallout of the Snowden revelations and the drafting and garnering support of the USA Freedom Act. I can tell you, I don't think you're going to like what comes out of congress.

SEWELL:

Congress, we will follow the law that comes out of this process. We certainly understand.

SENSENBRENNER:

OK. OK, well, the thing is I don't understand. You don't like what's being done with the lawfully issued warrant. And most warrants are issued on an ex parte basis where law enforcement submits an affidavit before a magistrate or a judge. And the judge determines whether the allegations of the affidavit are sufficient for the warrant to issue.

Now, you're operating in a vacuum. You told us what you don't like. You said that Congress opted debate and pass legislation. You haven't told us one thing about what you do like. When are we going to hear of what you do like so that Apple has a positive solution to what you were complaining about?

You said it's Congress' job to do it. Now, we won't shirk from that. This hearing, you know, is part of this debate. The FBI has provided some policy suggestions on that. You haven't said what Apple will support. So all you've been doing is saying is no, no, no, no. Now, our job in Congress, honestly, you know, as we did with the Freedom Act and as we are doing with the Electronic Communications Privacy Act update is to balance our belief that there should be privacy for people who are not guilty or suspected of terrorist activity and that there should be judicial process which there has been in this case. And, you know, I guess that what you're position is because you don't

have anything positive, you know, is to simply leave us to our own devices. Well, we would be very to do that but I guarantee you, you aren't going to like the result. I yield back.

SEWELL:

Congressman, I do think we have said what we stand for and what we believe this constant placing.

SENSENBRENNER:

No. You know, the thing is, is may ask Congress to do something and I asked you what Congress should do. You said, we have nothing. Then I said the FBI has provided specific policy proposals to ensure law enforcement is able to get this information. Now, here we're talking about the iPhone of a dead terrorist that was not owned by the terrorist but was owned by San Bernardino County.

Now, you know, the thing is, is that I don't have a government iPhone. I have my own iPhone which I use extensively. But the terrorist had, you know, a government iPhone which belonged to the government. I think the government of San Bernardino County specifically would like to get to the bottom of this and you're resisting it.

I said my piece.

GOODLATTE:

The time of the gentleman has expired. Gentleman from New York, Mr. Nadler, is recognized is five minutes,

NADLER:

Thank you, Mr. Chairman. Let me begin by welcoming my constituent and the great district attorney of New York County, Cyrus Vance and saying that I appreciate his enlightenment of the district attorney's use of this dilemma that we all face. Let me also suggest in answer to Mr. Sensenbrenner's questions that I assume that Apple may have legislative suggestions for us after the courts come out with their determinations and Apple decide they like their determination. So they don't like the determinations, at which point Apple and a lot of other people and institutions, I assume, will decide on specific legislative proposals. And it may very well be that this Congress will wait to see what the courts do. But we will see.

Let me then begin my questions. District Attorney Vance, Director Comey suggested earlier today that the release sought by the FBI is limited to this

one device running this particular operating software in this one case. Now, I gather that you've mentioned you have over 200 phones facing a similar problem that you don't really think that this case will be limited to the one device. So obviously, it's going to set a precedent, maybe not the only precedent, for a large of devices including the ones that you're interested in.

VANCE:

Well, there may well be an overlap between action in federal court where the FBI is in litigation and in state court. I do believe that what we should be seeking collectively is not a phone by phone by phone solution to accessing devices and the content when the problem was we should be creating a framework in which there are standards that are required to -- for a court to authorize access to a device and that it's not based upon litigation as to whether you can get to West Coast phone or East Coast phone.

NADLER:

I assume that, eventually, either the court will set one standard or Congress will.

VANCE:

Right.

NADLER:

I have to consider it.

VANCE:

Yeah.

NADLER:

Professor Landau, several of your colleagues recently published the results of as survey of over 600 -- and this is similar to a question I asked Director Comey Dicomney, several of your colleagues recently published the results of a survey of over 600 encryption products that are available online. More than 400 of these products are open-source and made or owned by foreign entities. If Congress were to pass a law or, for that matter, if the courts were to impose a requirement that forcing U.S. companies to provide law enforcement with access to encrypted systems, would that law stop bad actors from using encryption open from open sources or foreign sources?

LANDAU: Absolutely not, absolutely not. And what Apple's product does is it makes encryption easy by default. And so it means that, as I said, the Secretary to the Chair of the Federal Reserve, the HVAC employee, the chief of staff in your office. Of course, your office should be protected anyway but the regular person using a phone has the phone Secured. What the change -- if Congress were to pass a law prohibiting use of encryption on Apple phones or however you -- you know, you wouldn't say it's just for apple. What it would do is it would weaken us but not change it for the bad guys.

NADLER:

And if someone purchased a phone from a foreign company can have the encryption that we prohibit in an American from creating?

LANDAU:

If someone purchased a foreign phone, somebody could just download the app from abroad. They don't have to buy a foreign phone. They can just download the app from anywhere.

NADLER:

And let's assume the Congress decided to prohibit purchase of foreign encryption systems, is there any practical way we can enforce that?

LANDAU:

No. So -- I mean you would have to start inspecting so much as it comes over the internet that it becomes an intrusive...

NADLER:

So what you're saying is that we are really debating something that's undoable?

LANDAU:

That's right. And we were there 20 years ago which the open-source issue was part of the reason for the U.S. Government to change in export controls which is part of what enabled...

NADLER:

OK. Let me ask two very quick questions before my time runs out. Mr. Sewell, the Eastern district Court yesterday in its ruling has been referred to - - cited no limiting principle to the legal authority behind the FBI's request as a reason to deny the order. Is there a limiting principle in the San Bernardino case?

SEWELL:  
Absolutely none, Congressman.

NADLER:  
None. So it can be expanded indefinitely. And finally, Mr. Sewell, your brief, Apple's brief to the court lays out several constitutional concerns, this computer code speeches to protect them to the First Amendment. What are the First and Fifth Amendment question? Well, let me just ask, what are the First and Fifth Amendment case -- questions does this case raise? We've been talking about statute but let's ask about the First and Fifth Amendment questions.

SEWELL:  
Right. Good question, Congressman. And bear in mind that what we're being asked to do is write a brand new computer code right in new operating system. The law, with respect to the applicability of computer codes to speech, I think is well- established. So this is compelled speech by the government for the purpose of the government...

NADLER:  
Which is a First Amendment problem.

SEWELL:  
Which is absolutely First Amendment problem. And bear in mind that this speech which Apple does not want to make, this is our position. On the Fifth Amendment, the issue is conscription, the issue is forced activity, forced labor.

NADLER:  
Does anybody else on the panel want to comment on that question? None? Thank you. My time is expired, Mr. Chairman.

GOODLATTE:



ISSA:

Thank you, Mr. Chairman and I'll pick up where you left off on forced labor. Do you know of any place in our history in which -- except in time of war, when things are commandeered and people are told do that or when police are in the hot pursuit, do you know a time in which people were forced to apply their inventive genius against their will?

SEWELL:

Congressman, I'm not aware of it. There's still cases during the war that must (ph) be applicable.

ISSA:

Sure. And I certainly understand a different time and different set of circumstances. Now, I want to do two things. So Miss Landau, I'm going to come to you first. Your expertise is encryption. You were probably very young but you remember 20 years ago the argument wasn't that the FBU and then the Late Mike Oxley and others that were championing that if we allowed more than 256 bit encryption, then the FBI couldn't easily decode it and that would be the ruin of their investigations.

LANDAU:

Right. And what you get instead is over the last 20 years, the NSA has increasingly supported the secured technologies for private sector communications infrastructure including the 256 bit algorithm.

ISSA:

OK. I'm going to ask you a quick question and it's old technology because I'm very good with analog world but this happens to P.A. January 29, 2015. Patent is already in the record and its patent on, basically, self-destructing the contents inside if someone tries to forcibly open it.

Now, the funny thing is I was looking for the old patent that's going back decades and decades because the military and others have used this. They've had acids and even more punitive, if you will, responses inside when we wanted to secure it. It's not a new technology but there's a new twist on it. Aren't we, in a sense, the equivalent of saying, "Well, you can make something that destroys the documents but then you have to tell us how to defeat it?"

LANDAU:

That's exactly right.

ISSA:

OK. And I'm looking and saying that there's no history on that but we've had plain safes for a very, very long time. This isn't new. Do you know of any shredder company that's been told that they have to show you how to reassemble what they've shredded?

LANDAU:

I don't study shredding companies but I'd be would be very surprised if they were.

ISSA:

Mr. Vance, have you ever ordered a shredding company to put the paper back together, use their inventive genius?

VANCE:

Of course, I haven't, Congressman.

ISSA:

OK. So, you're asking, in this case, for somebody to create a product for your service and I want to focus on that and I'll get to you, I promise. But, Mr. Sewell, I'm going to look at you as the representative of one of the great technology companies in our country, Apple gets its great technology people, I assume, from Stanford and MIT and other great universities, right?

SEWELL:

We do. Yes, we do.

ISSA:

And you don't get all the graduates, right?

SEWELL:

No, we don't. We wish we do.

ISSA:

So when I was talking to the director and saying, Well, if you take, and it's a hypothetical. My level of knowledge is way less than any of your folks and probably any of the FBIs but if you take this hard drive, solid state hard drive, you pull it apart and even use the word mirroring, obviously you'd some discussion at some point, and you make as many images as you want, then you have a true original that even if the self-destruct occurs, that original, you throw it away, you take another one. So, that part of what this asking you to do, they can do themselves by pulling the chip out and having it imaged, if you will, in all likelihood. We're not saying for sure but he hadn't checked it. So that's a possibility, is that right?

SEWELL:

I believe so. We don't know what the condition of the phone is and we don't know what the condition around this.

ISSA:

Sure. And of course, we're not really talking about one phone. We know that. We're talking about thousands of phones. And as I understand, the technology used in your chip is you have burnable traces in your chips. So randomly or in some way when you're producing each chip, you burn traces which create the encryption algorithm and that's internal. So the chip has its algorithm separate from the software. But that chip, when interfacing with an image, if you keep giving it new images, that's the part that changes.

So, isn't it at least conceivable that as to that phone and perhaps the 175 in New York and others, that the FBI or NSA could, in fact, come up with an elegant brute force attack that would work on your phones and also would work on hundreds of other types of phones around the World and that that technology with, if you will, those brilliant young minds from Stanford, MIT and Kent State, my alma mater, you know, could in fact, produce something that would not be available to the public, they would have control over and they would be able to make it more universal than just trying to go through your source code which, is it correct, they've never asked for. Is that right?

SEWELL:

We've never been asked for a source code.

ISSA:

OK. Mr. Chairman, if anyone else wants to opine on that, I would appreciate they'll be able to.

GOODLATTE:

Sure. Thanks, gentleman. And I recognize the gentlewoman from California, Ms. Lofgren, for five minutes.

LOFGREN:

Well, thank you very much. I think this hearing is very helpful and just to get it on the record, Mr. Sewell, I mean, you're not objecting -- let me step back. If you have something and you are served with a warrant, you give that something up. Is that correct?

SEWELL:

It's absolutely correct, yes ma'am.

LOFGREN:

So the issue here is you don't have it, you've got no way to get it, therefore, you can't give it, right?

SEWELL:

That's correct.

LOFGREN:

No it that were possible to do something that would get just this one thing without opening the door to everybody else's stuff, would you have a problem with that?

SEWELL:

Let me...

LOFGREN:

Oh, let me rephrase that because you're in court.

SEWELL:

Sure.

LOFGREN:

That would be a different issue than breaking encryption, generally, wouldn't it be?

SEWELL:

The best analogy that I can come up with that I've been struggling with is how do we create the right kind of analogy for this situation. If Apple had a box somewhere that we could guarantee, we could assure 100 percent certainty that anything that was put in that box was not susceptible to thievery, to attack, to corruption. If we had such a place in the world, we wouldn't be here today.

LOFGREN:

Right.

SEWELL:

I think what we would have done is gone to our customers and we would have said, "Give us your passwords." We can absolutely...

LOFGREN:

Correct.

SEWELL:

... 100 percent protect them. And then if you lose your phone, if you need our help, we can just give you the passcode.

LOFGREN:

But you didn't do that because you can't guarantee that which is why you encrypted this phone?

SEWELL:

Exactly right. And now the bizarre situation is that, essentially, the FBI is saying, "We all realize it's silly that everybody would give you your password. But instead, we want you to build a tool that will get those passwords and you're -- we're telling you, you can put that tool in this box doesn't exist.

LOFGREN:

So let me ask you this, is it possible, theoretically, to create code that would preclude you from creating a system that would allow you to defeat the ten try erase function?

We could write a program that would suppress that protected method.

LOFGREN:

So you couldn't do what it is you're being asked to do.

SEWELL:

Right. We're being asked to do three things. But we -- it is capable. We are capable of doing those three things. The issue is what's the consequence of doing that.

LOFGREN:

Right. But the question is also -- I mean this hearing cost me to go in and turn on the ten erase function which I neglected to do before the hearing. Thank you very much. But, you know, as you go forward, people are insecure about what's safe.

SEWELL:

Absolutely.

LOFGREN:

And, you know for example, you don't have -- and I think for good reason what's in iCloud is not encrypted. Is it possible to encrypt the data in iCloud?

SEWELL:

Yes. Actually in the iOS 8 and 9 generation, we have encrypted the iCloud data. It's encrypted in a different way than it was before and we think in a more secure way.

LOFGREN:

Right. But you can still provide access to that.

SEWELL:

It is encrypted in a different way and so...

LOFGREN:

But you could change that if you wished?

SEWELL:

Yes.

LOFGREN:

Now, let me ask you this, Dr. Landau. You were involved with that paper that was published, I think, last year.

LANDAU:

Yes.

LOFGREN:

Thank you. That was an excellent paper. And I think for anybody who has danced ahead to read some pages two or three times to understand it but for anybody and I would have to ask unanimous consent, Mr. Chairman, to put that paper in the record from the cryptographers.

GOODLATTE:

Without objection, it will be a made part of the record.

LOFGREN:

If you just go to the questions at the end, you see that this is a fool's errand. We'll never be able to do what is being asked us by the FBI. It's a practical matter, it is just not achievable. But I'm interested in your take on -- you know, Director Comey, you know, they don't want the master key, they just want this one bypass on security. Isn't that exactly the same?

LANDAU:

It's wrong and it's just as pursuance (ph) said, once they've built that software, that software works for other phones. Of course, it has to have the serial number of the particular phone. So Apple has to sign, you know, has to take the software, put in a new serial number and sign it so the new phone accepts it and that's where all the security risks come in because it becomes a routine process and as I mentioned during my remarks, routine processes get subverted.

LOFGREN:

I'll ask the final question. It was asked earlier by my colleague Mr. Richmond, about whether somebody, these other countries have better security than we do. If I take my phone, my iPhone, with the current operating system to Russia or China, can they break into it?

SEWELL:

With respect to the phone itself, we believe that the encryption we provided in iOS 8 makes that effectively impossible. With respect to the things that are going on at the internet level, there are very sophisticated techniques that can be used by malicious actors who have access to the internet itself. There are ways to fool the internet into thinking that something is what it isn't. And so I think there is a vulnerability still in that regard. But on the phone, what we've tried to do is to remove that possibility with iOS 8 and 9.

LOFGREN:

Thank you very much for all of you for your testimony.

GOODLATTE:

The chair thanks the gentlewoman and recognized the gentleman from Texas, Mr. Poe, for five minutes.

POE:

Thank you, Chairman. Thank you all for being here. Fascinating, important discussion on this issue of as you say security and security. As you know, I'm a former prosecutor and a former judge and dealt with warrants for 30 years either requesting them or signing them. And this particular case, I think we're really talking about two cases now. We're not talking just about the San Bernardino case but the New York case as well, different facts, different issues.

Fourth Amendment, we have discussed. Fourth Amendment, that didn't really apply too much to this situation because the possession of the item is lawful in the possession of government. I do think it's ironic, however, we're talking about privacy. United States is supposed to lead on the issue, I think, on the issue of privacy. We're the only one that has a Fourth Amendment. But we see that other countries seem to have more concern about privacy in their technology than maybe we do. I find that somewhat ironic.

Let me ask you a couple of questions. You discussed the idea of constitutional right, right of privacy, but in one of your testimonies, now I think it was Mr. Nadler from New York, he and I have a language barrier problem



so I'm not sure I understood his question. You mentioned the First Amendment and the Fifth Amendment, is that correct?

NADLER:

I did. That's correct.

POE:

Briefly explain how you see this is a First Amendment issue as well as a Fifth Amendment issue. We don't need to talk about the Fourth Amendment. We've discussed that.

SEWELL:

The Fifth Amendment issue derives from the fact that we're being asked to a write code and the code is speech and the Supreme Court has held that speech is protectable. So we're being asked to speak by the government. That speech is not speech that we want to make. And the First Amendment provides us with protections against being compelled to speak by the government. So that would be the First Amendment argument in a nutshell. The Fifth Amendment provides us with protection from conscription, protection from being forced into labor at the governments will except under the most extraordinary of circumstances which I discussed with Congressman Issa. But that's the Fifth Amendment issue.

POE:

Right. Thank you. What -- this request, the results of the request, how would that affect Apple worldwide in other countries?

SEWELL:

Well, there are a number of parts of that question, Congressman, so thank you. The way that this would affect Apple is that it would affect our customers. It would affect everyone who owns an iPhone and it would create a risk for everyone who owns a phone that their data could be compromised if their security could be compromised.

With respect to the international question, I agree with you. I think America should be leading on this issue and I think that the world is watching what happens right now in our government and what happens even today with respect to this particular debate. Our ability to maintain a consistent position around the world, our ability to say that we will not compromise the safety and security of any of our users anywhere in world is substantially weakened

if we are forced to make that compromise here in our own country. So I urge this Congress and I urge the government, generally, to understand and to take a leadership role. Give us the strong support that we need to resist any effort by other governments to weaken security and privacy.

POE:

One of the questions that was asked, it was talking about what is your solution and I actually agree with Mr. Nadler. I know this is going to bother him a little bit, that there may be after all this litigation, then there may be a solution that we haven't thought of yet. But would not one option be Congress take into position that prohibits the back door key security system, the viper system, as I call it, from...

SEWELL:

Thank you, Mr. Poe.

POE:

I said that earlier but you stepped out. The viper system from being imposed, required, prohibit that from government requiring that type of system in specific technology like an iPhone.

SEWELL:

I think that is certainly one possibility, yes.

POE:

So prohibit the key. Let me consider -- ask you something else. If courts rule that you're required to develop the technology, develop the software, would that have -- would that software be able to be used on all those other hundreds of phones that are out there that the government lawfully has in their possession but they can't get into?

SEWELL:

Absolutely. There is nothing that would preclude it from being used on any iPhone that is in use today.

POE:

And my last question, would other countries, then if we -- U.S. takes the position thou shalt give government the key or what will other countries like China require or request or demand of Apple?

SEWELL:

So to date, we have not had demands like that from any other country. The only place that we're having this debate is in our own country. But I -- as I said before, I think if we are ordered to do this, it will be a hot minute before we get those requests from other places.

POE:

Right. Thank you, Mr. Chairman. I yield back.

GOODLATTE:

The chair thanks the gentleman and recognized the gentleman from Georgia, Mr. Johnson, for five minutes.

JOHNSON:

Thank you and I thank the witnesses for being here. Mr. Vance, what's the difference between a company being ordered to use its best efforts? I think the language is, let's see, an order, a court order requiring reasonable technical assistance. What's the difference between a court order requiring reasonable technical assistance to accomplish the bypassing or disabling of the auto-erase function versus a civil subpoena or a court order pursuant to a subpoena, motion to compel the delivery of information under that person's custody and control? Is there a difference?

VANCE:

I'm not sure, Congressman, there is a difference. They're both court orders that are directing an end result. One may be in a civil context, one in a criminal context. But I would say that in this discussion, it's very much a part of our history in America that when companies produce items or objects or commerce becomes ubiquitous in a particular area, that the company has to have a realization that part of the group of people who are using its products are using it to commit criminal purposes. Take a look at banking system, currency transaction reports.

So, we -- once it became obvious that criminals were moving cash through the banks, the response was you have to create and file transaction reports when cash is moved. So when a company -- when two companies like these two hugely successful and important companies own 96.7 percent of the world's smartphone market and we know that criminals are using the devices

to commit crimes, we've heard some of those stories, I don't think that it is new in American history or in the context of business ethics or oversight for companies to have to adapt to the realities of the product they've created.

JOHNSON:

Because they are the only ones that can -- a bank that received the cash would be the only entity in a position to submit a currency transaction report.

VANCE:

It would be the only one required to. If someone else had information about it, they could submit it but it would be the only one who had firsthand knowledge.

JOHNSON:

OK. Now, Mrs. Landau, is it your opinion that the government should not have the ability to compel Apple to use its best efforts to accomplish a technical feat? Is that your opinion?

LANDAU:

So there are two answers to that. If you're asking me as a lawyer question, then I'm not a lawyer and I'll dodge. But if you're asking me as a technologist, then I will say that it is a security mistake. It's a security mistake because that code...

JOHNSON:

Because what Apple would do would inherently cause an insecurity in their system.

LANDAU:

That's right. And it will be the target of organized crime and nation-states because it will be very valuable for somebody who puts a phone down as they go through customs, for somebody who goes to a business meeting and they're not allowed to bring their phone in because it's a meeting under a nondisclosure and the phone is sitting outside for a few hours, all sorts of situations, the phone will become very interesting and if there's code that can actually get into the phone and get the data, that code is going to be the target of nation-states...

JOHNSON:

So once Apple creates the code, then it makes it susceptible to being stolen and misused.

LANDAU:

That's right., that's right. There's not...

JOHNSON:

So, therefore, Apple should not be required to comply with the court order.

LANDAU:

I'm not answering a legal question. I'm answering the security question. The security question, it makes a real mistake.

JOHNSON:

Yeah, OK. And Mr. Sewell, you would agree with that?

SEWELL:

I would agree if we're forced to create this tool that it reduces the safety and security not within our own systems...

JOHNSON:

Well, now, let me ask you a question. What about the security and safety of those whose liberty can be taken and lives can be taken due to an ongoing security situation which the FBI is seeking to get access to information about? Do those -- is there an interest in the public security that we're talking about here?

SEWELL:

Congressman, that's what...

GOODLATTE:

The time of the gentleman has expired but Mr. Sewell may answer the question.

SEWELL:

That's what makes this such a hard issue because we're balancing two very different but very similar issues, private security, the security of people who use iPhones, the location of your children, the ability to prevent your children

from being kidnapped or harmed versus the security that's inherent in being able to solve crimes. So it's about how do we balance these security needs, how do we develop the best security for the United States. If you read the statements by general -- any of the encryption specialists today will say that defeating or debilitating encryption makes our society less safe overall. And so, that's what we're balancing. Is it the right thing to make our society overall less safe in order to solve crime? That's the issue that we're wrestling.

JOHNSON:

Thank you. I yield back.

GOODLATTE:

The chair recognized the gentleman from South Carolina, Mr. Gowdy, for five minutes.

GOWDY:

Thank you, Mr. Chairman. Mr. Sewell, you just mentioned the balancing. Can you give me a fact pattern where Apple would consent to the magistrate judge's order in California?

SEWELL:

Congressman, we will follow the law if we're ordered.

GOWDY:

NO, I'm asking for a fact pattern. You mentioned balancing. I want you to imagine a fact pattern where you balance the interest in favor of what the bureau is asking you to do as opposed to your current position. Give me a fact pattern.

SEWELL:

Congressman, what I said was we have to balance what is the best security for the country. Not balance when we should give law enforcement what they're asking, but balance what's the best security for the country.

GOWDY:

I thought that's what we were balancing is public safety versus privacy. You also mentioned the First and Fifth Amendment. Can you give me a fact pattern where Apple would consent to the order of the magistrate judge?

SEWELL:

Congressman, what I said was privacy, security, personal safety.

GOWDY:

Perhaps I'm being ambiguous in my asking of the question. Can you give me a fact pattern where you would agree to do what the bureau is asking you to do in California, whether it would be nuclear weaponry, whether it be a terrorist plot? Can you imagine a fact pattern where you would do what the bureau is asking?

SEWELL:

Where we would create a tool that doesn't exist.

GOWDY:

Yes.

SEWELL:

... in order to reduce the security and safety...

GOWDY:

Yes.

SEWELL:

... of our users.

GOWDY:

Yes.

SEWELL:

I'm not aware of such a fact.

GOWDY:

So there is no balancing to be done. You have already concluded that you're not going to do it.

SEWELL:

GOWDY:  
There is an order.

SEWELL:  
That order is being challenged at the moment as we speak. There's an order in New York that says...

GOWDY:  
I'm glad you mentioned that. I'm glad you mentioned the order in New York. That's a drug case. So you would agree with me the analysis in drug cases is very different from the analysis of National Security Cases. And even if you didn't agree with that, you would agree that in footnote 41, the magistrate judge in New York invited this conversation about a legislative remedy which brings me back to Chairman Sensenbrenner's question, where is your proposed legislative remedy?

SEWELL:  
So we don't have legislation to propose today, Congressman.

GOWDY:  
Well then how will we know whether or not you think it strikes the right balance if you don't tell us what you think?

SEWELL:  
Congressman, when we get to the point where we -- where it's appropriate for us to propose legislation, not just Apple, but the other stakeholders that engaged in this process, I'm sure there will be legislation.

GOWDY:  
Well, let the record reflect, I'm asking you for it now. I would like you to tell us what legislative remedy you could agree with.

SEWELL:  
I don't have an answer for you today. No one's had an answer to that.



GOWDY: Can you give me why? Can you -- I don't know whether apple has lobbyists. I suspect that you may have a government relations department. Possibly. Can you submit legislation to Chairman Sensenbrenner's question that you could wholeheartedly support and lobby for that resolves this conundrum between you and the bureau?

SEWELL:

It is my firm belief that such legislation can be drafted. I do not have language for you today, Congressman.

GOWDY:

Well, but see, Mr. Sewell, we draft it and then your army of government relations folk opposes it. So I'm just trying to save us time. The judge in New York talked about a lengthy conversation. Sometimes, circumstances are exigent where we don't have time for a lengthy conversation. So, why don't we just save the lobbying and the opposing of whatever, Cedric Richmond or Hakim or Luis and I come up with, why don't you propose it? Tell us what you could agree to.

SEWELL:

Congressman, we're willing to and we've offered to engage in that process.

GOWDY:

Well, the legislative process or with the debate process?

SEWELL:

Both, of course.

GOWDY:

Will you submit legislation to us that you could live with and agree with?

SEWELL:

If after we have the debate to determine what the right balance is, then I think that's a natural outcome.

GOWDY:

Well, how long is the debate going to last?

SEWELL:

I can't anticipate that, Congressman.

GOWDY:

Well, let me ask you this. You mentioned the First Amendment which I found interesting. Are you familiar with voice exemplars?

SEWELL:

I'm sorry, is that a case, Congressman?

GOWDY:

No. Voice exemplars are ordered by courts and judges for witnesses or defendants to actually have to speak so a witness can see whether or not that was the voice that they heard during a robbery, for instance. How about -- because you mentioned you have a First Amendment right to not speak. What about those who have been immunized and still refuse to cooperate with a grand jury and they are held in contempt and imprisoned? So there are lines of cases where you can be forced to speak.

SEWELL:

Congressman, we've made an argument, a constitutional argument, if the courts determine that that argument is infirm, then we will...

GOWDY:

I'm asking you whether or not you agree there are exceptions.

SEWELL:

You've given me two examples that I've not heard of before.

GOWDY:

All right, how about back to the Fifth Amendment because I'm out of time. Real quickly the Fifth Amendment you say you are being conscripted to do something. But there's also a line of cases where folks are conscripted to perform surgical procedures or cavity searches or other things I won't go into in mixed company where they are looking for contraband. So that's a nurse or a doctor or an anesthesiologist that is conscripted by the government. You would agree?

SEWELL:

I'm not familiar with these cases.

GOWDY:

All right, here's what I'll do. I'm out of time. I'll get you the cases I'm relying on if you'll help me with the legislative remedy. Deal?

SEWELL:

I look forward to the cases.

GOWDY:

Deal. Thank you.

GOODLATTE:

The time of the gentleman has expired. The chair recognized the gentleman from Florida, Mr. Deutsch, for five minutes.

DEUTSCH:

Thank you, Mr. Chairman. I would start by saying I don't -- this is really hard. I don't -- I'm not looking to Apple to write the legislation to balance these very difficult issues between privacy and public safety. It's -- I don't expect you to do it. I expect us to grapple with it. And that's what we're trying to do here today. And I had raised this point earlier but I -- it's a perfect lead-in to the questions I want to ask.

This focus on surgical procedures and we can force the government can force a surgical procedure to be done. It sounds like it's somehow equivalent and, well, certainly if we can do that, then we can require that a company create a way in to its phone. Except as I said earlier with Director Comey, that surgical procedure is going to be done by the person that the government says should do it and there is no one from around the world who from their remote location is going to be able to figure out how to conduct surgery on that individual. Yet in this case, and this is why this is so hard for me, in this case, there are people all over America and around the world who will be trying to figure out how to utilize whatever it is that's created here, if this is where this goes, to access the phone. And Director Comey earlier, Mr. Sewell, Director Comey said it's a three-step -- he believes it's a three-step process that they're asking. Can you just speak to that process?

I absolutely can. Thank you, Congressman. First, I agree with you that this is not a problem which -- there are people that are trying to break into these systems. There are people who are trying to steal this information if it existed. And their capabilities are increasing every day. So, this is not a threat which is static. This is a threat which is increasing. The three parts that we're being asked to develop are, first, a method to suppress the data deletion after ten failed attempts. The second thing that we're being asked to suppress is the time delay between successive attempts. Both of these are specifically tailored to deal with the situation where your phone is stolen or some bad person is trying to break into it and it's specifically designed to defeat the brute force attack.

DEUTSCH:

Right.

SEWELL:

The third piece is interesting because the third piece is the government asking for us to rewrite the code that controls the touch screen and allow them to put a probe into the phone and to bypass the need to enter numeric digits through the touch screen. The only reason that that makes sense, Congressman, is if you anticipate that this is going to be technology used on other phones and other phones that likely have more complicated passcode.

DEUTSCH:

Thanks. So, that's the question. And, Mr. Sewell, it's a question for you and, Mr. Vance, it's a question for you. And I -- this is one where if I believe -- if I understand that what's being asked of you is to create this way in to this one phone, then I want you to do it. I do. And I can get pass a lot of these privacy issues if I believe that it's once in and then can then be disposed or destroyed and that will be the end of it. The question is, is that the case? And when you create it for this one, is it something that can be used on other phones? Director Comey I don't think was clear about that, so I'd ask you that question. And, Mr. Vance, I'd ask you the same question.

VANCE:

If I can...

DEUTSCH:

Please.

VANCE:

... refer to actually the doctor's own paper, you need the phone physically at Cupertino to open it. And I refer you to her...

DEUTSCH:

I don't -- but I don't have much time. I'm not sure I understand what that means. I just want to know, cutting to the chase, I just want to understand if this is created, is it something that not just -- that could be used by you in the pursuit of justice, but by the criminal cyberterrorist hackers and really dangerous people who are looking to do bad things everyday of the year going forward?

VANCE:

Congressman, my point is simply that if this code is created and you were looking at the risk to other devices, other Apple phones in the world, those phones are going to have to come to Cupertino to be opened. This is...

DEUTSCH:

Well, let me ask Mr. Sewell before we -- I only have a couple seconds, left.

VANCE:

But that was incorrect...

DEUTSCH:

Well the -- but the question is even if that's correct, I'd like you to speak to it. Is it true that the hackers of the world, that there will be those that try to find a way to get around having to take the phone to Cupertino in order to conduct whatever operation is necessary to break in?

SEWELL:

Yeah. Unquestionably, Congressman, and that's exactly the risk and the danger that we foresee. With respect to the comment that Mr. Vance just made, in fact, the request that we got from the government in this case was that we should take this tool and piece -- put it on a hard drive and send the hard drive to the FBI. The FBI would then load that hard drive into a computer, hook the phone up to the computer, and they would perform the entire operation. So that this whole tool is transportable on a hard drive. So, this is a very real possibility.

DEUTSCH:

So, should we be concerned, Mr. Vance? I mean, look, I want to get into this phone but shouldn't we be concerned if that's accurate that there's something that's being created that's transported on a hard drive that winds up on another computer that there is at least the risk that that gets stolen and then -- and suddenly you -- there is -- not just into a bad person and these terrorists that we desperately want to get and get this information, but suddenly, all the rest of us who are trying to protect ourselves from the bad people and who are trying to protect our kids from these bad people are potentially at risk, too?

VANCE:

Congressman, I respectfully disagree with the colleague from Apple but I will confess that I -- you know, his knowledge of the company is great. Apple has created a technology which is default disk encryption. It didn't exist before. It exists now. Apple is now claiming a right of privacy about a technology that it just created that right of privacy didn't exist before Apple created the technology, number one.

Number two, I can't answer how likely it is that if the Federal Government is given a source code to get through the front door of the phone, that is at risk of going viral. I think it may be overstated to suggest that. But I can tell you this, if there's an incremental risk that providing the source code creates a vulnerability, what is that risk. Don't tell us just millions of phones might be affected. Tell us -- I think we can do better than just giving us broad generalizations without specifics.

But I can tell you this, the consequence -- the other side of the weight, the consequence is in cases all over the country right now in my jurisdiction, your jurisdiction, everywhere, families like the Mills family, are not getting justice. And the direct consequence of this disk encryption is that innocent victims all over the country are not getting their cases solved, prosecutors are not doing the job that they have been elected and sworn to do, and there is a significant consequence to default disk encryption that I think needs to be balanced against a speculative claim of increased insecurity.

LANDAU:

I'd like to just add a couple of comments. This is not about a new right of privacy. It's about a new form of security. And if we think about how the phones are used and increasingly how the phones are used, I certainly have

And if you make the phone itself insecure, which is what is being asked for by law enforcement, you preclude that and that is the best way to prevent the stealing of login credentials, the use of a phone as authenticator.

In terms of the risk of the disk and so on, it's not the risk of the disk going out because the disk is tied to a particular phone. The risk is that somebody will come into Apple and provide a rogue certificate that they, you know, they're from law enforcement or wherever and will get the ability to decrypt a phone that should not be decrypted, whether it's the Chinese Government or an organized crime group or whatever. That's the risk we're facing.

VANCE:

May I -- Congressman, with the Chairman's permission?

DEUTSCH:

My time is up. The chairman has been generous.

GOODLATTE:

Well beyond the time, but briefly.

VANCE:

The professor has not answered what about the people, the residents, the citizens, the victims, whose cases are being put on the side and not addressed while we have an academic discussion, an important one?

DEUTSCH:

Well, it's an important academic discussion because before these phones existed, the evidence that you're talking about didn't exist in the form that you've had access to. Now the technology is moving to a new generation and we're going to have to figure out a different way to help law enforcement but I don't think we say we're not going to ignore these vulnerabilities that exist in order to not change the fact that the law enforcement is going to have to change the way it investigates and gathers evidence.

GOODLATTE:

The time of the gentleman has expired. The chair recognized the gentleman from Illinois, Mr. Gutierrez.

Thank you, Mr. Chairman. First of all, I'd like to ask through the chair if Congresswoman Lofgren has a need for any time, I'd like to yield to her first before mine.

LOFGREN:

Well, thank you very much. You know, I don't know you, Mr. Vance, but I'm sure you're a great prosecutor. I do know Mr. Sewell. He's a great general counsel but the person that really knows technology on the panel is Dr. Landau. And I'm interested in your comments about the vulnerabilities that would be created by complying with the magistrate's order. And some have suggested that it's speculative and, you know, academic and the like. But is that what your take on this is?

LANDAU:

Absolutely not.

LOFGREN:

And the theory -- I mean, we are moving to a world where everything is going to be digital. And you could keep track of, you know, my, you know, when I'm walking around the house I'm in, my temperature, opening the refrigerator, driving my car, and if that all is open to a legitimate warrant, I'm not downplaying the problem the prosecutors have but this is evidence you currently don't have access to. How vulnerable is -- are -- is our country going to be? That's the question for you.

LANDAU:

Extremely vulnerable. David Sanger's article in today's New York Times is about the Ukraine Power Grid says that they got in as I mentioned earlier through the login credentials. It's based on a DHS memorandum that talks about locking down various systems. I served for a number of years on NIST's Information Security and Advisory -- Security and Privacy Advisory Board and we used to talk to people from the Power Grid, and they would say, "Oh, it's okay, we're not -- our systems aren't connected to the internet." Well, they were fully connected.

We are -- whether you're talking about the Power Grid, the water supply, whatever, we're connected in all sorts of disastrously unsafe ways. And as I mentioned earlier, the best way to get at those systems is through login credentials.



Phones are going to provide the best way to secure ourselves. And so, this is not just about the personal safety of the data you have on your phone and it's not just about the location of where your family is, and it's not just about the business credentials, but it's really about the, as you say, Congressman Lofgren, it's really about the way that we are going to secure ourselves in the future. And what law enforcement is asking for is going to preclude those strong security solutions.

It also is a very much a 20th century way of looking at a 21st century problem. And I didn't get a chance to answer Congressman Gowdy, but the FBI, although it has excellent people, it hasn't put in the investment. So Director Comey said, we talked to everyone who will talk to us, but I was at a meeting -- I briefed at FCC a couple of years ago and some senior people from DOJ were there and I said, "Well, you know, NSA has scale X and Y." And DOJ said, they won't share it with the FBI except in exceptional circumstances." They keep it for themselves.

We're in this situation where I think law enforcement needs to really develop that skill -- those skills up by themselves and then that you ask about what it is this committee can do. It's thinking about the right way for law enforcement to develop those capabilities, the right level of funding. The funding is well below what it should be but they also don't have the skills.

GUTIERREZ:

Thank you. So, I'm happy I yielded the time to you. I always know it's one of the smartest things I do is work with Congresswoman Lofgren on this committee. But I just want to share with you, look, I understand the competing interests here. But I think, Mr. Sewell, you should understand that I love your products. You know, I used to think, you know, house, then a car, now I think technology between what they charge me for the internet, all the stuff I buy, just to get information everyday, it's -- but don't worry, I can afford it. I'm not going into the poorhouse because of it. So I'm excited about all of the new things that I get to and how it improves my life.

And so I'm thankful to men and women in technology for doing that. But a lot of times in this place, there's adversarial positions taken and I would hope simply that we would look for a way in which we put the safety interests of the American people. I understand that you think that if we find a back door that that causes all kinds of insecurities. But in this committee, I'm going to work with Congresswoman Lofgren but I'm also going to work with Trey Gowdy.

We're going to work a lot of time bipartisanship and this place has many times promote it but very, very rarely rewarded in this place because everybody is, "Oh, you should take one position or another." I'm going to take a position for the American people. While you might dispute, I kind of look at Apple as an American company. I look at Toyota as a Japanese company, BMW as a German. I look at you as an American company. And so, that's the way I see you, you can dispute that. You may look at yourself as an international entity, but I always look at you as U.S. pride.

When I take this phone as a member of the intelligence committee and I take this phone to China, the intelligence community of the United States, the first thing before I get off that plane, they take it away from me.

So there are bad actors out there already intervening with your products or I don't think the fine people of the intelligence community would take away one of the things that I need the most in my life. So having said that, I hope we might find a way so that we could balance the security needs and the safety needs of the people of the United States and their right to privacy. I think it's essential and important. I want to thank you guys for coming and talking to us and let's try to figure it out all together. Thanks.

SEWELL:

Thank you, Congressman. And I absolutely I agree with what you said, and I think that -- I am proud to work for Apple and I think Apple embodies so many of the most valuable characteristics that make up America, make America a great place. We stand for innovation. We stand for entrepreneurship, we stand for empathy. We stand for all boats rising.

So, I'm very proud. And we are an American company and we're very, very proud of that. The point about security outside of the United States is exactly the point that drives us. We are on a path to try to create the very best, most secure and most private phones that we can. That's a path that will probably never end because the people that we're competing with, the bad guys not just in the United States but all over the world, are on an equally aggressive path to defeat everything that we put into the phone. So we will continue from generation to generation to improve the technology, to provide our users with a safer experience.

GUTIERREZ:

Thank you, Mr. Chairman.

GOODLATTE:

RICHMOND:

And I'm happy to follow Luis, because I guess we're going to start -- I'll start where he left off and I think about a 9- year-old girl who asked, you know, why can't they open the phone so we could see who killed my mother because I was there and heard it happen? So, let me start with this. If the FBI developed the ability to brute force open a phone, would you have a position on that?

SEWELL:

Without involving Apple, without having Apple...

RICHMOND:

Yes.

SEWELL:

... complicit (ph) in that. I don't think we have a position to object or not object to that. I think if the FBI has a method to brute force a phone, we have no ability to stop them.

RICHMOND:

But are you okay with it?

SEWELL:

Well, I think that privacy and security are vitally important national interests. I think that if you weaken the encryption on the phone, then you compromise those vital importance.

RICHMOND:

I'm not asking you about the encryption. If they could brute force open a phone, do you have a problem with that? Is this -- it's -- I think that's just an easy question.

SEWELL:

Then, I'm sorry, perhaps I'm misunderstanding. If the FBI had the ability to brute force a phone, I would suggest that that's the security vulnerability in the phone. So, I would have a problem with it, yes.

RICHMOND:

Let me ask you another question, because I see you're a lawyer, I'm a lawyer. And I would feel awful if I didn't ask this...

LANDAU:

Can I just say something for a second?

RICHMOND:

In a second. Let me get through this question. Brittany Mills had a 5S phone operating on an 8 -- with 8.2 IOS. Does Apple, any employee, subcontractor, subsidiary or anyone that you know of possess the knowledge or the ability to open that phone or unlock that phone?

SEWELL:

We don't and I am glad that you asked about the Mills case because I think it's instructive about the way that we do work together cooperatively. I know that we met with members of your staff...

RICHMOND:

Look, and I'm not suggesting that you all don't. But I just want to know, does anybody have the ability to unlock the phone, first? And if you tell me no, then I get a no in public on the record and I feel a lot better about what I'm doing.

SEWELL:

Let me be clear. We have not said that we cannot create the tool that the FBI has asked us to create.

RICHMOND:

Right. No, I'm not asking about creating anything. I'm saying, does it exist now? Do you know anybody or does anyone have the ability to do it right now?

SEWELL:

Short (ph) of creating something new, no.

RICHMOND:

Now, in a -- oh, I'm sorry, Miss. I promised to let you answer.

LANDAU:

I just wanted to add that in security, we have an arms race. People build good products, somebody finds a vulnerability. It could be the FBI. It could be not the FBI. I may not tell anybody about the vulnerability, but we have this arms race where as soon as somebody finds a problem, the next roll of technology comes out and that's the way we do things.

RICHMOND:

So what would be your feeling if the FBI developed the technology that they can plug something into the iPhone?

LANDAU:

I think that the FBI should be developing the skills and capabilities to do those kinds of investigations. I think it's absolutely crucial and I think that they have some expertise but it's not at the level that they ought to have. And I think we're having this conversation exactly because they are really using techniques from -- they're using a mindset from long ago, from 20 years ago rather than the present.

RICHMOND:

So they're antiquated?

GOODLATTE:

Will the gentleman yield?

RICHMOND:

Sure.

GOODLATTE:

Because I just want to clarify both Mr. Sewell and Ms. Landau did not say subject to the unauthorized court order warrant.

LANDAU:

Well, I certainly did not subject to that.

GOODLATTE:

They're not suggesting they develop this technology and then do what they think is they best. They have to do it subject to a warrant.

LANDAU:

Of course, thank you.

RICHMOND:

And I am glad you cleared that up because I want to make sure that everybody understands what I'm saying.

I don't think any of this should happen without a court order. Now, you know, maybe I watch too many movies and maybe I listen to Trey Gowdy too much, some people would suggest if I listen to him at all, that's too much. But in the instance that there's a terrorist that has put the location of a nuclear bomb on the phone and he dies, how long would it take Apple to develop the technology to tell us where that nuclear bomb was? Or would Apple not be able to develop that technology to tell us in a short period of time?

SEWELL:

The first thing we would do is to try to look at all of the data that surrounds that phone. There is an enormous change in the landscape over the last 25 years with respect to what law enforcement has access to. So when we have an emergency situation like that, whether it be a lost child or the airplane, when the Malaysia Airline went down, within one hour of that plane being declared missing, we had Apple operators cooperating with telephone providers all over the world with the airlines and with local, well, the FBI to try to find a ping, to try to find some way that we could locate where that plane was. So the very first thing that we would do in this situation is to bring to bear all of the emergency procedures that we have available at Apple to try to find it.

RICHMOND:

Thank you. Mr. Chairman, can I just clarify, because I don't want anyone to leave out of here thinking that Apple has not been cooperative with our district attorney in the effort to access the data. And, in fact, they came up with new suggestions. But my questions are just about the government's ability to just brute open a phone at any point with a court order. So, I don't want to suggest that Apple has not been working diligently with my DA who has also been working diligently, thank you, Mr. Chairman. I yield back.

SEWELL: I appreciate that, Mr. Congressman.

GOODLATTE:

The chair thanks the gentleman. And I recognize the gentlewoman from Washington State, Ms. DelBene, for five minutes.

DELBENE:

Thank you, Mr. Chairman. Thanks to all you for being here and for enduring this for a while. It's very, very important. In the earlier part of the hearing, Director Comey said that it is not a company's job to worry about public safety and I think that that is -- would be very concerning for a company to send that message given that we have technologies that impact people's everyday lives in so many ways and I assume you agree with that, Mr. Sewell.

SEWELL:

I absolutely do. I do not subscribe to the position articulated by Director Comey.

DELBENE:

I worked at Silicon Valley Companies, Sun Microsystems and Google and that's certainly not what I saw in either of them.

In the Brooklyn case decided yesterday, Judge Orenstein stated in his opinion that the world of the internet, of things the connected devices on sensors that we see coming forward, the government's arguments would lead quickly to a world of virtually limitless surveillance and intrusions on personal privacy. So I'd like to explore the issue of encryption and securing the internet of things a little bit.

We often talk about security by design when it comes to the internet of things and I'm sure we can all imagine the horror stories of insecure internet of things types of devices like appliances being hacked to cause a fire or spying through baby monitors, hacking into a car or tampering with a home security system.

So, I'm wondering, Dr. Landau, I'm wondering if you could comment on what it means in the encryption context and whether directives we've heard from the FTC, for example, to adopt security by design in the interest of protecting consumers from malicious actors is inherently incompatible with what you might call insecurity by design should that be mandated by the courts?

LANDAU:

Well, here you're in a situation where the companies often want to collect the data. So, for example, if you're using smart meters, the company wants the data. The electric company wants the data to tell your dishwasher, "No, don't turn on at 4:00 in the afternoon when air-conditioning requirements are high in Silicon Valley right now, turn it on at 8:00 at night or 2:00 a.m.

And so, in fact, it actually wants the individualized data and if it has the individualized data then it can certainly share it with law enforcement under court order.

The security by design is often in the internet of things, securing the data on the device and securing the transmission of the data elsewhere. The issue in the Apple phone is the data stays on the device and that's the conflict that we're having. For the internet of things, it's most useful if the data goes off the device to somewhere elsewhere, where it can be used in a certain way.

DELBENE:

And, Mr. Sewell, could companies open themselves up to liability if vulnerabilities for law enforcement end up being exploited by a bad actor?

SEWELL:

I think that's absolutely true. Somewhat ironically I suppose we have the FTC at this point actively policing the way in which technology companies deal with these issues and we can be liable under the section 5 or under the authority of the FTC if we fail to close a known vulnerability.

DELBENE:

And, Ms. Landau, you talked about the question of security versus -- or the issue of security versus security. And that this really is a debate about security versus security. Could you explain a little bit more why...

LANDAU:

Sure.

DELBENE:

... our national security and cybersecurity incompatible in your opinion?

LANDAU:



So, what we really have here over the last 20 years as I mentioned earlier is you see the NSA and Snowden revelations aside, we don't have time for me to describe all of the subtle points there, but you really see the NSA working to secure private sector telecommunications infrastructure, many, many examples.

We have moved to a world of electronic devices, you talk about the internet of things, that leak all sorts of data. And in order to protect ourselves, whether ourselves, our health data or our bank data, the locations of our children and so on, we need -- we need encryption and so on. But if you think more broadly about the risks that our nation faces and the risks of people coming in and attacking the power grid, people coming in and stealing data from whatever company and stealing patented information and so on, you see a massive national security risk. And you've been hearing it from General Keith Alexander, we've been hearing it from Hayden, we've been hearing it from Mike McConnell, we've been hearing it from Chertoff, all the people who have been involved on the DHS and NSA side.

The only thing that can secure that is security everywhere and the move that Apple makes to secure the phones is one of the many steps we need in that direction.

DELBENE:

Thank you. My time's expired. I yield back, Mr. Chair.

GOODLATTE:

Thank you. I'm going to recognize myself for some questioning, so welcome in.

I'm sorry, Mr. Sewell, pronouncing that name correctly?

SEWELL:

You are.

GOODLATTE:

All right. I have some questions for you concerning China.

In 2014, you moved your -- what's referred to as your Chinese Cloud to China, is that correct?

SEWELL:

That is correct.

GOODLATTE:

Okay. And can you -- can you tell me who's data is stored in that Chinese Cloud? Is it just people in China? Is my data stored in that Cloud as well?

SEWELL:

Your data is not stored in that Cloud.

GOODLATTE:

Is it strictly limited to Chinese people?

SEWELL:

There are a number of things that in the cloud, so I should probably be clear about what's there.

GOODLATTE:

Okay.

SEWELL:

With respect to personal data, no personal data is there unless the individual's data -- the individual himself has registered as having a Chinese address and having a Chinese access point. In addition, we have other data which has to do with film content, movies, books, iTunes, music. The reason we do that is because of something called latency. If you're streaming across the internet and you have to bring the data from the United States to China, there's a live time, there's a latency piece, whereas if we move that data closer to China either Hong Kong or Mainland China, then we can provide a much better service to our customers.

MARINO:

OK. Can you tell me, what was the cost in the ballpark figure in the time to make the move to -- from the United States to move Chinese information over to China and their Cloud?

SEWELL:

I'm sorry, did you say in time?

MARINO:  
Cost in time.

SEWELL:

So, the time -- the cost is building the facilities. I don't have a number for that. It's certainly not something that I'm aware of, although, of course, the company has that information. In terms of the time, once the server exists, once there is a receptacle for the data in theory it's instantaneous.

MARINO:

OK. You may or may not know but I was a prosecutor for a while both at the state and federal level and we prosecutors are focused on the case and the crime concerned and we want to get our hands on anything we can to see that justice is served. But on the other side of this, too, we're talking about privacy issues. And I'm very concerned about to what extent if for some reason you were to change your mind about working with the FBI or the court ordered that, what does that mean to our privacy?

SEWELL:

I think it means that we have put our privacy at risk. The tool that we're being asked to prepare is something which could be used to defeat both the safety and the privacy aspects of the...

MARINO:

Let me get this clear, because there are many rumors flying around, and you probably into his couple times, and I apologize, I had to run and do something else. Are you saying that there is no method that exists now that you could unlock that phone and let the FBI know what is in there?

SEWELL:

Short of creating the tool that they have asked us...

MARINO:

Right.

SEWELL:

We are not aware of such a method, you know.

Now, you talk about the cost is an unreasonable burden and the time involved, that's why I asked you what did it cost to move the Cloud, what was the time, and you're the expert. I'm not.

SEWELL:

Congressman (ph), to be fair, we haven't claimed that the time that it would take to create the tool is the undue burden. Our claim is that the undue burden is to compromise the safety and security of all of our customers.

MARINO:

So, it's your position that if you do what the FBI wants to one phone, could you elaborate on that in the 33 seconds I have left as to why that would be an undue burden, keeping in mind that, I'm very critical about our privacy.

SEWELL:

Congressman, the answer is very simple. We don't believe this is a one-phone issue. We don't believe it can be contained to one phone or that it would be contained to one phone.

MARINO:

OK. I see that my time is just about run out, so I'm going to yield back and who's next? Mr. Jeffries, Congressman Jeffries, is next.

JEFFRIES:

Thank my good friend from Pennsylvania for yielding.

I want to thank all the witnesses for your presence here today. It's been very informative discussion. In particular I want to thank D.A. Vance for your presence and certainly for the many progressive and innovative programs that you have in Manhattan, proving that you can be both tough and fair as a prosecutor and that has not gone unnoticed.

Let me start with Mr. Sewell, there's an extensive record of cooperation that Apple has with law enforcement in this San Bernardino case, isn't that fair to say?

SEWELL:

That's correct. For over 75 days we've been working with the FBI to try to get more information and try to help solve this crime.

JEFFRIES:

I think it's useful to put some of this on the record. On December 5th, the Apple emergency 24/7 call center received a call concerning the San Bernardino shooting, is that right?

SEWELL:

That's right. In fact, the call came in to us at 2:47 a.m. on a Saturday morning. We have a hotline that exists. We have people that are manning that hotline.

JEFFRIES:

And you responded with two document productions, is that correct?

SEWELL:

By 2:48 that morning, we were working on the case and we responded by giving the FBI all of the information that we could immediately pull from our sources and then we continued to respond to subpoenas and to work directly with the FBI on a daily basis.

JEFFRIES:

Right. In fact, the next day I think Apple received a search warrant for information relating to at least three e-mail accounts, is that right?

SEWELL:

That's correct.

JEFFRIES:

And you complied with that request?

SEWELL:

We did comply with that and subsequent requests.

JEFFRIES:

And so I think also on January 22nd, you received another search warrant for iCloud information related to the iPhone that was in position of the male terrorist, is that right?

That's right and it's important that in the intervening stage, we had actually sent engineers to work directly with FBI technicians in Washington, D.C. and Cupertino. And we provided a set of alternatives or options that we thought should be tried by the FBI to see if there might be some possibility that we could get into this phone without having to do the tool that we're now being asked to create.

JEFFRIES:

So the issue here is not really about cooperation as I understand it. Apple has clearly cooperated in an extensive fashion as it relates to all of the information that you possess. The question I think that we all on the judiciary committee and beyond have to consider is the notion of you being asked as a private company to create anti-encryption technology that currently does not exist and could jeopardize the privacy and security of presumably hundreds of millions of iPhone users throughout the country and the world, is that right?

SEWELL:

We're being asked to create a method to hack our own phones.

JEFFRIES:

Now, Mr. Vance, are you familiar with the Arizona v. Hicks Supreme Court case from the late '80s.

VANCE:

If you give me the facts, I'm sure I will have read it.

JEFFRIES:

OK. Well, the Supreme Court held that the police conducted an unconstitutional search of evidence that was not in plain view. It was a decision that was written by Justice Antonin Scalia and the most important point that I want you to reflect upon is he stated, "In authoring the majority opinion, that there is nothing new about the realization that the constitution sometimes insulates the criminality of the few in order to protect the privacy of us all."

Do you agree that embedded in the fabric of our constitution, the Fourth Amendment and beyond, is the notion that we value the privacy rights of Americans so deeply that at times it is something that will trump law

VANCE:

Congressman, I do sincerely believe that. What concerns me about the picture we are seeing from the state perspective is that Apple has decided that it's going to strike that balance now with no access by law enforcement for full disk encrypted devices even with a warrant. So, they have created their own balance. They now have decided what the rules are. And that changes radically, the balance that existed previously. And it was done unilaterally so this could be...

JEFFRIES:

Well, I think -- if I can just interject. I mean I think that that's a balance that ultimately the Congress is going to have to work out and also the article three court systems certainly beyond an individual magistrate who is not even appointed for lifetime tenure is going to have to work itself through the court system. A district court judge and maybe the ninth circuit, ultimately the Supreme Court.

And so, the company exercising its right in an adversarial system to have all facts being aired on both sides of the debate is very consistent in my view with American democracy and jurisprudence. Just one last question that I wanted to ask as my time is expiring. Because you raised an interesting point earlier in your testimony about an individual who is a suspected criminal who claimed that the encryption technology was a gift from God. But I also noted, I think, in your testimony that this individual communicated that, in an intercepted phone conversation that presumably your office or others were wiretapping. Is that right?

VANCE:

No. It's not right. All phone calls from prison, out of Rikers, are recorded.

JEFFRIES:

Right.

VANCE:

And there's a sign when you pick up the phone, if you are in Rikers Island that this is happening. So, there's a tape. And ultimately that tape was subpoenaed, and it's from that tape that that conversation was transcribed.

JEFFRIES: And if I could just -- in conclusion, I appreciate the chair's indulgence. I mean I think that illustrates the point. Presumably that it's fair to say that in most instances bad actors will make a mistake. And at the same time that he's heralding the availability of encryption technology to shield his activity from law enforcement, surveillance and engagement, he's ignoring a plain view sign that these conversations are being recorded and subjecting himself to unfettered government surveillance.

And I think that I have faith in your ability and the FBI's ability ultimately to outsmart the criminals and the bad actors without jeopardizing the privacy and security of the American people.

VANCE:

And in that case, our challenge is because of our inability to access the phone, our inability to investigate further any evidence of sex trafficking, is not made available to us. So yes, he did something that was not smart. But the greater harm is the inability, in my opinion, of being able to get to the true facts which in fact are extremely important as matter of public safety to get access to.

JEFFRIES:

My time is expired. I thank you.

GOODLATTE:

I thank the gentleman from New York and the chair recognized now the gentleman from Rhode Island, Congressman Cicilline.

CICILLINE:

Thank you Mr. Chairman. Thank you to our witnesses for your testimony. These are very important discussion.

I think we all recognize there are few be absolute in the law and so balancing, you know, occurs all the time. There are risks in developing the software that have been articulated very well during this hearing and indeed there are risks associated with inability to access critical information. So that, I think we are living in a world with our risks in both ways forward.

And I guess my first question is, many people who agree that Apple or any other company should not be required, and there's no authorization to require them, to produce a product that doesn't exist or to develop an intellectual property that doesn't exist. Many people who think that that's



correct wonder whether Apple has considered in limited circumstances and maybe a standard you would set internally, if it in fact is a situation that would prevent immediate death or serious bodily injury coupled with a consent of the person or lack of objection.

In this case, this person is deceased, where there is no privacy claim asserted, in some very narrow category, whether there's a set of protocols you might voluntarily adopt to provide that information or that software within instructions that it be immediately destroyed if they done in a skip in a security. I mean is that practical, something like that? Should that be part of this discussion that we keep hoping that the industry and the justice department will have and trying to develop something or is that fraught with so many problems that's...

SEWELL:

Thank you for the question Congressman.

We have, and spend a lot of time thinking about, how we can assist our customers in the event that they have a problem, if they've lost a phone, if they are in a situation where they are trying to recover data. We have a number of mechanisms to do that and we will continue to improve those mechanisms as we move forward. It's very important to us that we try to think about the consequences of the devices that we create.

In this particular case, the pass code unlock is not something that we think lends itself to a small usage. The problem with this particular issue is that once you take that step, once you create the mechanism to unlock the phone, then you have created a back door and we cannot think of a way to create a back door that can only be used beneficially and not be used by that thing.

CICILLINE:

So you have in fact already contemplated other ways in which you could make this information available in this case that would not have those sorts of broader implications.

SEWELL:

And we have provided information in this case. We have provided logs. We have provided iCloud backup. We've provided all the things that at our disposal.

CICILLINE:

Thank you. (inaudible), you say in your written testimony, the point is that solutions to accessing the data already exist with the forensic analysis community. We did ask Director Comey and we probably limit our question too narrowly because we ask about the intelligence communities of the United States. It sounds like you're suggesting that there may be capabilities outside the United States government that the justice department or the FBI could contract with that are capable of doing what it is they are asking a court to order Apple to do.

LANDAU:

That's right. So I noticed when Director Comey answered the question, he said, we talk to everyone who will talk with us and as I mentioned earlier, I don't know if you were here at that point, I had a conversation with some senior DOJ people a few years ago about using NSA tools in law enforcement cases and they said, NSA is very low to share because of course when you share a tool, it can get into a court case and then the tool is exposed.

And so I don't know in the -- we talked with everyone who will talk with us, how much NSA revealed about what they know and what they can do. So that's the first place I would ask. Now, I phrased let me correct it. That's the first place that I suspect have some tools for exactly this problem.

But yes, there were discussions last week in Silicon Valley. There's been discussions I've had with colleagues, where people believe as Congressman Issa put various potential solutions that there are ways to break in to the phone. There is of course a risk that data might be destroyed. But I have described both in my written and verbal testimony, the FBI has not tried to develop this level of expertise, and it should.

CICILLINE:

It seems that you know, we are contemplating whether or not Congress should take some action to either grant this authority and then figure out what is the appropriate standard and test et cetera. It sounds as if you think that is problematic and that in fact the real answer is a substantial increase investment in the intelligence capability, the law enforcement capability that sort of keeps pace with the advances that come is like Apple are making. But that's really the best protection in terms of both law enforcement and the long-term security in the United States.

LANDAU:

That's right. I don't think actually there needs to be more authority but there needs to be a completely different view of how it's done. There's probably needs to be some authority in terms of how do you handle it for state and local because state and local will not have the resources. And so there have to be some sort of sharing of tools and not as jurisdictional issue and also, you know, an issue between bureaucracies that we'll have to work out and that we'll be have to work out for law and policy.

But in terms of creating new authority, the FBI already has that authority. But if users that at a much lower level and it should expanded in a much lower level, they need to move from the situation they're in to dealing with the 21st century technologies in the appropriate way.

CICILLINE:

Thank you, Mr. Chairman. I yield back.

GOODLATTE:

You bet. Chair recognizes Lofgren California.

LOFGREN:

Could I ask just one quick question, Mr. Sewell. I forgot when it was my turn. And we had asked Mr. Comey, somebody asked Mr. Comey about the changing of the password of apparently the county did at the request of the FBI. What did that do? Can you explain what happened?

SEWELL:

Certainly, one of the methods that we might enable the phone in San Bernardino, to do what's called the auto back up, that issue that the FBI is struggling with, is to find data between a certain time frame, the time of the last backup and the time of the horrific incident in San Bernardino. If the phone would back up, that evidence, that information would become available to the FBI.

The way that we can back these phones up in an automatic way is we connect them to a known Wi-Fi source. A source that the phone has already connected to before and recognizes. If you plug the phone in and you connect it to a known Wi-Fi source, it will, in certain circumstances, auto backup.

And so the very information that the FBI is seeking would have been available and we could have pulled it down from the Cloud. By changing the password, this is different from the pass code, but by changing the pass

word, it was no longer possible for that phone to auto backup.

LOFGREN:

Thank you. And thank you Mr. Chairman, for letting me get that information out.

MARINO:

Mr. Sewell, I have one more question for you. Does the Chinese government have access to the Cloud or is there any indication that they've tried to hack the Cloud in China to get information on the Chinese people?

SEWELL:

Let me be clear about the question. The Chinese undoubtedly have the ability to access their own Cloud.

MARINO:

Yes.

SEWELL:

But with respect to the U.S. Cloud, we believe that -- again, I'm struggling because of the words. The Cloud is a synonym for the Internet. So of course Chinese people have access to the Internet. Are we aware of a Chinese hack through Apple? No.

MARINO:

OK.

SEWELL:

But beyond that, I can't say.

MARINO:

You answered my question. Thank you.

GOODLATTE:

This concludes today's hearing. I want to thank the panel very much for being here. Without objection, all members, we have five legislative days to submit additional questions for the witnesses or additional materials for the record.

The hearing is adjourned.

CQ Transcriptions, March 1, 2016

### **List of Panel Members and Witnesses**

PANEL MEMBERS:

REP. ROBERT W. GOODLATTE, R-VA. CHAIRMAN

REP. LAMAR SMITH, R-TEXAS

REP. JIM SENSENBRENNER, R-WIS.

REP. DARRELL ISSA, R-CALIF.

REP. J. RANDY FORBES, R-VA.

REP. STEVE KING, R-IOWA

REP. TRENT FRANKS, R-ARIZ.

REP. LOUIE GOHMERT, R-TEXAS

REP. JIM JORDAN, R-OHIO

REP. TED POE, R-TEXAS

REP. JASON CHAFFETZ, R-UTAH

REP. STEVE CHABOT, R-OHIO

REP. TOM MARINO, R-PA.

REP. TREY GOWDY, R-S.C.

REP. RAUL R. LABRADOR, R-IDAHO

REP. BLAKE FARENTHOLD, R-TEXAS

REP. DOUG COLLINS, R-GA.

REP. RON DESANTIS, R-FLA.

REP. MIKE BISHOP, R-MICH.

REP. KEN BUCK, R-COLO.

REP. JOHN RATCLIFFE, R-TEXAS

REP. DAVE TROTT, R-MICH.

REP. MIKE WALTERS, R-CALIF.

REP. JOHN CONYERS JR., D-MICH. RANKING MEMBER

REP. JERROLD NADLER, D-N.Y.

REP. ZOE LOFGREN, D-CALIF.

REP. SHEILA JACKSON LEE, D-TEXAS

REP. STEVE COHEN, D-TENN.

REP. HANK JOHNSON, D-GA.

RES. CMMSR. PEDRO R. PIERLUISI, D-P.R.

REP. JUDY CHU, D-CALIF.

REP. TED DEUTCH, D-FLA.

REP. LUIS V. GUTIERREZ, D-ILL.

REP. KAREN BASS, D-CALIF.

REP. CEDRIC L. RICHMOND, D-LA.

REP. SUZAN DELBENE, D-WASH.

REP. HAKEEM JEFFRIES, D-N.Y.

REP. DAVID CICILLINE, D-R.I.

REP. SCOTT PETERS, D-CALIF.

WITNESSES:

BRUCE SEWELL, SENIOR VICE PRESIDENT AND GENERAL COUNSEL,  
APPLE, INC.

SUSAN LANDAU, PROFESSOR, WORCESTER POLYTECHNIC INSTITUTE

CYRUS R. VANCE JR., DISTRICT ATTORNEY, NEW YORK COUNTY

---

Source: **CQ Transcriptions**

© 2016 CQ Roll Call All Rights Reserved.