1	THEODORE J. BOUTROUS JR., SBN 13	32099			
2	tboutrous@gibsondunn.com NICOLA T. HANNA, SBN 130694				
3	nhanna@gibsondunn.com ERIC D. VANDEVELDE, SBN -0699				
_	evandevelde@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP				
4	333 South Grand Avenue				
5	Los Angeles, CA 90071-3197 Telephone: 213.229.7000				
6	Facsimile: 213.229.7520				
7	THEODORE B. OLSON, SBN 38137 tolson@gibsondunn.com				
8	tolson@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP 1050 Connecticut Avenue, N.W.				
9	1050 Connecticut Avenue, N.W. Washington, DC, 20036-5306 Telephone: 202.955.8500				
10	Facsimile: 202.467.0539				
11	MARC J. ZWILLINGER*				
12	marc@zwillgen.com JEFFFREY G. LANDIS*				
13	jeff@zwillgen.com ZWILLGEN PLLC				
14	1900 M Street N.W., Suite 250 Washington, D.C. 20036				
15	Telephone: 202.706.5202 Facsimile: 202.706.5298				
16	*Pro Hac Vice Admission Pending				
	Attorneys for Apple Inc.				
17	UNITED STATES	S DISTRICT COURT			
18	CENTRAL DISTRI	ICT OF CALIFORNIA			
19	EASTER	N DIVISION			
20	IN THE MATTER OF THE SEARCH	ED No. CM 16-10 (SP)			
21	OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A	APPLE INC'S MOTION TO VACATE			
22	SEARCH WARRANT ON A BLACK	ORDER COMPELLING APPLE INC.			
23	LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	TO ASSIST AGENTS IN SEARCH, AND OPPOSITION TO			
24		GOVERNMENT'S MOTION TO COMPEL ASSISTANCE			
25		Hearing:			
26		Date: March 22, 2016 Time: 1:00 p.m.			
27		Place: Courtroom 3 or 4 Judge: Hon. Sheri Pym			
28					
∪∟	1				

Apple Inc. ("Apple"), by and through its counsel of record, hereby files this 1 Motion to Vacate the Order Compelling Apple Inc. to Assist Agents in Search, and 2 Opposition to the Government's Motion to Compel Assistance. 3 This Motion and Opposition is based upon the attached memorandum of points 4 and authorities, the attached declarations of Nicola T. Hanna, Lisa Olle, and Erik 5 Neuenschwander and exhibits, the files and records in this case, and such further 6 evidence and argument as the Court may permit. 7 8 Dated: February 25, 2016 Respectfully submitted, 9 10 GIBSON, DUNN & CRUTCHER LLP 11 /s/ Theodore J. Boutrous, Jr. By: Theodore J. Boutrous, Jr. 12 13 Theodore J. Boutrous, Jr. Nicola T. Hanna 14 Eric D. Vandevelde Gibson, Dunn & Crutcher LLP 15 333 South Grand Avenue Los Angeles, CA 90071-3197 Telephone: 213.229.7000 16 17 Facsimile: 213.229.7520 18 Theodore B. Olson Gibson, Dunn & Crutcher LLP 19 1050 Connecticut Avenue, N.W. 20 Washington, DC, 20036-5306 Telephone: 202.955.8500 21 Facsimile: 202.467.0539 22 Marc J. Zwillinger * Jeffrey G. Landis * 23 ZwillGen PLLC 1900 M Street N.W., Suite 250 24 Washington, D.C. 20036 Telephone: 202.706.5202 25 202.706.5298 Facsimile: 26 *Pro Hac Vice Admission Pending 27 Attorneys for Apple Inc. 28

TABLE OF CONTENTS

2						<u>Page</u>
3	I.	INTRODUCTION			1	
4	II.	BAC	KGRC	UND		5
5		A.	Apple	e's Ind	lustry-Leading Device Security	5
6		B.	The C For N	Goverr Aandat	ment Abandoned Efforts To Obtain Legal Authority ed Back Doors.	6
7		C.	Apple	e's Sul	bstantial Assistance In The Government's Investigation	10
8 9		D.	The C And	Govern This C	nment's <i>Ex Parte</i> Application Under The All Writs Act, ourt's Order	11
10		E.	The H Dema	Resour anded	ces And Effort Required To Develop The Software By The Government	13
11	III.	ARG	UMEN	٧T		14
12 13		A.	The A	All Wr reate S	its Act Does Not Provide A Basis To Conscript Apple Software Enabling The Government To Hack Into	14
1415			1.	The A	All Writs Act Does Not Grant Authority To Compel stance Where Congress Has Considered But Chosen To Confer Such Authority.	
16 17 18			2.	New The I	York Telephone Co. And Its Progeny Confirm That All Writs Act Does Not Authorize Courts To Compel Unprecedented And Unreasonably Burdensome cription Of Apple That The Government Seeks	
19 20				a.	Apple's Connection To The Underlying Case Is "Far Removed" And Too Attenuated To Compel Its Assistance	20
21 22				b.	The Order Requested By The Government Would Impose An Unprecedented And Oppressive Burden On Apple And Citizens Who Use The iPhone	23
23 24				c.	The Government Has Not Demonstrated Apple's Assistance Was Necessary To Effectuating The Warrant.	29
25			3.	Other Type	r Cases The Government Cites Do Not Support The Of Compelled Action Sought Here.	30
2627		B.			Would Violate The First Amendment And The Fifth t's Due Process Clause.	32
28			1.		First Amendment Prohibits The Government From pelling Apple To Create Code	32

TABLE OF AUTHORITIES

1	$\underline{Page(s)}$
2	Cases
3 4	321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004)
56	Alzheimer's Inst. of Am. Inc. v. Elan Corp., 2013 WL 8744216 (N.D. Cal. Jan. 31, 2013)
7 8 9	In the Matter of an Application of U.S. of Am. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011)
10	Application of U.S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities, 616 F.2d 112221, 22, 27, 29
11 12 13	In re Application of U.S. of Am. for an Order Directing a Provider of Commc'n Servs. to Provide Tech. Assistance to Agents of the U.S. Drug Enf't Admin., 2015 WL 5233551 (D.P.R. Aug. 27, 2015)
14 15 16	In re Application of U.S. of Am. for an Order Directing X to Provide Access to Videotapes ("Videotapes"), 2003 WL 22053105 (D. Md. Aug. 22, 2003)
17 18	Ayres v. Ocwen Loan Serv., LLC, 2013 WL 4784190 (D. Md. Sept. 5, 2013)
19 20	Baker v. Carr, 369 U.S. 186 (1962)
21 22	Bernstein v. Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996)
23 24	Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164 (1994)
25 26	Clark v. Martinez, 543 U.S. 371 (2005)
27	Clinton v. Jones, 520 U.S. 681 (1997)

TABLE OF AUTHORITIES (Continued)

1	(Continuea)	
2		Page(s)
3	Cnty. of Sacramento v. Lewis, 523 U.S. 833 (1998)	34
4	Costanich v. Dep't of Soc. & Health Servs., 627 F.3d 1101 (9th Cir. 2010)	34
5		
6 7	Diamond v. Chakrabarty, 447 U.S. 303 (1980)	19
8	Douglas Oil Co. of Cal. v. Petrol Stops Nw., 441 U.S. 211 (1979)	33
9	<i>Grannis v. Ordean</i> , 234 U.S. 385 (1914)	11
11 12	Junger v. Daley, 209 F.3d 481 (6th Cir. 2000)	
13 14	Members of City Council v. Taxpayers for Vincent, 466 U.S. 789 (1984)	
15 16	Mich. Bell Telephone Co. v. United States, 565 F.2d 385 (6th Cir. 1977)	
17 18	Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306 (1950)	11
19 20	In re Order, 2015 WL 5920207	16, 19, 22
21	In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone,	
2223	2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014) ("Order Requiring [XXX]")	28
24	In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court,	
2526	E.D.N.Y No. 15 MC 1902, Dkt. 19	22
27	In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court,	
28	E.D.N.Y No. 15-MC-1902, Dkt. 27	3

TABLE OF AUTHORITIES (Continued)

1	(Continued)	
2 3	Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34 (1985)	<u>Page(s)</u>
4 5	Pipe Trades Council, U.A. Loc. 159 v. Underground Contractors Ass'n, 835 F.2d 1275 (9th Cir. 1987)	
6 7	Plaut v. Spendthrift Farm, Inc., 514 U.S. 211 (1995)	18
8	Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283 (9th Cir. 1979) 1	, 14, 15, 31, 32
10	Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008)	17
11 12	Riley v. California, 134 S. Ct. 2473 (2014)	25
13 14	Riley v. Nat'l Fed. of the Blind of N.C., Inc., 487 U.S. 781,796 (1988)	32
15 16	Saldana v. Occidental Petroleum Corp., 774 F.3d 544 (9th Cir. 2014) (per curiam)	19
17 18 19	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 35KGD203, No. ED 15-0451M (Feb. 16, 2016), Dkt. 19	
20 21	State v. Underdahl, 767 N.W.2d 677 (Minn. 2009)	
22 23	Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622 (1994)	33
2425	United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012)	24
26 27	United States v. Cameron, 699 F.3d 621 (1st Cir. 2012)	26
28	United States v. Catoggio, 698 F.3d 64 (2d Cir. 2012) (per curiam)	30

Case 5:16-cm-00010-SP Document 16 Filed 02/25/16 Page 8 of 47 Page ID #:88

TABLE OF AUTHORITIES (Continued)

2	United States v. Cooper,	Page(s)
3	983 F.2d 928 (9th Cir. 1993)	24
4 5	United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002)	32
6 7	United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012)	30
8	United States v. Hall, 583 F. Supp. 717 (E.D. Va. 1984)	21, 23, 27
10	United States v. Navarro, No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013), ECF No. 39	28
11 12	United States v. New York Telephone Co., 434 U.S. 159 (1977)	20, 21, 22, 29, 30
13 14	Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001)	32
15 16	Vieth v. Jubelirer, 541 U.S. 267 (2004) (plurality opinion)	19
17 18	Xi v. INS, 298 F.3d 832 (9th Cir. 2002)	19
19	Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952)	18
20 21	Statutes	
22	18 U.S.C. § 2518(4)	17
23	18 U.S.C. § 3282	35
24	28 U.S.C. § 1651	11, 15, 19
25	47 U.S.C. § 1001	8, 17
2627	47 U.S.C. § 1002	

28

TABLE OF AUTHORITIES (Continued)

(00-10-100)	
Other Authorities	Page(s)
Apple Inc., A Message to Our Customers (Feb. 16, 2016)	3, 22
Apple Inc. and Apple Distrib. Int'l, Written Evidence (IPB0093), (Dec. 21, 2015)	7
Apple Inc., iCloud: Back up your iOS device to iCloud	11
Apple Inc., iOS Security: iOS 9.0 or later (September 2015)	6
Apple Inc., Privacy, Government Information Requests	33
Cyrus R. Vance Jr., No Smartphone Lies Beyond the Reach of a Judicial Search Warrant, N.Y. Times (Feb. 18, 2016)	10, 24
Damian Paletta, How the U.S. Fights Encryption—and Also Helps Develop It, Wall St. J. (Feb. 22, 2016)	6
Ellen Nakashima, <i>Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say</i> , Wash. Post (July 9, 2015)	1
Ellen Nakashima and Mark Berman, FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup, Wash. Post (Feb. 20, 2016)	34
Ellen Nakashima, Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders, Wash. Post (Apr. 28, 2013)	9
FBI, Operational Technology, <i>Going Dark Issue</i> (last visited Feb. 23, 2016)	4, 7
Gen. Michael Hayden Gives an Update on the Cyberwar, Wall St. J. (Feb. 17, 2016)	5
H.R. 2233, 114th Cong. (2015) (same, adding additional amendments to the Foreign Intelligence Surveillance Act of 1978)	9
H.R. Rep. No. 103-827(I), (1994)	8, 17
James Comey, Director Discusses Encryption, Patriot Act Provisions (May 20, 2015)	10
James Comey, Encryption, Public Safety, and "Going Dark,"	4

TABLE OF AUTHORITIES (Continued)

1	(Continued)	
2		Page(s)
3	James Comey, Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption, Joint Statement with Deputy	
4	Atty Gen. Sally Quillian Yates Before the Sen. Judiciary Comm. (July 8, 2015)	7
5 6	James Comey, Statement Before the Senate Comm. on Homeland Sec. & Governmental Affairs (Oct. 8, 2015)	9
7 8	James Comey, We Could Not Look the Survivors in the Eye if We Did Not Follow This Lead	
9 10	Kara Swisher, White House. Red Chair. Obama Meets Swisher (Feb. 15, 2015)	10
11 12	Margaret Coker, et al., <i>The Attacks in Paris: Islamic State Teaches Tech Savvy</i> , Wall St. J. (Nov. 17, 2015)	4
13 14	Mike McConnell et al., Why The Fear Over Ubiquitous Data Encryption Is Overblown, Wash. Post (July 28, 2015)	8
15	New America's Open Technology Institute, <i>Joint Letter to President</i> Barack Obama (May 19, 2015)	9
16 17	NPR, Weekend Edition, It's Not Just the iPhone Law Enforcement Wants to Unlock (Feb. 21, 2016)	10
18 19	Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference (Jan. 16, 2015)	10
20	Secure Data Act of 2015, H.R. 726, 114th Cong. (2015)	9
21	Secure Data Act of 2015, S.135, 114th Cong. (2015)	9
222324	Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption, House Comm. on the Judiciary, Democrats (Feb. 18, 2016)	9
25 26	Seung Lee, The Murder Victim Whose Phone Couldn't Be Cracked and Other Apple Encryption Stories, Newsweek (Feb. 19, 2016)	
27 28	Susan Landau, <i>The National-Security Needs for Ubiquitous Encryption</i> (Feb. 1, 2016)	7

Case 5:16-cm-00010-SP Document 16 Filed 02/25/16 Page 11 of 47 Page ID #:91

TABLE OF AUTHORITIES (Continued)

1		
2	Rules	Page(s)
3	Fed. R. Evid. 404	35
5	Fed. R. Evid. 702	24
6	Constitutional Provisions	
7	U.S. Const. amend. I	32
8	U.S. Const. amend. IV	35
9	U.S. Const. amend. V	34
10		
11		
12		
13 14		
15		
16		
17		
18		
19		
20		
21		
22		
2324		
2 4 25		
26		
27		
28		

Gibson, Dunn &

CIUICIICI LLE

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This is not a case about one isolated iPhone. Rather, this case is about the Department of Justice and the FBI seeking through the courts a dangerous power that Congress and the American people have withheld: the ability to force companies like Apple to undermine the basic security and privacy interests of hundreds of millions of individuals around the globe. The government demands that Apple create a back door to defeat the encryption on the iPhone, making its users' most confidential and personal information vulnerable to hackers, identity thieves, hostile foreign agents, and unwarranted government surveillance. The All Writs Act, first enacted in 1789 and on which the government bases its entire case, "does not give the district court a roving commission" to conscript and commandeer Apple in this manner. *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). In fact, no court has ever authorized what the government now seeks, no law supports such unlimited and sweeping use of the judicial process, and the Constitution forbids it.

Since the dawn of the computer age, there have been malicious people dedicated to breaching security and stealing stored personal information. Indeed, the government itself falls victim to hackers, cyber-criminals, and foreign agents on a regular basis, most famously when foreign hackers breached Office of Personnel Management databases and gained access to personnel records, affecting over 22 million current and former federal workers and family members. In the face of this daily siege, Apple is dedicated to enhancing the security of its devices, so that when customers use an iPhone, they can feel confident that their most private personal information—financial records and credit card information, health information, location data, calendars, personal and political beliefs, family photographs, information about their children—

See, e.g., Hanna Decl. Ex. A [Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Wash. Post (July 9, 2015)] (explaining that hackers used stolen logins and passwords to gain access to federal employee records databases for six months before detection).

will be safe and secure. To this end, Apple uses encryption to protect its customers from cyber-attack and works hard to improve security with every software release because the threats are becoming more frequent and sophisticated. Beginning with iOS 8, Apple added additional security features that incorporate the passcode into the encryption system. It is these protections that the government now seeks to roll back by judicial decree.

There are two important and legitimate interests in this case: the needs of law enforcement and the privacy and personal safety interests of the public. In furtherance of its law enforcement interests, the government had the opportunity to seek amendments to existing law, to ask Congress to adopt the position it urges here. But rather than pursue new legislation, the government backed away from Congress and turned to the courts, a forum ill-suited to address the myriad competing interests, potential ramifications, and unintended consequences presented by the government's unprecedented demand. And more importantly, by invoking "terrorism" and moving *ex parte* behind closed courtroom doors, the government sought to cut off debate and circumvent thoughtful analysis.

The order demanded by the government compels Apple to create a new operating system—effectively a "back door" to the iPhone—that Apple believes is too dangerous to build. Specifically, the government would force Apple to create new software with functions to remove security features and add a new capability to the operating system to attack iPhone encryption, allowing a passcode to be input electronically. This would make it easier to unlock the iPhone by "brute force," trying thousands or millions of passcode combinations with the speed of a modern computer. In short, the government wants to compel Apple to create a crippled and insecure product. Once the process is created, it provides an avenue for criminals and foreign agents to access millions of iPhones. And once developed for our government, it is only a matter of time before foreign governments demand the same tool.

The government says: "Just this once" and "Just this phone." But the government knows those statements are not true; indeed the government has filed multiple other applications for similar orders, some of which are pending in other courts.² And as news of this Court's order broke last week, state and local officials publicly declared their intent to use the proposed operating system to open hundreds of other seized devices—in cases having nothing to do with terrorism.³ If this order is permitted to stand, it will only be a matter of days before some other prosecutor, in some other important case, before some other judge, seeks a similar order using this case as precedent. Once the floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound without so much as a congressional vote. As Tim Cook, Apple's CEO, recently noted: "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." Declaration of Nicola T. Hanna ("Hanna Decl."), Ex. D [Apple Inc., A Message to Our Customers (Feb. 16, 2016)].

Despite the context of this particular action, no legal principle would limit the use of this technology to domestic terrorism cases—but even if such limitations could be imposed, it would only drive our adversaries further underground, using encryption technology made by foreign companies that cannot be conscripted into U.S.

22

23

24

25

26

27

28

18

19

²¹

² Hanna Decl. Ex. B [Letter to Court, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, E.D.N.Y No. 15-MC-1902, Dkt. 27].

³ E.g., Hanna Decl. Ex. C [Seung Lee, *The Murder Victim Whose Phone Couldn't Be Cracked and Other Apple Encryption Stories*, Newsweek (Feb. 19, 2016)] (Cyrus Vance, Manhattan District Attorney stating that he has "155 to 160" devices that he would like to access, while officials in Sacramento have "well over 100" devices for which they would like Apple to produce unique software so that they can access the devices' contents); Hanna Decl. ¶ 5 at 18:28 [Charlie Rose, Television Interview of Cyrus Vance (Feb. 18, 2016)] (Vance stating "absolutely" that he "want[s] access to all those phones that [he thinks] are crucial in a criminal proceeding").

government service⁴—leaving law-abiding individuals shouldering all of the burdens on liberty, without any offsetting benefit to public safety. Indeed, the FBI's repeated warnings that criminals and terrorists are able to "go dark" behind end-to-end encryption methods proves this very point. *See* Hanna Decl. Ex. F [FBI, Operational Technology, *Going Dark Issue* (last visited Feb. 23, 2016) ("FBI, Going Dark")].

Finally, given the government's boundless interpretation of the All Writs Act, it is hard to conceive of any limits on the orders the government could obtain in the future. For example, if Apple can be forced to write code in this case to bypass security features and create new accessibility, what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user? Nothing.

As FBI Director James Comey expressly recognized:

Democracies resolve such tensions through robust debate. . . . It may be that, as a people, we decide the benefits [of strong encryption] outweigh the costs and that there is no sensible, technically feasible way to optimize privacy and safety in this particular context, or that public safety folks will be able to do their job well enough in the world of universal strong encryption. Those are decisions Americans should make, but I think part of my job is [to] make sure the debate is informed by a reasonable understanding of the costs.

Hanna Decl. Ex. G [James Comey, *Encryption, Public Safety, and "Going Dark,"*Lawfare (July 6, 2015, 10:38 AM) ("Comey, *Going Dark"*)]; *see also* Hanna Decl. Ex. H [James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow This Lead*, Lawfare (Feb. 21, 2016, 9:03 PM) ("Comey, *Follow This Lead"*)] (reiterating that the tension between national security and individual safety and privacy "should not be resolved by the FBI, which investigates for a living[, but rather] . . . by the American people"). The government, by seeking an order mandating that

⁴ See Hanna Decl. Ex. E [Margaret Coker, et al., *The Attacks in Paris: Islamic State Teaches Tech Savvy*, Wall St. J. (Nov. 17, 2015) ("Coker, *Tech Savvy*")] (describing the technological sophistication of terrorists groups, including, for example, ISIS's ability and willingness to shift to more secure communication methods).

Apple create software to destabilize the security of the iPhone and the law-abiding citizens who use it to store data touching on every facet of their private lives, is not acting to inform or contribute to the debate; it is seeking to avoid it.

Apple strongly supports, and will continue to support, the efforts of law enforcement in pursuing justice against terrorists and other criminals—just as it has in this case and many others. But the unprecedented order requested by the government finds no support in the law and would violate the Constitution. Such an order would inflict significant harm—to civil liberties, society, and national security—and would preempt decisions that should be left to the will of the people through laws passed by Congress and signed by the President. Accordingly, the Court should vacate the order and deny the government's motion to compel.⁵

II. BACKGROUND

A. Apple's Industry-Leading Device Security.

Apple is committed to data security. Encryption provides Apple with the strongest means available to ensure the safety and privacy of its customers against threats known and unknown.⁶ For several years, iPhones have featured hardware- and

The government filed its motion to compel notwithstanding the Court allowing an eight-day period within which Apple could challenge the order compelling assistance, Apple's express indication during the parties' February 18 status conference that it intended to seek relief from the order, the Court's entry of a briefing schedule to permit the parties to address the validity of the order, and the Court's own skepticism about the utility of such a motion. That skepticism proved warranted. Only three pages into the government's 25-page motion, it concedes the motion is "not legally necessary." Dkt. 1 at 3 n.3. Nor could the government claim otherwise, as the motion—substantial portions of which appear to have been cut and pasted from the government's ex parte application—seeks no relief beyond that contemplated by the order compelling assistance. Because the government's motion serves no legal purpose, and the issues it raises will be fully briefed and addressed in Apple's motion to vacate and the government's opposition thereto, it should be denied. See, e.g., Pipe Trades Council, U.A. Loc. 159 v. Underground Contractors Ass'n, 835 F.2d 1275, 1279 (9th Cir. 1987) (concluding a district court properly denied a motion to compel as premature); cf. Ayres v. Ocwen Loan Serv., LLC, 2013 WL 4784190, at *3 (D. Md. Sept. 5, 2013) (striking sua sponte a motion that was "not technically ripe" and "meandering, redundant, transparent, and largely oblivious to the posture of the case").

⁶ Former NSA and CIA Director Michael Hayden has recognized that, on balance, America is more secure because of "end-to-end unbreakable encryption." Hanna Decl. Ex. I [Gen. Michael Hayden Gives an Update on the Cyberwar, Wall St. J.

(Cont'd on next page)

1 SO 2 N 3 en 4 ¶ 5 (" 6 pn 7 oj 8 iO 9 pn 10 N 11 12 us

software-based encryption of their password-protected contents. Declaration of Erik Neuenschwander ("Neuenschwander Decl.") ¶ 8. These protections safeguard the encryption keys on the device with a passcode designated by the user during setup. *Id.* ¶ 9. This passcode immediately becomes entangled with the iPhone's Unique ID ("UID"), which is permanently assigned to that one device during the manufacturing process. *Id.* ¶ 13. The iPhone's UID is neither accessible to other parts of the operating system nor known to Apple. *See generally* Hanna Decl. Ex. K [Apple Inc., *iOS Security: iOS 9.0 or later* (September 2015)]. These protections are designed to prevent anyone without the passcode from accessing encrypted data on iPhones. Neuenschwander Decl. ¶ 8.

Cyber-attackers intent on gaining unauthorized access to a device could break a user-created passcode, if given enough chances to guess and the ability to test passwords rapidly by automated means. To prevent such "brute-force" attempts to determine the passcode, iPhones running iOS 8 and higher include a variety of safeguards. *Id.* ¶ 10. For one, Apple uses a "large iteration count" to slow attempts to access an iPhone, ensuring that it would take years to try all combinations of a six-character alphanumeric passcode. *Id.* ¶ 11. In addition, Apple imposes escalating time delays after the entry of each invalid passcode. *Id.* ¶ 12. Finally, Apple also includes a setting that—if activated—automatically deletes encrypted data after ten consecutive incorrect attempts to enter the passcode. *Id.* This combination of security features protects users from attackers or if, for example, the user loses the device.

B. The Government Abandoned Efforts To Obtain Legal Authority For Mandated Back Doors.

Some in the law enforcement community have disparaged the security improvements by Apple and others, describing them as creating a "going dark"

⁽Cont'd from previous page)

⁽Feb. 17, 2016)]; cf. Hanna Decl. Ex. J [Damian Paletta, How the U.S. Fights Encryption—and Also Helps Develop It, Wall St. J. (Feb. 22, 2016)] (describing funding by U.S. government of stronger encryption technologies).

problem in which law enforcement may possess the "legal authority to intercept and access communications and information pursuant to court orders" but lack the "technical ability to carry out those orders because of a fundamental shift in communications services and technologies." As a result, some officials have advanced the view that companies should be required to maintain access to user communications and data and provide that information to law enforcement upon satisfaction of applicable legal requirements. This would give the government, in effect, a back door to otherwise encrypted communications—which would be precisely the result of the government's position in this case.

Apple and other technology companies, supported by leading security experts, have disagreed with law enforcement's position, observing that any back door enabling government officials to obtain encrypted data would also create a vulnerability that could be exploited by criminals and foreign agents, weakening critical security protections and creating new and unforeseen access to private information. For these reasons, Apple and others have strongly opposed efforts to require companies to enable the government to obtain encrypted information, arguing that this would compromise the security offered to its hundreds of millions of law-abiding customers in order to weaken security for the few who may pose a threat.¹⁰

As leading former national security officials have made clear, Apple's "resistance to building in a back door" in whatever form it may take is well-justified,

⁷ Hanna Decl. Ex. F [FBI, *Going Dark*].

See, e.g., Hanna Decl. Ex. L [James Comey, Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption, Joint Statement with Deputy Atty. Gen. Sally Quillian Yates Before the Sen. Judiciary Comm. (July 8, 2015)]. The repeated concern about the broader "going dark" problem, and the focus on universal back doors, stands in stark contrast to the comments by government officials that this case is about just one iPhone.

⁹ See Hanna Decl. Ex. M [Susan Landau, The National-Security Needs for Ubiquitous Encryption (Feb. 1, 2016)].

See Hanna Decl. Ex. N, ¶ 20 [Apple Inc. and Apple Distrib. Int'l, Written Evidence (IPB0093), (Dec. 21, 2015)].

because "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."¹¹

In recent years, however, the government, led by the Department of Justice, has considered legislative proposals that would have mandated such a back door. Those proposals sought to significantly expand the reach of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1001 *et seq.*, in which Congress defined the circumstances under which private companies must assist law enforcement in executing authorized electronic surveillance and the nature of—and limits on—the assistance such companies must provide.¹² In addressing the twin needs of law enforcement and privacy, Congress, through CALEA, specified when a company has an obligation to assist the government with decryption of communications, and made clear that a company has no obligation to do so where, as here, the company does not retain a copy of the decryption key. 47 U.S.C. § 1002(b)(3). Congress, keenly aware of and focusing on the specific area of dispute here, thus opted *not* to provide authority to compel companies like Apple to assist law enforcement with respect to data stored on a smartphone they designed and manufactured.¹³

Hanna Decl. Ex. O [Mike McConnell et al., Why The Fear Over Ubiquitous Data Encryption Is Overblown, Wash. Post (July 28, 2015)].

Following a vigorous lobbying effort led by the FBI for enhanced surveillance and informational-access powers in the digital age, Congress "balance[d] 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." H.R. Rep. No. 103-827(I), at 13 (1994), as reprinted in 1994 U.S.C.C.A.N. 3489, 3493; see also id. at 17, 1994 U.S.C.C.A.N. at 3497 ("[A]s the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.").

The government has acknowledged this. Dkt. 1 at 23. CALEA requires only "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. CALEA defines "telecommunications carrier" to exclude persons or entities providing "information services," such as Apple. *Id.* § 1001(8).

2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |

The government's proposed changes to CALEA would have dramatically expanded the law's scope by mandating that companies install back doors into their products to ensure that authorities can access encrypted data when authorized to do so. ¹⁴ In the face of this proposal—commonly referred to as "CALEA II"—leading technology companies, including Apple, as well as public interest organizations like the ACLU and Human Rights Watch, urged President Obama to "reject any proposal that U.S. companies deliberately weaken the security of their products . . . [and] instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology." ¹⁵

The Executive Branch ultimately decided not to pursue CALEA II, and Congress has left CALEA untouched, meaning that Congress never granted the authority the government now asserts. Moreover, members of Congress have recently introduced three pieces of legislation that would affirmatively prohibit the government from forcing private companies like Apple to compromise data security. On October 8, 2015, FBI Director Comey confirmed that the Obama Administration would not seek passage of CALEA II at that time. Instead, Director Comey expressed his view

See Hanna Decl. Ex. P [Ellen Nakashima, *Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, Wash. Post (Apr. 28, 2013)].

Hanna Decl. Ex. Q [New America's Open Technology Institute, *Joint Letter to President Barack Obama* (May 19, 2015)].

See Secure Data Act of 2015, S.135, 114th Cong. (2015) (proposal to prohibit a federal agency from requiring hardware or software manufacturers to design or alter the 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, adding additional amendments to the Foreign Intelligence Surveillance Act of 1978). In fact, just last week, four senior members of the House Judiciary Committee issued a statement expressing concern that the order in this case constitutes an "end-run around the legislative process." Hanna Decl. Ex. R [Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption, House Comm. on the Judiciary, Democrats (Feb. 18, 2016)]. Recognizing that Congress has not yet determined to act on this issue, they stated that "there is little reason for the government to make this demand on Apple—except to enact a policy proposal that has gained no traction in Congress and was rejected by the White House." Id.

Hanna Decl. Ex. S [James Comey, Statement Before the Senate Comm. on Homeland Sec. & Governmental Affairs (Oct. 8, 2015)] (noting that while the (Cont'd on next page)

that the "going dark" debate raises issues that "to a democracy should be very, very concerning" and therefore the issue is "worthy of a larger public conversation." ¹⁸ 2 President Obama has also remarked that it is "useful to have civil libertarians and 3 others tapping us on the shoulder in the midst of this process and reminding us that 4 there are values at stake as well," noting further that he "welcome[s] that kind of 5 debate." 19 As the President has recognized, these issues are part of "a public 6 conversation that we should end up having."²⁰ 7

C. Apple's Substantial Assistance In The Government's Investigation

Apple was shocked and saddened by the mindless savagery of the December 2, 2015 terrorist attack in San Bernardino. In the days following the attack, the FBI approached Apple for help in its investigation. Apple responded immediately, and devoted substantial resources on a 24/7 basis to support the government's investigation of this heinous crime. Declaration of Lisa Olle ("Olle Decl.") ¶ 5-9.

Apple promptly provided all data that it possessed relating to the attackers' accounts and that the FBI formally requested via multiple forms of legal process, in keeping with Apple's commitment to comply with all legally valid subpoenas and

(Cont'd from previous page)

1

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

[&]quot;United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services . . . the administration is not seeking legislation at this time.").

See Hanna Decl. Ex. T [James Comey, Director Discusses Encryption, Patriot Act Provisions, (May 20, 2015)]. Even Manhattan District Attorney Cyrus Vance, Jr., who is eager to see the government prevail here, has acknowledged that these issues should be resolved by Congress. Hanna Decl. Ex. Z [Cyrus R. Vance Jr., No Smartphone Lies Beyond the Reach of a Judicial Search Warrant, N.Y. Times (Feb. 18, 2016)]; Hanna Decl. Ex. U [NPR, Weekend Edition, It's Not Just the iPhone Law Enforcement Wants to Unlock (Feb. 21, 2016)] ("... I think that the United States Congress is going to have to step in here." We need to look at this with States Congress is going to have to step in here . . . We need to look at this with independent eyes. And I believe Congress ultimately is going to have to make the judgment call of where we draw that line [between privacy and public safety]".).

Hanna Decl. Ex. V [Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference (Jan. 16, 2015)].

Hanna Decl. Ex. W [Kara Swisher, White House. Red Chair. Obama Meets Swisher, Re/Code.com (Feb. 15, 2015)].

search warrants that the company receives. Id. Additionally, Apple has furnished valuable informal assistance to the government's investigation—participating in teleconferences, providing technical assistance, answering questions from the FBI, and suggesting potential alternatives for the government to attempt to obtain data from the iPhone at issue. Id. \P 6.

Unfortunately, the FBI, without consulting Apple or reviewing its public guidance regarding iOS, changed the iCloud password associated with one of the attacker's accounts, foreclosing the possibility of the phone initiating an automatic iCloud back-up of its data to a known Wi-Fi network, *see* Hanna Decl. Ex. X [Apple Inc., *iCloud: Back up your iOS device to iCloud*], which could have obviated the need to unlock the phone and thus for the extraordinary order the government now seeks.²¹ Had the FBI consulted Apple first, this litigation may not have been necessary.

D. The Government's *Ex Parte* Application Under The All Writs Act, And This Court's Order

On February 16, 2016, the government filed an *ex parte* application and proposed order asking the Court to compel Apple to assist in the government's investigation under the authority of the All Writs Act, codified at 28 U.S.C. § 1651.²²

In its motion to compel, filed February 19 with this Court, the government sought to shift the blame to the "owner" (San Bernardino County) in describing who changed the password and why it allegedly has no other viable alternatives besides the creation of a new operating system. Dkt. 1 at 18 n.7. The FBI later issued a press release acknowledging that it "worked with" the County to reset the password. See Hanna Decl. Ex. Y [Statement to Address Misleading Reports that the County of San Bernardino Reset Terror Suspect's iPhone Without Consent of the FBI, issued by the FBI to Ars Technica (Feb. 21, 2016)].

The government obtained the Order without notice to Apple and without allowing Apple an opportunity to be heard. See Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306, 314 (1950) (recognizing that one of the "fundamental requisite[s] of due process of law is the opportunity to be heard") (quoting Grannis v. Ordean, 234 U.S. 385, 394 (1914)). But this was not a case where the government needed to proceed in secret to safeguard its investigation; indeed, Apple understands that the government alerted reporters before filing its ex parte application, and then, immediately after it was signed and confirmed to be on the docket, distributed the application and Order to the public at about the same time it notified Apple. Moreover, this is the only case in counsel's memory in which an FBI Director has blogged in real-time about pending litigation, suggesting that the government does not believe the data on the phone will yield critical evidence about other suspects. (Cont'd on next page)

With no opposition or other perspectives to consider, the Court granted the government's request and signed the government's proposed order, thereby compelling Apple to create new software that would allow the government to hack into an iPhone 5c used by one of the attackers. Order Compelling Apple Inc. to Assist Agents in Search, *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 35KGD203*, No. ED 15-0451M (Feb. 16, 2016), Dkt. at 19 (the "Order").

The Order directs Apple to provide "reasonable technical assistance to assist law enforcement agents in obtaining access to the data" on the device. Id. ¶ 1. The Order further defines this "reasonable technical assistance" to include creating custom software that can be loaded on the iPhone to accomplish three goals: (1) bypass or disable the iPhone's "auto-erase" function, designed to protect against efforts to obtain unauthorized access to the device's encrypted contents by deleting encrypted data after ten unsuccessful attempts to enter the iPhone's passcode, (2) enable the FBI to electronically submit passcodes to the device for testing, bypassing the requirement that passcodes be manually entered, and (3) remove any time delays between entering incorrect passcodes. Id. ¶ 2. Because the government proceeded ex parte, Apple had no opportunity to weigh in on whether such assistance was "reasonable," and thus the government's request was assumed to be.

The software envisioned by the government simply does not exist today. Thus, at bottom, the Order would compel Apple to create a new version of the iPhone operating system designed to defeat the critical security features noted previously for the specific purpose of accessing the device's contents in unencrypted form—in other words, to write new software to create a back door to the device's encrypted data.

(Cont'd from previous page)

See Hanna Decl. Ex. G [Comey, Going Dark]; Hanna Decl. Ex. H [Comey, Follow This Lead].

E. The Resources And Effort Required To Develop The Software Demanded By The Government

The compromised operating system that the government demands would require significant resources and effort to develop. Although it is difficult to estimate, because it has never been done before, the design, creation, validation, and deployment of the software likely would necessitate six to ten Apple engineers and employees dedicating a very substantial portion of their time for a minimum of two weeks, and likely as many as four weeks. Neuenschwander Decl. ¶ 22. Members of the team would include engineers from Apple's core operating system group, a quality assurance engineer, a project manager, and either a document writer or a tool writer. *Id*.

No operating system currently exists that can accomplish what the government wants, and any effort to create one will require that Apple write new code, not just disable existing code functionality. *Id.* ¶¶ 24-25. Rather, Apple will need to design and implement untested functionality in order to allow the capability to enter passcodes into the device electronically in the manner that the government describes. *Id.* ¶ 24. In addition, Apple would need to either develop and prepare detailed documentation for the above protocol to enable the FBI to build a brute-force tool that is able to interface with the device to input passcode attempts, or design, develop and prepare documentation for such a tool itself. *Id.* ¶ 25. Further, if the tool is utilized remotely (rather than at a secure Apple facility), Apple will also have to develop procedures to encrypt, validate, and input into the device communications from the FBI. *Id.* This entire development process would need to be logged and recorded in case Apple's methodology is ever questioned, for example in court by a defense lawyer for anyone charged in relation to the crime. *Id.* ¶ 28.

Once created, the operating system would need to go through Apple's quality assurance and security testing process. Id. ¶ 29. Apple's software ecosystem is incredibly complicated, and changing one feature of an operating system often has ancillary or unanticipated consequences. Id. ¶ 30. Thus, quality assurance and security testing would require that the new operating system be tested on multiple

devices and validated before being deployed. *Id.* Apple would have to undertake additional testing efforts to confirm and validate that running this newly developed operating system to bypass the device's security features will not inadvertently destroy or alter any user data. *Id.* ¶ 31. To the extent problems are identified (which is almost always the case), solutions would need to be developed and re-coded, and testing would begin anew. *Id.* ¶ 32. As with the development process, the entire quality assurance and security testing process would need to be logged, recorded, and preserved. *Id.* ¶ 33. Once the new custom operating system is created and validated, it would need to be deployed on to the subject device, which would need to be done at an Apple facility. *Id.* ¶¶ 34-35. And if the new operating system has to be destroyed and recreated each time a new order is issued, the burden will multiply. *Id.* ¶¶ 44-45.

III. ARGUMENT

A. The All Writs Act Does Not Provide A Basis To Conscript Apple To Create Software Enabling The Government To Hack Into iPhones.

The All Writs Act (or the "Act") does not provide the judiciary with the boundless and unbridled power the government asks this Court to exercise. The Act is intended to enable the federal courts to fill in gaps in the law so they can exercise the authority they already possess by virtue of the express powers granted to them by the Constitution and Congress; it does not grant the courts free-wheeling authority to change the substantive law, resolve policy disputes, or exercise new powers that Congress has not afforded them. Accordingly, the Ninth Circuit has squarely rejected the notion that "the district court has such wide-ranging inherent powers that it can impose a duty on a private party when Congress has failed to impose one. To so rule would be to usurp the legislative function and to improperly extend the limited federal court jurisdiction." *Plum Creek*, 608 F.2d at 1290 (emphasis added).

Congress has never authorized judges to compel innocent third parties to provide decryption services to the FBI. Indeed, Congress has expressly withheld that authority in other contexts, and this issue is currently the subject of a raging national

policy debate among members of Congress, the President, the FBI Director, and state and local prosecutors. Moreover, federal courts themselves have *never* recognized an inherent authority to order non-parties to become de facto government agents in ongoing criminal investigations. Because the Order is not grounded in any duly enacted rule or statute, and goes well beyond the very limited powers afforded by Article III of the Constitution and the All Writs Act, it must be vacated.

1. The All Writs Act Does Not Grant Authority To Compel Assistance Where Congress Has Considered But Chosen Not To Confer Such Authority.

The authority the government seeks here cannot be justified under the All Writs Act because law enforcement assistance by technology providers is covered by existing laws that specifically omit providers like Apple from their scope. The All Writs Act authorizes 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), but as the Supreme Court has held, it "does not authorize [courts] to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate," Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 38, 43 (1985) (holding that the Act did not confer power on the district court to compel noncustodians to bear the expense of producing the prisoner-witnesses); see also In the Matter of an Application of U.S. of Am. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 578 (D. Md. 2011) (holding that the Act does not authorize an "end run around constitutional and statutory law"). The Ninth Circuit likewise has emphasized that the "All Writs Act is not a grant of plenary power to federal courts. Rather, it is designed to aid the courts in the exercise of their jurisdiction." *Plum Creek*, 608 F.2d at 1289 (holding that the Act "does not give the district court a roving commission to order a party subject to an investigation to accept additional risks at the bidding" of the government); see also Ex parte Bollman, 8. U.S. 75 (1807) ("[C]ourts which are created by written law, and whose jurisdiction is defined by written law, cannot transcend that jurisdiction.").

25

26

27

Thus, in another pending case in which the government seeks to compel Apple to assist in obtaining information from a drug dealer's iPhone, Magistrate Judge Orenstein issued an order stating that while the Act may be appropriately invoked "to fill in a statutory gap that Congress has failed to consider," it cannot be used to grant the government authority "Congress chose not to confer." *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court* ("*In re Order*"), No. 15-MC-1902, 2015 WL 5920207, at *2 (E.D.N.Y. Oct. 9, 2015).

Congress knows how to impose a duty on third parties to facilitate the government's decryption of devices. Similarly, it knows exactly how to place limits on what the government can require of telecommunications carriers and also on manufacturers of telephone equipment and handsets. And in CALEA, Congress decided not to require electronic communication service providers, like Apple, to do what the government seeks here. Contrary to the government's contention that CALEA is inapplicable to this dispute, Congress declared via CALEA that the government cannot dictate to providers of electronic communications services or manufacturers of telecommunications equipment any specific equipment design or software configuration.

In the section of CALEA entitled "Design of features and systems configurations," 47 U.S.C. § 1002(b)(1), the statute says that it "does not authorize any law enforcement agency or officer—

- (1) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.
- (2) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

Apple unquestionably serves as a provider of "electronic communications services" through the various messaging services it provides to its customers through iPhones.

See Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008). Apple also makes mobile phones. As such, CALEA does not allow a law enforcement agency to require Apple to implement any specific design of its equipment, facilities, services or system configuration. Yet, that is precisely what the government seeks here. Thus, CALEA's restrictions are directly on point.

Moreover, CALEA also intentionally excludes information services providers, like Apple, from the scope of its mandatory assistance provisions.²³ This exclusion precludes the government from using the All Writs Act to require Apple to do that which Congress eschewed. But even if Apple were covered by CALEA, the law does not require covered telecommunication carriers (which Apple is not) to be responsible for "decrypting, or *ensuring the government's ability to decrypt*, any communication encrypted by a subscriber or customer unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." 47 U.S.C. § 1002(b)(3) (emphasis added).

Thus, here again, CALEA makes a specific choice to allow strong encryption (or any other security feature or configuration) with keys chosen by end users to be deployed, and prevents the government from mandating that such encryption schemes contain a "back door." *See also* H.R. Rep. 103-827(I), at 24, 1994 U.S.C.C.A.N. 3489, 3504 (emphasizing that CALEA does not "prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access"; "[n]or does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, [§ 1002] protects the right to use encryption.").

Similarly, outside of CALEA, Congress also knows how to require third parties to provide "technical assistance," *see* Wiretap Act, 18 U.S.C. § 2518(4) (providing that

Information service providers are defined to include services that permit a customer to retrieve stored information from, or file information for storage in, information storage facilities; electronic publishing; and electronic messaging services. *See* 47 U.S.C. § 1001.

upon the lawful execution of a wiretap, the government can seek an order compelling a third party to furnish "all information, facilities, and technical assistance necessary to accomplish the interception"); Pen/Trap Statute, *id.* § 3123(b)(2) (similar), but Congress has intentionally opted not to compel third parties' assistance in retrieving stored information on devices. That Congress, confronted over the years with the contentious debate about where to draw the lines among competing security and privacy interests, made this decision, "indicates a deliberate congressional choice with which the courts should not interfere." *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver*, N.A., 511 U.S. 164, 184 (1994). The Executive Branch, having considered and then declined to urge Congress to amend CALEA to enable it to compel the type of assistance demanded here, cannot seek that same authority via an *ex parte* application for a court order under the Act.

For the courts to use the All Writs Act to expand sub rosa the obligations imposed by CALEA as proposed by the government here would not just exceed the scope of the statute, but it would also violate the separation-of-powers doctrine. Just as the "Congress may not exercise the judicial power to revise final judgments," Clinton v. Jones, 520 U.S. 681, 699 (1997) (citing Plaut v. Spendthrift Farm, Inc., 514 U.S. 211 (1995)), courts may not exercise the legislative power by repurposing statutes to meet the evolving needs of society, see Clark v. Martinez, 543 U.S. 371, 391 (2005) (court should "avoid inventing a statute rather than interpreting one") (citation, quotation marks, and alterations omitted); see also Alzheimer's Inst. of Am. Inc. v. Elan Corp., 2013 WL 8744216, at *2 (N.D. Cal. Jan. 31, 2013) (Congress alone has authority "to update" a "technologically antiquated" statute "to address the new and rapidly evolving era of computer and cloud-stored, processed and produced data"). Nor does Congress lose "its exclusive constitutional authority to make laws necessary and proper to carry out the powers vested by the Constitution" in times of crisis (whether real or imagined). Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 588–89 (1952). Because a "decision to rearrange or rewrite [a] statute falls within

1

3

4 5

6 7 8

9 10

11

12 13

14

16

15

17

18 19

20

21 22

23

24

25

26

28

the legislative, not the judicial prerogative[,]" the All Writs Act cannot possibly be deemed to grant to the courts the extraordinary power the government seeks. Xi v. INS, 298 F.3d 832, 839 (9th Cir. 2002).

If anything, whether companies like Apple should be compelled to create a back door to their own operating systems to assist law enforcement is a political question, not a legal one. See Baker v. Carr, 369 U.S. 186, 217 (1962) (holding that a case is a nonjusticiable political question if it is impossible to decide "without an initial policy determination of a kind clearly for nonjudicial discretion"); see also Vieth v. Jubelirer, 541 U.S. 267, 277–290 (2004) (plurality opinion) (dismissing claims of political gerrymandering under the political question doctrine because there was no "judicially discoverable and manageable standard for resolving" them); Diamond v. Chakrabarty, 447 U.S. 303, 317 (1980) ("The choice [the court is] urged to make is a matter of high policy for resolution within the legislative process after the kind of investigation, examination, and study that legislative bodies can provide and courts cannot."); Saldana v. Occidental Petroleum Corp., 774 F.3d 544, 552 (9th Cir. 2014) (per curiam) (affirming district court's holding that the claims were "inextricably bound to an inherently political question" and thus were "beyond the jurisdiction of our courts").

In short, a decision to "short-circuit public debate on this controversy seems fundamentally inconsistent with the proposition that such important policy issues should be determined in the first instance by the legislative branch after public debate—as opposed to having them decided by the judiciary in sealed, ex parte proceedings." In re Order, 2015 WL 5920207, at *3 n.1. Such an important decision with such widespread global repercussions goes well beyond the purview of the All Writs Act, which merely provides courts with a limited grant of ancillary authority to issue orders "in aid of their respective jurisdictions." 28 U.S.C. § 1651(a).

2
 3
 4

2. New York Telephone Co. And Its Progeny Confirm That The All Writs Act Does Not Authorize Courts To Compel The Unprecedented And Unreasonably Burdensome Conscription Of Apple That The Government Seeks.

The government relies heavily on the Supreme Court's decision in *United States* v. New York Telephone Co., 434 U.S. 159 (1977), to assert that the All Writs Act permits the Court to compel private third parties like Apple to assist the government in effectuating a search warrant by writing new software code that would undermine the security of its own product. The government misapplies this case.

In *New York Telephone Co.*, the district court compelled the company to install a simple pen register device (designed to record dialed numbers) on two telephones where there was "probable cause to believe that the [c]ompany's facilities were being employed to facilitate a criminal enterprise on a continuing basis." 434 U.S. at 174. The Supreme Court held that the order was a proper writ under the Act, because it was consistent with Congress's intent to compel third parties to assist the government in the use of surveillance devices, and it satisfied a three-part test imposed by the Court.

First, the Court found that the company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." *Id*. Second, the assistance sought was "meager," and as a public utility, the company did not "ha[ve] a substantial interest in not providing assistance." *Id*. Third, "after an exhaustive search," the FBI was unable to find a suitable location to install its own pen registers without tipping off the targets, and thus there was "no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished" without the company's meager assistance. *Id*. at 175. Applying these factors to this case confirms that the All Writs Act does not permit the Court to compel the unprecedented and unreasonably burdensome assistance that the government seeks.

a. Apple's Connection To The Underlying Case Is "Far Removed" And Too Attenuated To Compel Its Assistance

Nothing connects Apple to this case such that it can be drafted into government service to write software that permits the government to defeat the security features on

21

22

23

24

25

26

27

28

Apple's standard operating system. Apple 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 in any way to the events giving rise to the investigation. This case is nothing like *New York Telephone Co.*, where there was probable cause to believe that the phone company's own facilities were "being employed to facilitate a criminal enterprise on a continuing basis." *Id.* at 174.

The government relies on *United States v. Hall*, 583 F. Supp. 717 (E.D. Va. 1984), and In re Application of U.S. of Am. for an Order Directing X to Provide Access to Videotapes ("Videotapes"), 2003 WL 22053105 (D. Md. Aug. 22, 2003), but these cases involved mere requests to produce existing business records, not the compelled creation of intellectual property. In Hall, the court found that the All Writs Act permitted an order compelling a credit card company to produce the credit card records of a federal fugitive's former girlfriend, because the government had reason to believe that she was harboring and supporting the fugitive, and thus potentially using her credit card to perpetrate an ongoing crime. 583 F. Supp. at 720 (reasoning that a credit card issuer "has an interest" in a transaction "when a credit card is used for an illegal purpose even though the act itself be not illegal"). Similarly, in Videotapes, the court compelled an apartment complex to provide access to videotape surveillance footage of a hallway in the apartment to assist with executing an arrest warrant on a fugitive. 2003 WL 22053105, at *3. This case is nothing like *Hall* and *Videotapes*, where the government sought assistance effectuating an arrest warrant to halt ongoing criminal activity, since any criminal activity linked to the phone at issue here ended more than two months ago when the terrorists were killed.

Further, unlike a telecommunications monopoly, Apple is not a "highly regulated public utility with a duty to serve the public." *New York Telephone Co.*, 434 U.S. at 174; *see also Application of U.S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities* ("Mountain Bell"), 616 F.2d 1122, 1132 (9th Cir. 1980) (discussing *New York Telephone Co.* and noting that its

18

19

20

21

22

23

24

25

26

27

28

ruling compelling assistance under the All Writs Act relied "[t]o a great extent . . . upon the highly regulated, public nature" of the phone company); *In re Order*, 2015 WL 5920207, at *4–5. Whereas public utilities have no "substantial interest in not providing assistance" to the government, 434 U.S. at 174, and "enjoy a monopoly in an essential area of communications," *Mountain Bell*, 616 F.2d at 1131, Apple is a private company that believes that encryption is crucial to protect the security and privacy interests of citizens who use and store their most personal data on their iPhones, "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." Hanna Decl. Ex. D at 1 [Apple Inc., *A Message to Our Customers* (Feb. 16, 2016)].

That Apple "designed, manufactured and sold the SUBJECT DEVICE, and wrote and owns the software that runs the phone," Memorandum of Points and Authorities in Support of Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search, 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 35KGD203, No. ED 15-0451M (Feb. 16, 2016), Dkt. 18 at 11 (the "Ex Parte App."), is insufficient to establish the connection mandated by *New York* Telephone Co. The All Writs Act does not allow the government to compel a manufacturer's assistance merely because it has placed a good into the stream of commerce. Apple is no more connected to this phone than General Motors is to a company car used by a fraudster on his daily commute. Moreover, that Apple's software is "licensed, not sold," Ex Parte App. at 5, is "a total red herring," as Judge Orenstein already concluded, Hanna Decl. Ex. DD at 42:4–10 [In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, E.D.N.Y No. 15 MC 1902, Dkt. 19 ("October 26, 2015 Transcript")]. A licensing agreement no more connects Apple to the underlying events than a sale. The license does not permit Apple to invade or control the private data of its customers. It merely

limits customers' use and redistribution of Apple's software. Indeed, the government's position has no limits and, if accepted, would eviscerate the "remoteness" factor entirely, as any company that offers products or services to consumers could be conscripted to assist with an investigation, no matter how attenuated their connection to the criminal activity. This is not, and never has been, the law.

b. The Order Requested By The Government Would Impose An Unprecedented And Oppressive Burden On Apple And Citizens Who Use The iPhone.

An order pursuant to the All Writs Act "must not [1] adversely affect the basic interests of the third party or [2] impose an undue burden." *Hall*, 583 F. Supp. at 719. The Order violates both requirements by conscripting Apple to develop software that does not exist and that Apple has a compelling interest in not creating. The government's request violates the first requirement—that the Act "must not adversely affect the basic interests of the third party"—because Apple has a strong interest in safeguarding its data protection systems that ensure the security of hundreds of millions of customers who depend on and store their most confidential data on their iPhones. An order compelling Apple to create software that defeats those safeguards undeniably threatens those systems and adversely affects Apple's interests and those of iPhone users around the globe. *See id*.

The government's request violates the second requirement—that the Act "must not . . . impose an undue burden"—because the government's unprecedented demand forces Apple to develop new software that destroys the security features that Apple has spent years building. As discussed *supra* in section II.E, no operating system currently exists that can accomplish what the government wants, and any effort to create one would require that Apple write new code, not just disable existing functionality. Neuenschwander Decl. ¶¶ 23-25. Experienced Apple engineers would have to design, create, test, and validate the compromised operating system, using a hyper-secure isolation room within which to do it, and then deploy and supervise its operation by the FBI to brute force crack the phone's passcode. *Id.* ¶¶ 21-43; Olle Decl. ¶ 14. The

system itself would have to be tested on multiple devices to ensure that the operating system works and does not alter any data on the device. Neuenschwander Decl. ¶¶ 30-31. All aspects of the development and testing processes would need to be logged and recorded in case Apple's methodology is ever questioned. *Id.* ¶¶ 28, 33.

Moreover, the government's flawed suggestion to delete the program and erase every trace of the activity would not lessen the burden, it would actually increase it since there are hundreds of demands to create and utilize the software waiting in the wings. *Id.* ¶¶ 38-45. If Apple creates new software to open a back door, other federal and state prosecutors—and other governments and agencies—will repeatedly seek orders compelling Apple to use the software to open the back door for tens of thousands of iPhones. Indeed, Manhattan District Attorney Cyrus Vance, Jr., has made clear that the federal and state governments want access to *every* phone in a criminal investigation.²⁴ *See* Hanna Decl., Ex. Z [(Cyrus R. Vance, Jr., *No Smartphone Lies Beyond the Reach of a Judicial Search Warrant*, N.Y. Times (Feb. 18, 2016)]; Hanna Decl. ¶ 5 at 18:28 [Charlie Rose, Television Interview of Cyrus Vance (Feb. 18, 2016)] (Vance stating "absolutely" that he "want[s] access to all those phones that [he thinks] are crucial in a criminal proceeding"). This enormously intrusive burden—building everything up and tearing it down for each demand by law enforcement—lacks any support in the cases relied on by the government, nor do such cases exist.

Use of the software in criminal prosecutions only exacerbates the risk of disclosure, given that criminal defendants will likely challenge its reliability. *See* Fed. R. Evid. 702 (listing requirements of expert testimony, including that "testimony [be] the product of reliable principles and methods" and "the expert has reliably applied the principles and methods to the facts of the case," all of which a defendant is entitled to challenge); *see also United States v. Budziak*, 697 F.3d 1105, 1111–13 (9th Cir. 2012) (vacating order denying discovery of FBI software); *State v. Underdahl*, 767 N.W.2d 677, 684–86 (Minn. 2009) (upholding order compelling discovery of breathalyzer source code). The government's suggestion that Apple can destroy the software has clearly not been thought through, given that it would jeopardize criminal cases. *See United States v. Cooper*, 983 F.2d 928, 931–32 (9th Cir. 1993) (government's bad-faith failure to preserve laboratory equipment seized from defendants violated due process, and appropriate remedy was dismissal of indictment, rather than suppression of evidence).

The alternative—keeping and maintaining the compromised operating system and everything related to it—imposes a different but no less significant burden, i.e., forcing Apple to take on the task of unfailingly securing against disclosure or misappropriation the development and testing environments, equipment, codebase, documentation, and any other materials relating to the compromised operating system. Id. \P 47. Given the millions of iPhones in use and the value of the data on them, criminals, terrorists, and hackers will no doubt view the code as a major prize and can be expected to go to considerable lengths to steal it, risking the security, safety, and privacy of customers whose lives are chronicled on their phones. Indeed, as the Supreme Court has recognized, "[t]he term 'cell phone' is itself misleading shorthand; . . . these devices are in fact minicomputers" that "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." Riley v. California, 134 S. Ct. 2473, 2488–89 (2014) (observing that equating the "data stored on a cell phone" to "physical items" "is like saying a ride on horseback is materially indistinguishable from a flight to the moon"). By forcing Apple to write code to compromise its encryption defenses, the Order would impose substantial burdens not just on Apple, but on the public at large. And in the meantime, nimble and technologically savvy criminals will continue to use other encryption technologies, while the law-abiding public endures these threats to their security and personal liberties—an especially perverse form of unilateral disarmament in the war on terror and crime. See n.4 supra (describing ISIS's shift to more secure communication methods).

In addition, compelling Apple to create software in this case will set a dangerous precedent for conscripting Apple and other technology companies to develop technology to do the government's bidding in untold future criminal investigations. If the government can invoke the All Writs Act to compel Apple to create a special operating system that undermines important security measures on the iPhone, it could argue in future cases that the courts should compel Apple to create a version to track

24

25

26

27

the location of suspects, or secretly use the iPhone's microphone and camera to record sound and video. And if it succeeds here against Apple, there is no reason why the government could not deploy its new authority to compel other innocent and unrelated third-parties to do its bidding in the name of law enforcement. For example, under the same legal theories advocated by the government here, the government could argue that it should be permitted to force citizens to do all manner of things "necessary" to assist it in enforcing the laws, like compelling a pharmaceutical company against its will to produce drugs needed to carry out a lethal injection in furtherance of a lawfully issued death warrant,²⁵ or requiring a journalist to plant a false story in order to help lure out a fugitive, or forcing a software company to insert malicious code in its autoupdate process that makes it easier for the government to conduct court-ordered surveillance. Indeed, under the government's formulation, any party whose assistance is deemed "necessary" by the government falls within the ambit of the All Writs Act and can be compelled to do anything the government needs to effectuate a lawful court order. While these sweeping powers might be nice to have from the government's perspective, they simply are not authorized by law and would violate the Constitution.

Moreover, responding to these demands would effectively require Apple to create full-time positions in a new "hacking" department to service government requests and to develop new versions of the back door software every time iOS changes, and it would require Apple engineers to testify about this back door as government witnesses at trial. *See, e.g., United States v. Cameron*, 699 F.3d 621, 643–44 (1st Cir. 2012) (holding that reports generated by an Internet provider were testimonial, and thus could not be admitted without "giving [defendant] the opportunity to cross-examine the [provider's] employees who prepared the [] [r]eports"). Nothing in federal law allows the courts, at the request of prosecutors, to

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

Magistrate Judge Orenstein posed this same hypothetical to the government, and the government had no answer. Hanna Decl. Ex. DD at 43–47 [October 26, 2015 Transcript].

coercively deputize Apple and other companies to serve as a permanent arm of the

government's forensics lab. Indeed, the government fails to cite any case—because

none exists—to support its incorrect contention that courts have invoked the All Writs Act to conscript a company like Apple to "to write some amount of code in order to gather information in response to subpoenas or other process." Ex Parte App. at 15.

The burden imposed on Apple is thus in sharp contrast to *New York Telephone*Co., where the public utility was compelled to provide "meager assistance" in setting up a pen register—a step which "required minimal effort on the part of the [c]ompany

up a pen register—a step which "required minimal effort on the part of the [c]ompany and no disruption to its operations." 434 U.S. at 174–75 (noting that the company routinely employed pen registers without court order for purposes of checking billing

operations and detecting fraud); see also Mountain Bell, 616 F.2d at 1132 (order

compelling the phone company to use a tracing technique akin to a pen register did not impose a substantial burden because it "was extremely narrow in scope," and

"prohibit[ed] any tracing technique which required active monitoring by company personnel"). The very limited orders in those cases thus "should not be read to authorize the wholesale imposition upon private, third parties of duties pursuant to search warrants." *Id*.

The other cases the government relies on involve similarly inconsequential burdens where third parties were asked to turn over records that were already in their possession or readily accessible, *Videotapes*, 2003 WL 22053105, at *3 (directing apartment complex owner to share surveillance footage "maintained in the ordinary course of business"); *Hall*, 583 F. Supp. at 722 (directing bank to produce credit card records), or where the third party provided minimal assistance to effect a lawful wiretap, *In re Application of U.S. of Am. for an Order Directing a Provider of Commc'n Servs. to Provide Tech. Assistance to Agents of the U.S. Drug Enf't Admin.*, 2015 WL 5233551, at *5 (D.P.R. Aug. 27, 2015). But unlike those cases, where the government directed a third party to provide something that already existed or sought assistance with a minimal and routine service, here the government wants to compel

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Apple to deploy a team of engineers to write and test software code and create a new operating system that undermines the security measures it has worked so hard to establish—and then to potentially do that over and over again as other federal, state, local and foreign prosecutors make demands for the same thing.

The government's reliance on two phone "unlocking" cases is similarly misplaced. Ex Parte App. at 9 (citing *United States v. Navarro*, No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013), ECF No. 39; In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014) ("Order Requiring [XXX]"). As an initial matter, the *Navarro* order is a minute order that does not contain any analysis of the All Writs Act, and it is unclear whether its limitations were ever raised or considered. The Navarro order is also distinguishable because it involved the government's request to unlock an iPhone on an older operating system that did not require the creation of any new software. Order Requiring [XXX], which was also issued without the benefit of adversarial briefing, is equally unavailing. 2014 WL 5510865, at *3 (granting ex parte application to compel a third party to bypass a lock screen on a phone to effectuate a search warrant). Although the court purported to apply New York Telephone Co., it did not analyze all of the factors set forth in that case, such as whether the All Writs Act could be used to compel third parties to hack into phones, whether the cellphone company was "too far removed" from the matter, or whether hacking into the phone adversely affected the company's interests. Rather, the court simply concluded the technical service sought was not "burdensome," akin to "punching a few buttons" or installing a pen register. 2014 WL 5510865, at *2 (internal quotation marks omitted). As Apple has explained, the technical assistance sought here requires vastly more than simply pressing a "few buttons."

The government has every right to reasonably involve the public in the law enforcement process. Indeed, each year Apple complies with thousands of lawful requests for data and information by law enforcement, and on many occasions has

extracted data from prior versions of its operating system for the FBI's use. *See* Olle Decl. ¶¶ 15-16. But compelling minimal assistance to surveil or apprehend a criminal (as in most of the cases the government cites), or demanding testimony or production of things that already *exist* (akin to exercising subpoena power), is vastly different, and significantly less intrusive, than conscripting a private company to create something *entirely new* and dangerous. There is simply no parallel or precedent for it.

c. The Government Has Not Demonstrated Apple's Assistance Was Necessary To Effectuating The Warrant.

A third party cannot be compelled to assist the government unless the government is authorized to act *and* the third party's participation is imperative. The order in *New York Telephone Co.* satisfied that requirement because the court had authorized surveillance, and "there [was] no conceivable way" to accomplish that surveillance without the company's assistance. 434 U.S. at 175 (noting that FBI had conducted "an exhaustive search" for a way to install a pen register in an undetectable location). The order compelling the phone company's assistance was therefore necessary "to prevent nullification of the court's warrant" and "to put an end to this venture." *Id.* at 174, 175 & n.23; *see also Mountain Bell*, 616 F.2d at 1129 (holding that an order compelling a third party to assist with tracing was necessary to carry out a wiretap and halt ongoing criminal activity); *Mich. Bell Telephone Co. v. United States*, 565 F.2d 385, 389 (6th Cir. 1977) (concluding that telephone company was "the only entity that c[ould] effectuate the order of the district court to prevent company-owned facilities from being used in violation of both state and federal laws").

Here, by contrast, the government has failed to demonstrate that the requested order was absolutely necessary to effectuate the search warrant, including that it exhausted all other avenues for recovering information. Indeed, the FBI foreclosed one such avenue when, without consulting Apple or reviewing its public guidance regarding iOS, the government changed the iCloud password associated with an attacker's account, thereby preventing the phone from initiating an automatic iCloud

back-up. *See supra* II.C. Moreover, the government 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. *See* Hanna Decl. Ex. DD at 34–36 [October 26, 2015 Transcript] (Judge Orenstein asking the government "to make a representation for purposes of the All Writs Act" as to whether the "entire Government," including the "intelligence community," did or did not have the capability to decrypt an iPhone, and the government responding that "federal prosecutors don't have an obligation to consult the intelligence community in order to investigate crime"). As such, the government has not demonstrated that "there is no conceivable way" to extract data from the phone. *New York Tel. Co.*, 434 U.S. at 174.

3. Other Cases The Government Cites Do Not Support The Type Of Compelled Action Sought Here.

The government does not cite a single case remotely approximating the demand it makes here; indeed, its cases only confirm the wild overreach of the Order.

The government relies, for example, on cases compelling *a criminal defendant* to take certain actions—specifically, *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012) and *United States v. Catoggio*, 698 F.3d 64 (2d Cir. 2012) (per curiam)—but those cases say nothing about the propriety of compelling an innocent third party to do so. In *Fricosu* the government moved to require the defendant to produce the "unencrypted contents" of her laptop computer. 841 F. Supp. 2d at 1235. This order placed no undue burden on the defendant because she could access the encrypted contents on her computer, and the court preserved her Fifth Amendment rights by not compelling the password itself, which was testimonial in nature. *See id.* at 1236–38. By contrast, the government's request here creates an unprecedented burden on Apple and violates Apple's First Amendment rights against compelled speech, as discussed below. And unlike the compelled creation of a compromised operating system for iOS devices, the order in *Fricosu* merely required the defendant

3

567

8910

12 13

11

15 16

14

17 18

19

2021

22

24

23

25

2627

28

to hand over her own personal files, and thus posed no risk to third parties' privacy or security interests.

The government's reliance on *Catoggio*, which involved the seizure of defendant's property, is also inapt. Though the district court had not invoked the All Writs Act, the appellate court cited the Act in affirming the district court's order retaining a convicted defendant's property in anticipation of a restitution order. 698 F.3d at 68–69. But whereas courts have uniformly held that the Act enables a court to restrain a convicted defendant's property pending a restitution order, *id.* at 67, no court has ever held that the All Writs Act permits the government to conscript a private company to build software for it.

Finally, the government relies on the Ninth Circuit's decision in *Plum Creek* but that case only serves to illustrate the government's vast overreach under the All Writs Act. There, the Ninth Circuit affirmed the district court's order declining OSHA's request to compel an employer to rescind a company policy forbidding employees from wearing OSHA air-quality and noise-level testing devices, so that OSHA could more efficiently investigate the company's premises. 608 F.2d at 1289– 90. The court reasoned that a government agency's interest in conducting an efficient investigation is not grounds for issuing a writ requiring a company to comply with the government's demands. Id. at 1290. This was particularly true where OSHA "c[ould] not guarantee that these devices would [not] cause" industry accidents, and the company bore the costs of those accidents. *Id.* at 1289 & n.4 (internal quotation marks omitted). Even though the investigation would take five times as long to complete without the use of the equipment OSHA sought to compel, the court could not compel their use absent a law requiring it. *Id.* at 1289 & n.6. The court held that the All Writs Act "does not give the district court a roving commission to order a party subject to an investigation to accept additional risks at the bidding of OSHA inspectors." *Id.* at 1289. Plum Creek thus provides no support for the government's attempt to compel Apple to create new software "when Congress has failed to impose" such a duty on

Apple. *Id.* at 1290. Forcing Apple to write software that would create a back door to millions of iOS devices would not only "usurp the legislative function," *id.*, but also unconstitutionally compel speech and expose Apple iPhone users to exceptional security and privacy risks.

B. The Order Would Violate The First Amendment And The Fifth Amendment's Due Process Clause.

1. The First Amendment Prohibits The Government From Compelling Apple To Create Code.

The government asks this Court to command Apple to write software that will neutralize safety features that Apple has built into the iPhone in response to consumer privacy concerns. Order ¶ 2. The code must contain a unique identifier "so that [it] would only load and execute on the SUBJECT DEVICE," and it must be "'signed' cryptographically by Apple using its own proprietary encryption methods." Ex Parte App. at 5, 7. This amounts to compelled speech and viewpoint discrimination in violation of the First Amendment.

Under well-settled law, computer code is treated as speech within the meaning of the First Amendment. *See, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1099–1100 (N.D. Cal. 2004); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002); *Bernstein v. Dep't of State*, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).

The Supreme Court has made clear that where, as here, the government seeks to *compel* speech, such action triggers First Amendment protections. As the Court observed in *Riley v. Nat'l Fed. of the Blind of N.C., Inc.*, 487 U.S. 781,796 (1988), while "[t]here is certainly some difference between compelled speech and compelled silence, . . . in the context of protected speech, the difference is without constitutional significance." Compelled speech is a content-based restriction subject to exacting scrutiny, *id.* at 795, 797–98, and so may only be upheld if it is narrowly tailored to

obtain a compelling state interest, *see Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 662 (1994).

The government cannot meet this standard here. Apple does not question the government's legitimate and worthy interest in investigating and prosecuting terrorists, but here the government has produced nothing more than speculation that this iPhone might contain potentially relevant information. Hanna Decl. Ex. H [Comey, *Follow This Lead*] ("Maybe the phone holds the clue to finding more terrorists. Maybe it doesn't."). It is well known that terrorists and other criminals use highly sophisticated encryption techniques and readily available software applications, making it likely that any information on the phone lies behind several other layers of non-Apple encryption. *See* Hanna Decl. Ex. E [Coker, *Tech Savvy*] (noting that the Islamic State has issued to its members a ranking of the 33 most secure communications applications, and "has urged its followers to make use of [one app's] capability to host encrypted group chats").

Even more problematically, the Court's Order discriminates on the basis of Apple's viewpoint. When Apple designed iOS 8, it wrote code that announced the value it placed on data security and the privacy of citizens by omitting a back door that bad actors might exploit. *See, e.g.*, Hanna Decl. Ex. AA [Apple Inc., *Privacy, Government Information Requests*]. The government disagrees with this position and asks this Court to compel Apple to write new software that advances its contrary views. This is, in every sense of the term, viewpoint discrimination that violates the

If the government did have any leads on additional suspects, it is inconceivable that it would have filed pleadings on the public record, blogged, and issued press releases discussing the details of the situation, thereby thwarting its own efforts to apprehend the criminals. See Douglas Oil Co. of Cal. v. Petrol Stops Nw., 441 U.S. 211, 218-19 (1979) ("We consistently have recognized that the proper functioning of our grand jury system depends upon the secrecy of grand jury proceedings. . . . [I]f preindictment proceedings were made public, many prospective witnesses would be hesitant to come forward voluntarily, knowing that those against whom they testify would be aware of that testimony. . . . There also would be the risk that those about to be indicted would flee, or would try to influence individual grand jurors to vote against indictment.").

First Amendment. See Members of City Council v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984).

Finally, the FBI itself foreclosed what would have likely been a promising and vastly narrower alternative to this unprecedented order: backing up the iPhone to iCloud. Apple has extensively cooperated and assisted law enforcement officials in the San Bernardino investigation, but the FBI inadvertently foreclosed a ready avenue by changing the passcode, which precluded the iCloud back-up option.²⁷

To avoid the serious First Amendment concerns that the government's request to compel speech presents, this Court should vacate the Order.

2. The Fifth Amendment's Due Process Clause Prohibits The Government From Compelling Apple To Create The Request Code.

In addition to violating the First Amendment, the government's requested order, by conscripting a private party with an extraordinarily attenuated connection to the crime to do the government's bidding in a way that is statutorily unauthorized, highly burdensome, and contrary to the party's core principles, violates Apple's substantive due process right to be free from "arbitrary deprivation of [its] liberty by government." *Costanich v. Dep't of Soc. & Health Servs.*, 627 F.3d 1101, 1110 (9th Cir. 2010) (citation omitted); *see also, e.g., Cnty. of Sacramento v. Lewis*, 523 U.S. 833, 845-46 (1998) ("We have emphasized time and again that '[t]he touchstone of due process is protection of the individual against arbitrary action of government,' . . . [including] the exercise of power without any reasonable justification in the service of a legitimate governmental objective." (citations omitted)); *cf. id.* at 850 ("Rules of due process are not . . . subject to mechanical application in unfamiliar territory.").

²⁷ Hanna Decl. Ex. BB [John Paczkowski and Chris Geidner, *FBI Admits It Urged Change Of Apple ID Password For Terrorist's iPhone*, BuzzFeed News (updated Feb. 21, 2016 2:01 AM)]; Hanna Decl. Ex. CC [Ellen Nakashima and Mark Berman, *FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup*, Wash. Post (Feb. 20, 2016)].

IV. CONCLUSION

Apple has great respect for the professionals at the Department of Justice and FBI, and it believes their intentions are good. Moreover, Apple has profound sympathy for the innocent victims of the attack and their families. However, while the government's desire to maximize security is laudable, the decision of how to do so while also protecting other vital interests, such as personal safety and privacy, is for American citizens to make through the democratic process. Indeed, examples abound of society opting *not* to pay the price for increased and more efficient enforcement of criminal laws. For example, society does not tolerate violations of the Fifth Amendment privilege against self-incrimination, even though more criminals would be convicted if the government could compel their confessions. Nor does society tolerate violations of the Fourth Amendment, even though the government could more easily obtain critical evidence if given free rein to conduct warrantless searches and seizures. At every level of our legal system—from the Constitution, ²⁸ to our statutes, ²⁹ common law, 30 rules, 31 and even the Department of Justice's own policies 32—society has acted to preserve certain rights at the expense of burdening law enforcement's interest in investigating crimes and bringing criminals to justice. Society is still debating the important privacy and security issues posed by this case. The government's desire to leave no stone unturned, however well intentioned, does not authorize it to cut off debate and impose its views on society.

23

24

25

26

27

28

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

²¹²²

See, e.g., U.S. Const. amend. IV (limitations on searches and seizures), amend. V (limitations on charging; prohibition on compelling testimony of accused).

See, e.g., 18 U.S.C. § 3282 (prohibition on prosecuting crimes more than five years' old), CALEA (limitations on ability to intercept communications).

³⁰ E.g., attorney-client privilege, spousal privilege, and reporter's privilege, and priest-penitent privilege, all of which limit the government's ability to obtain evidence.

³¹ See, e.g., Fed. R. Evid. 404 (limitations on use of character evidence), 802 (limitations on use of hearsay).

³² See, e.g., U.S. Attorneys' Manual §§ 9-13-200 (limitations on communicating with witnesses represented by counsel), 9-13.400 (limitations on subpoenaing news media), 9-13-410 (limitations on subpoenaing attorneys), 9-13-420 (limitations on searches of attorneys' offices).

	I		
1	Dated: February 25, 2016		Respectfully submitted,
2			GIBSON, DUNN & CRUTCHER LLP
3		By:	/s/ Theodore J. Boutrous Jr.
4			Theodore J. Boutrous, Jr.
5			Theodore J. Boutrous, Jr. Nicola T. Hanna
6			Eric D. Vandevelde
7			Gibson, Dunn & Crutcher LLP 333 South Grand Avenue
8			Los Angeles, CA 90071-3197 Telephone: 213.229.7000 Facsimile: 213.229.7520
9			Facsimile: 213.229.7520
10			Theodore B. Olson
11			Gibson, Dunn & Crutcher LLP 1050 Connecticut Avenue, N.W.
12			Washington, DC 20036-5306 Telephone: 202.955.8500 Facsimile: 202.467.0539
13			Facsimile: 202.467.0539
14			Marc J. Zwillinger *
15			Jeffrey G. Landis * ZwillGen PLLC
16			1900 M Street N.W., Suite 250 Washington, D.C. 20036
17			Telephone: 202.706.5202 Facsimile: 202.706.5298
18			*Pro Hac Vice Admission Pending
19			Attorneys for Apple Inc.
20			
21			
22			
23			
24			
25			
26			
27			
	1		

1	THEODORE J. BOUTROUS JR., SBN 13	32099					
2	tboutrous@gibsondunn.com NICOLA T. HANNA, SBN 130694						
3	nhanna@gibsondunn.com ERIC D. VANDEVELDE, SBN 240699						
	evandevelde@gibsondunn.com						
4	GIBSON, DUNN & CRUTCHER LLP 333 South Grand Avenue						
5	Los Angeles, CA 90071-3197 Telephone: 213.229.7000 Facsimile: 213.229.7520						
6	Facsimile: 213.229.7520						
7	THEODORE B. OLSON, SBN 38137 tolson@gibsondunn.com						
8	GIBSON, DUNN & CRUTCHER LLP						
9	1050 Connecticut Avenue, N.W. Washington, DC 20036-5306						
10	Washington, DC 20036-5306 Telephone: 202.955.8500 Facsimile: 202.467.0539						
11	MARC J. ZWILLINGER*						
12	marc@zwillgen.com JEFFREY G. LANDIS*						
13	jeff@zwillgen.com ZWILLGEN PLLC						
14	1900 M Street N.W., Suite 250 Washington, D.C. 20036						
15	Washington, D.C. 20036 Telephone: 202.706.5202 Facsimile: 202.706.5298 *Pro Hac Vice Admission Pending						
16	Attorneys for Apple Inc.						
17	UNITED STATES DISTRICT COURT						
18	CENTRAL DISTRICT OF CALIFORNIA						
19	EASTERN DIVISION						
20	IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED	ED No. CM 16-10 (SP)·					
21	DURING THE EXECUTION OF A	DECLARATION OF NICOLA T. HANNA IN SUPPORT OF APPLE					
22	SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA	INC'S MOTION TO VACATE ORDER					
23	LICENSE PLÁTE 35KGD203	COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH, AND					
24		OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE					
25		Hearing:					
26	·	Date: March 22, 2016 Time: 1:00 p.m.					
27		Place: Courtroom 3 or 4					
28		Judge: Hon. Sheri Pym					

DECLARATION OF NICOLA T. HANNA

- 24

I, Nicola T. Hanna, 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 am one of the attorneys responsible for representing Apple Inc. in the above-captioned matter. I submit this declaration in support of Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance. 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 the Washington Post article, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, by Ellen Nakashima, originally published on July 9, 2015, available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. The article was printed on February 23, 2016.
- 3. Attached hereto as **Exhibit B** is a true and correct copy of the letter to the court filed by Apple Inc. on February 17, 2016 in *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, E.D.N.Y No. 15-MC-1902, Dkt. 27.
- 4. Attached hereto as **Exhibit C** is a true and correct copy of the Newsweek article, *The Murder Victim Whose Phone Couldn't Be Cracked and Other Apple Encryption Stories*, by Seung Lee, originally published on February 19, 2016, available at http://www.newsweek.com/apple-encryption-crime-428565. The article was printed on February 23, 2016.
- 5. The Charlie Rose television interview of Cyrus Vance aired on February 18, 2016, and is available at http://www.charlierose.com/watch/60689812.
- 6. Attached hereto as **Exhibit D** is a true and correct copy of the Apple Inc. document, *A Message to Our Customers*, originally published on February 16, 2016,

12

10

13 14

15

16 17

18

19

20 21

22

23 24

25

26

27

28

available at http://www.apple.com/customer-letter/. The document was printed on February 23, 2016.

- Attached hereto as Exhibit E is a true and correct copy of the Wall Street 7. Journal article, The Attacks in Paris: Islamic State Teaches Tech Savvy, by Margaret Coker et al., originally published on November 17, 2015, available at http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824. The article was printed on February 20, 2016.
- Attached hereto as Exhibit F is a true and correct copy of the Federal 8. Bureau of Investigation document, Going Dark Issue, available at https://www.fbi.gov/about-us/otd/going-dark-issue. The document was printed on February 23, 2016.
- Attached hereto as **Exhibit G** is a true and correct copy of the Lawfare 9. blog post, Encryption, Public Safety, and "Going Dark," by James Comey, originally posted on July 6, 2015 at 10:38 AM, available at https://www.lawfareblog.com/ encryption-public-safety-and-going-dark. The blog post was printed on February 23, 2016.
- 10. Attached hereto as **Exhibit H** is a true and correct copy of the Lawfare blog post, We Could Not Look the Survivors in the Eye if We Did Not Follow This Lead, by James Comey, originally posted on February 21, 2016 at 9:03 PM, available at https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-notfollow-lead. The blog post was printed on February 23, 2016.
- Attached hereto as **Exhibit I** is a true and correct copy of the Wall Street 11. Journal article, Gen. Michael Hayden Gives an Update on the Cyberwar, an interview with John Bussey, originally published on February 9, 2016, available at http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153. The article was printed on February 23, 2016.
- 12. Attached hereto as **Exhibit J** is a true and correct copy of the Wall Street Journal article, How the U.S. Fights Encryption—and Also Helps Develop It, by

Damian Paletta, originally published on February 22, 2016, available at http://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096. The article was printed on February 23, 2016.

- 13. Attached hereto as **Exhibit K** 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. The document was printed on February 23, 2016.
- 14. Attached hereto as **Exhibit L** is a true and correct copy of the Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption*, by James Comey, originally published on July 8, 2015, available at https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy. The document was printed on February 23, 2016.
- 15. Attached hereto as **Exhibit M** is a true and correct copy of the article *The National-Security Needs for Ubiquitous Encryption*, by Susan Landau, Appendix A to the Berkman Center for Internet & Society at Harvard University article *Don't Panic: Making Progress on the 'Going Dark' Debate*, originally published on February 1, 2016, available at https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. The article was printed on February 24, 2016.
- 16. Attached hereto as **Exhibit N** is a true and correct copy of the written evidence (IPB0093) submitted by Apple Inc. and Apple Distribution International to the Parliament of the United Kingdom on December 21, 2015, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/d http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/d http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/d http://data.parliament.uk/writtenevidence/committee/draft-investigatory-powers-bill/written/26341.pdf. The document was printed on February 23, 2016.

- 17. Attached hereto as **Exhibit O** is a true and correct copy of the Washington Post article, *Why The Fear Of Ubiquitous Data Encryption Is Overblown*, by Mike McConnell et al., 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. The article was printed on February 23, 2016.
- 18. Attached hereto as **Exhibit P** 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. The article was printed on February 23, 2016.
- 19. Attached hereto as **Exhibit Q** is a true and correct copy of the New America's Open Technology Institute document, *Joint Letter to President Barack Obama*, originally published on May 19, 2015, available at https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf. The document was printed on February 23, 2016.
- 20. Attached hereto as **Exhibit R** is a true and correct copy of the House Committee on the Judiciary press release, *Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption*, by The House Committee on the Judiciary, Democrats, originally published on February 18, 2016, available at http://democrats.judiciary-house-gov/press-release/senior-house-judiciary-committee-democrats-express-concern-over-government-attempts. The press release was printed on February 23, 2016.
- 21. Attached hereto as **Exhibit S** is a true and correct copy of the *Statement Before the Senate Committee on Homeland Security and Governmental Affairs*, by James Comey, originally published on October 8, 2015, available at

https://www.fbi.gov/news/testimony/threats-to-the-homeland. The document was printed on February 23, 2016.

- 22. Attached hereto as **Exhibit T** is a true and correct copy of the document *Director Discusses Encryption, Patriot Act Provisions*, by James Comey, originally published on May 20, 2015, available at https://www.fbi.gov/news/news_blog/director-discusses-encryption-patriot-act-provisions. The document was printed on February 23, 2016.
- 23. Attached hereto as **Exhibit U** is a true and correct copy of the transcript of the radio Interview with Cyrus Vance, *It's Not Just the iPhone Law Enforcement Wants to Unlock*, by NPR Weekend Edition, originally aired on February 21, 2016, available at http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock. The transcript was printed on February 23, 2016.
- 24. Attached hereto as **Exhibit V** is a true and correct copy of the document, Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference, published by the White House, Office of the Press Secretary, on January 16, 2015, available at https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-. The document was printed on February 23, 2016.
- 25. Attached hereto as **Exhibit W** is a true and correct copy of the ReCode. com article, *White House. Red Chair. Obama Meets Swisher*, by Kara Swisher, originally published on February 15, 2015, available at http://recode.net/2015/02/15/ white-house-red-chair-obama-meets-swisher/. The article was printed on February 23, 2016.
- 26. Attached hereto as **Exhibit X** is a true and correct copy of the Apple Inc. document, *iCloud: Back up your iOS device to iCloud*, last modified February 11, 2016, available at https://support.apple.com/kb/PH12520. The document was printed on February 23, 2016.

- 27. Attached hereto as **Exhibit Y** is a true and correct copy of the *Statement to Address Misleading Reports that the County of San Bernardino Reset Terror Suspect's iPhone Without Consent of the FBI*, issued by the Federal Bureau of Investigation to Ars Technhica on February 21, 2016, available at https://assets.documentcloud.org/documents/2716811/Statement-from-the-FBI-Feb-20-2016.pdf. The statement was printed on February 23, 2016.
- 28. Attached hereto as **Exhibit Z** is a true and correct copy of the New York Times article, *No Smartphone Lies Beyond the Reach of a Judicial Search Warrant*, by Cyrus R. Vance, Jr., originally published on February 18, 2016, available at http://www.nytimes.com/roomfordebate/2016/02/18/crimes-iphones-and-encryption/no-smartphone-lies-beyond-the-reach-of-a-judicial-search-warrant. The article was printed on February 23, 2016.
- 29. Attached hereto as **Exhibit AA** is a true and correct copy of the Apple Inc. document, *Privacy, Government Information Requests*, available at http://www.apple.com/privacy/government-information-requests/. The document was printed on February 23, 2016.
- 30. Attached hereto as **Exhibit BB** is a true and correct copy of the BuzzFeed News article, *FBI Admits It Urged Change Of Apple ID Password For Terrorist's iPhone*, by John Paczkowski and Chris Geidner, last updated on February 20, 2016 available at http://www.buzzfeed.com/johnpaczkowski/apple-terrorists-appleid-passcode-changed-in-government-cust#.pwX6NKVvW. The article was printed on February 23, 2016.
- 31. Attached hereto as **Exhibit CC** is a true and correct copy of the Washington Post article, *FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup*, by Ellen Nakashima and Mark Berman, originally published on February 20, 2016, available at https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-

backup/2016/02/ 20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html. The article was printed on February 23, 2016.

32. Attached hereto as **Exhibit DD** is a true and correct copy of the transcript of the hearing held before the Honorable James Orenstein on October 26, 2015 in *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, E.D.N.Y No. 15-MC-1902, Dkt. 19.

I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct. Executed at Irvine, California on February 25, 2016.

Nicola T. Hanna /2

Exhibit A

The Washington Post

Federal Insider

Hacks of OPM databases compromised 22.1 million people, federal authorities say

By Ellen Nakashima July 9, 2015

Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends, U.S. officials said Thursday.

The total vastly exceeds all previous estimates, and marks the most detailed accounting by the Office of Personnel Management of how many people were affected by cyber intrusions that U.S. officials have privately said were traced to the Chinese government.

[What you need to know about the hack of government background investigations]

Campaign 2016 Email Updates

Get the best analysis of the presidential race.

Sign up

But even beyond the rising number of apparent victims, U.S. officials said the breaches rank among the most potentially damaging cyber heists in U.S. government history because of the abundant detail in the files. Officials said hackers accessed not only personnel records of current and former employees but also extensive information about friends, relatives and others listed as references in applications for security clearances for some of the most sensitive jobs in government.

[Chinese hack of personnel files includes security clearance database]

"It is a very big deal from a national security perspective and from a counterintelligence perspective," FBI Director James B. Comey said at a meeting with reporters Thursday at the FBI headquarters. "It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government."

Hacks of OPM databases compromised 22.1 million people, federal authorities say - The ... Page 2 of 6 Case 5:16-cm-00010-SP Document 16-2 Filed 02/25/16 Page 3 of 7 Page ID #:138

Other U.S. officials said that a foreign intelligence service could use the information to identify U.S. intelligence operatives, and that China is suspected of stealing large amounts of data on Americans as part of a "strategic plan" to increase its intelligence collection.

The OPM release came after a months-long effort by the agency to take inventory of the damage, an endeavor that required surveying enormous and often outdated computer systems.

The vast majority of those affected — 21.5 million people — were included in an OPM repository of security clearance files, officials said. At least 4.2 million people were affected by the breach of a separate database containing personnel records including Social Security numbers, job assignments and performance evaluations.

[Graphic: How the federal government processes security clearance applications]

About 3.6 million of those affected were in both systems, an overlap that accounts for the 22.1 million total, officials said.

The hackers' access was so extensive that U.S. officials said they think it is "highly likely" that every file associated with an OPM-managed security clearance application since 2000 was exposed. Background checks before that time were less likely to be affected, officials said.

The CIA, largely appears to have been shielded from damage, especially for employees who have never worked at any other agency, officials said.

[Officials: Hackers had access to security data for a year]

Even so, some U.S. officials have said that a foreign spy service might be able to identify U.S. intelligence operatives by scrutinizing the OPM files. Names that appear on rosters of U.S. embassies but are missing from the OPM records might, through a process of elimination, reveal the identities of CIA operatives serving under diplomatic cover.

"That's not conclusive that the person might be undercover CIA," said one U.S. official, who spoke on the condition of anonymity to discuss the sensitive topic. "But it's certainly worth taking a look at."

Hacks of OPM databases compromised 22.1 million people, federal authorities say - The ... Page 3 of 6 Case 5:16-cm-00010-SP Document 16-2 Filed 02/25/16 Page 4 of 7 Page ID #:139

Of those whose data was in the OPM background-check system, 19.7 million had applied for a security clearance. An additional 1.8 million were spouses, family members and other non-applicants, officials said.

Also exposed were 1.1 million sets of fingerprints, detailed financial and health records, and computer usernames and passwords that applicants used to fill out their security-clearance forms online.

OPM Director Katherine Archuleta indicated during a conference call with reporters that there is no evidence that the breach has been exploited for criminal purposes, saying, "There is no information at this time to suggest any misuse."

[Watchdog: Shutdown of security clearance system "reactive" not "proactive"]

The U.S. government has said it will offer the affected employees at least three years of credit monitoring and other identity-protection services. But OPM faces rising anger among members of federal employee unions who say they have received scant information about the breaches.

Two class-action lawsuits have been filed against the agency and Archuleta.

"Today's new number is staggering," said William R. Dougan, president of the National Federation of Federal Employees. He added that "it is not yet clear how OPM can handle this massive increase, when they were already struggling with the initial 4.2 million. Now, not only do federal employees have to worry about their own personal information being exposed – but they must also worry about their spouse and children having their information compromised."

The White House is said to be weighing how to respond to what is being considered an aggressive act of espionage. U.S. officials said options include covert cyber-measures as well as punitive economic sanctions, although the nation's ability to claim outrage has been undermined by the exposure of its own global spying programs by former intelligence contractor Edward Snowden.

Those responsible for the hack appear to have had access to OPM records for months. U.S. officials said the theft of security-clearance data took place over a six-month stretch that ended in January. The personnel records were stolen from October to April.

The breach of personnel records was discovered in April as a result of new cybersecurity tools OPM had installed, said Andy Ozment, the Department of Homeland Security's assistant secretary for cybersecurity.

Officials said the thieves broke in by using stolen contractor logins and passwords. Although U.S. officials have said the intrusions were traced to the Chinese government, the Obama administration has not formally accused Beijing.

Comey said he thinks the hackers have obtained his "SF 86," referring to Standard Form 86, which all applicants for security clearances must fill out.

"If you have my SF 86, you know every place I've lived since I was 18, contact people at those addresses, neighbors at those addresses, all of my family, every place I've traveled outside the United States," Comey said. "Just imagine if you were a foreign intelligence service and you had that data."

One of the major U.S. concerns is that an adversary could use the data to identify U.S. government employees who might be susceptible to pressure or inducements to engage in espionage.

Thursday's disclosures prompted renewed calls among some on Capitol Hill for the resignation Archuleta and her chief information officer, Donna Seymour.

"Director Archuleta's slow and uneven response has not inspired confidence that she is the right person to manage OPM through this crisis," said Sen. Mark R. Warner (D-Va.), a member of the Senate Intelligence Committee. "It is time for her to step down, and I strongly urge the administration to choose new management with proven abilities to address a crisis of this magnitude with an appropriate sense of urgency and accountability."

Archuleta said that she will not step down, and that she remains "committed to the work that I am doing at OPM."

Agency officials say that it was only because of a strategic plan put in place by Archuleta shortly after she became director in November 2014 that the breaches were discovered.

"There are certainly some people I would like to see given the boot for not paying attention to cybersecurity, but Katherine Archuleta is not one of them," said one administration official, requesting anonymity to discuss personnel issues. "Maybe

Hacks of OPM databases compromised 22.1 million people, federal authorities say - The ... Page 5 of 6 Case 5:16-cm-00010-SP Document 16-2 Filed 02/25/16 Page 6 of 7 Page ID #:141

they didn't move as fast as they should have but they were at least moving in the right direction and were prioritizing it in an agency that didn't think of itself as having a security mission."

It has taken weeks for the agency to come up with the number, in large part because of the difficulty, officials say, of reviewing data contained in numerous computers that make up the background check system. Many of the computers are antiquated. There were many instances of names being duplicated — sometimes because someone was listed as a reference in several background checks as well as having their own clearance.

"The forensics for that ...investigation were extremely complicated," Ozment said.

In weighing how to respond, some U.S. officials caution against taking actions against foreign states when the cyber theft is conducted for traditional spying motives. The United States has not officially named China or the motive, but privately officials say

it appears China was conducting a form of traditional espionage.

"I think we have to be careful about the importance of continuing to draw a line between theft for economic advantage and traditional foreign intelligence activities, which may look untraditional now that they're in the cyber realm," said Rep. Adam Schiff (D-Calif.), a member of the House Intelligence Committee. "We want to draw a bright line" that hacking for economic benefit "is a violation of international norms."

If the United States blurs the line between economic spying and foreign intelligence spying, "we risk undermining the fight against economic theft."

He said rather than "simply place blame on the hackers, we need to acknowledge our own culpability in failing to adequately protect so obvious a target. Plainly, we need to do so much more to safeguard our networks."

The government has already begun taking steps to mitigate the damage in the intelligence and counterintelligence arena, Schiff said. "We're going to be doing that for years, in terms of the whole range of steps that we'll have to take to protect our people and our sources and methods."

He added: "The consequences will be very far-reaching."

Lisa Rein contributed to this story.

Hacks of OPM databases compromised 22.1 million people, federal authorities say - The ... Page 6 of 6 Case 5:16-cm-00010-SP Document 16-2 Filed 02/25/16 Page 7 of 7 Page ID #:142

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

Campaign 2016 X State of the 2016 race

>

Exhibit B



1900 M Street, NW, Ste. 250, Washington, D.C. 20036 marc@zwillgen.com

Marc J. Zwillinger (202) 706-5202 (phone) (202) 706-5298 (fax)

February 17, 2016

VIA ELECTRONIC FILING – UNDER SEAL

The Honorable James Orenstein United States Magistrate Judge United States District Court Eastern District of New York 225 Cadman Plaza East Brooklyn, NY 11201

Re: <u>In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. 15-MC-1902</u>

Dear Judge Orenstein:

I write in response to this Court's February 16, 2016 order (the "Order") requesting that Apple provide certain additional details regarding other requests it has received during the pendency of this matter that are of a similar nature to the one at issue in the instant case.

As recently as yesterday, Apple was served with an order by the United States Attorney's Office for the Central District of California. (See Exhibit A.) The government obtained that order on the basis of an ex parte application pursuant to the All Writs Act (see Exhibit B), regarding which Apple had no prior opportunity to be heard (despite having specifically requested from the government in advance the opportunity to do so). The attached order directs Apple to perform even more burdensome and involved engineering than that sought in the case currently before this Court—i.e., to create and load Apple-signed software onto the subject iPhone device to circumvent the security and anti-tampering features of the device in order to enable the government to hack the passcode to obtain access to the protected data contained therein. (See Exhibit A.) As invited by the California court's order, Apple intends to promptly seek relief. But, as this recent case makes apparent, the issue remains quite pressing.

In addition to the aforementioned order, Apple has received other All Writs Act orders during the pendency of this case, certain details of which are set forth in the table below. In particular, for each such request Apple provides the following categories of information requested in the Order:

(1) the jurisdiction in which the request was made, (2) the type of device at issue in the request, (3) the version of iOS being used on that device, and (4) Apple's response to the request and/or its current status, as applicable.

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)

With respect to the other categories of information sought in the Order (specifically, categories 4-6), Apple responds that following its objection or other response to each request there has not been any <u>final</u> disposition thereof to Apple's knowledge, and Apple has not agreed to perform any services on the devices to which those requests are directed.¹

Sincerely,

/s/ Marc J. Zwillinger

Marc J. Zwillinger

cc: All Counsel of Record (via ECF)

¹ Apple further notes that shortly preceding the pendency of the instant case, it received additional All Writs Act orders—specifically, two from the Southern District of Ohio (both on September 24, 2015) and Northern District of Illinois (on October 6, 2015). Apple objected to each of these orders, and to Apple's knowledge there have been no further developments since such objections were lodged.

Exhibit C



TECH & SCIENCE

THE MURDER VICTIM WHOSE PHONE COULDN'T BE CRACKED AND OTHER APPLE ENCRYPTION STORIES

BY **SEUNG LEE** ON 2/19/16 AT 11:58 AM



After Apple's refusal to comply with a court order to help the FBI access encrypted content on an iPhone owned by one of the San Bernardino shooters, tech companies and presidential candidates have spoken out on the controversy over digital encryption.

MICHAELA REHLE/REUTERS

Subscribe

Sign In

TECH & SCIENCE APPLE U.S. LAW ENFORCEMENT SACRAMENTO

MANHATTAN IPHONE ENCRYPTION

A few months ago, a man was murdered in Sacramento, California, and the police retrieved his iPhone on the spot. In a last-ditch effort to open his locked phone to check any last calls or messages from possible suspects, a police investigator rushed over to the coroner's office with the victim's iPhone, hoping to unlock it using his thumbprint. But the body was too cold for the iPhone to recognize the thumbprint, and the phone has remained locked since.

Another time, also in Sacramento, a murder suspect was arrested with his iPhone after being caught on a surveillance camera at a liquor store. When asked to open his phone to cooperate with the police, the suspect told the police he would "rather go to jail" than give up his pass code. That phone too has remained locked since.

These are two stories Rod Norgaard, assistant chief deputy in the Sacramento County district attorney's office, shared with *Newsweek* as he expressed his frustration over <u>Apple's opposing a court order</u> to unlock San Bernardino shooter Syed Rizwan Farook's iPhone 5C. Apple has steadfastly refused to grant the FBI backdoor access to its encrypted iPhones, saying once there is software to unlock Farook's iPhone it creates "the potential to unlock any iPhone in someone's physical possession."

Try Newsweek for only \$1.25 per week

Norgaard says there are "well over 100" iPhones in Sacramento County stowed away in police departments, and they cannot be opened for police investigations. The two anecdotes above involve unsolved homicides. "Things like these happen routinely with encrypted smartphones," Norgaard says.

Norgaard did not mince words about Apple CEO Tim Cook and the company's supporters in their resistance to the FBI and the court. He called Cook "Chicken Little" for calling the order a "threat to data security" and compared his supporters to the occupiers of Oregon's Malheur National Wildlife Refuge.

Subscribe

"I see those people in San Francisco as no better than those who occupied federal land in Oregon," Norgaard says. "If you lived in a fortified home and police came with a warrant reviewed by the judge and you still won't open the door, we will call this a standoff."

He also called Apple hypocritical in its new stance on encryption, recalling the pre-iOS 8 days when Apple would hesitantly cooperate with law enforcement in decrypting iPhones. In 2013, <u>CNET reported that Apple had a "waiting list" of police demands</u> for decrypting iPhones.

A couple of years ago, Sacramento investigators drive an hour and a half west to the Bay Area, hand-deliver the seized iPhones to an expert who decrypted the iPhones (he could not remember the expert's identity) and wait six to eight months to receive a broken-in iPhone, according to Norgaard. He says this process has not happened since 2014.

On the opposite side of the country, Manhattan District Attorney Cyrus Vance Jr. expressed the same frustration because his office can't get past Apple's encryption technology, which was strengthened after iOS 8 in 2014. "We now have about 155 to 160 devices that are running on iOS 8 that are blocked and we can't get in them," <u>Vance told NPR on Thursday</u>. Apple says it does not have the technology to crack its own iPhone.

Sign In

From September 2014 to October 2015, 111 search warrants were left incomplete due to law enforcement's inability to decrypt the phone, according to a report from Vance's office. The report also cites a recorded conversation from 2015 between an inmate and a friend talking about how having iOS 8 running on their phones was "another gift from God."

Subscribe

Sign In

Newsweek reached out to 10 district attorney offices across the United States on their experiences dealing with strong encryption technology. Two declined to speak, and six did not respond.

Only Manhattan and Sacramento answered, most likely because both offices have long been critical of the encryption. In the past two months, two state bills, in California and New York, were introduced to ban encrypted smartphones. <u>Both were coordinated</u> with the Manhattan and Sacramento district attorney's offices.

While calling the California assemblyman who introduced the bill "a good friend" for over 20 years, Norgaard concedes that encryption should be dealt with on the federal level. He then expressed outrage that Apple was treating the federal government lightly.

"That a company can overwrite federal law...it's crazy. We don't have a country anymore without rules," he says. "I'm telling ya, if there is a bomb threat in Silicon Valley, they will be unlocking phones left and right."

REQUEST REPRINT OR SUBMIT CORRECTION

Exhibit D

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.

Answers to your questions about privacy and security

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

Answers to your questions about privacy and security

Shop and Learn	Apple Store	For Education	Account	About Apple
Mac	Find a Store	Apple and Education	Manage Your Apple ID	Apple Info
iPad	Genius Bar	Shop for College	Apple Store Account	Job Opportunities
iPhone	Workshops and Learning		iCloud.com	Press Info
Watch	Youth Programs	For Business		Investors
TV	Apple Store App	iPhone in Business	Apple Values	Events
Music	Refurbished	iPad in Business	Environment	Hot News
iTunes	Financing	Mac in Business	Supplier Responsibility	Legal
iPod	Reuse and Recycling	Shop for Your Business	Accessibility	Contact Apple
Accessories	Order Status		Privacy	
Gift Cards	Shopping Help		Inclusion and Diversity	
			Education	

More ways to shop: Visit an Apple Store, call 1-800-MY-APPLE, or find a reseller.

Copyright © 2016 Apple Inc. All rights reserved. Privacy Policy | Terms of Use | Sales and Refunds | Site Map

United States

Exhibit E

The Attacks in Paris: Islamic State Teaches Tech Savvy

The Wall Street Journal

November 17, 2015 Tuesday

Copyright 2015 Factiva ®, from Dow Jones All Rights Reserved



Copyright © 2015, Dow Jones & Company, Inc.

THE WALL STREET JOURNAL.

Section: Pg. A9
Length: 758 words

Byline: By Margaret Coker, Sam Schechner and Alexis Flynn

Body

Terror groups have for years waged a technical battle with Western intelligence services that have sought to constrain them through a web of electronic surveillance.

The Paris attacks, apparently planned under the noses of French and Belgian authorities, raise the possibility that Islamic State adherents have found ways around the dragnet.

French authorities say two of the attackers knew each other in prison, but it isn't clear how the group communicated in plotting and coordinating the Friday attacks.

Low-tech methods exist for communicating off law enforcement's radar including passing written notes or relaying messages through friends or relatives.

But law-enforcement agencies also have long warned that encrypted platforms built for gaming or other commercial purposes to safeguard privacy are being used by would-be terrorists to communicate.

Islamic State, for its part, has built a tech-savvy division of commanders who issue tutorials to sympathizers about the most secure and least expensive ways of communicating.

The bloodshed in Paris will likely exacerbate a tense debate between governments that want inside access to those encrypted tools and tech companies that say are trying to protect customer data and are wary of government overreach.

Mike Morell, the former deputy director of the Central Intelligence Agency, said terrorists' ability to use encrypted communication is a huge problem.

"I think this is going to open an entire new debate about security versus privacy," he told CBS television on Sunday.

For more than a year, governments in Europe have pushed for companies such as Google, Facebook and Twitter to build "back doors" that allow law enforcement access into their encrypted tools.

Tech companies and security experts have resisted that push, which gained steam in Europe following the January attacks in Paris against the satirical magazine Charlie Hebdo.

The Attacks in Paris: Islamic State Teaches Tech Savvy

Security experts say inserting back doors would weaken the encryption and undermine trust in the Internet.

Islamic State is among the most technologically sophisticated extremist groups. Its advice to followers includes an eight-minute video released last year in Arabic that discusses the surveillance capabilities of hostile governments and how phones can be tracked. Bulletins also include advice about brands of electronic equipment that appear vulnerable.

In January, a follower known online as al-Khabir al-Taqni, who identifies himself as a "technical expert," provided would-be fighters with a list of what he determined were the safest encrypted communications systems available.

"Through this, we can break one of the strongest weapons of the Crusader governments in spying on and tracking the mujahedeen and targeting them with aircraft," the author said, referring to the U.S.-led coalition fighting Islamic State.

The missive, authenticated by the SITE Intelligence Group which monitors and tracks radical groups online, ranked 33 applications as unsafe, moderately safe, safe, and safest.

Soon after the list was published, Islamic State started moving official communications from Twitter to Telegram Messenger, which received the second-highest safety rating from the Islamic State tech team.

That included the group's claim of responsibility for the Paris attacks as well as the Oct. 31 Russian airline crash in Egypt.

Islamic State also has urged its followers to make use of the app's capability to host encrypted group chats.

A spokesman for Telegram didn't respond to requests to comment. Pavel Durov, the app's founder who also created the Russian social network VKontakte, criticized recent calls by the Russian government to ban Telegram.

"I propose we ban words," Mr. Durov wrote in a sarcastic VKontake post. "There is information that terrorists use them to communicate."

U.K. prosecutors convicted a British teen this year in part because police had access to his Telegram chats.

The boy, inspired by Islamic State, admitted to communicating with an Australian teenager and encouraging him to attack ceremonies commemorating military veterans.

He was convicted on one terrorism charge. Police and prosecutors have declined to comment about how they accessed those communications.

European law-enforcement officials have also expressed concern about gaming consoles, which also allow players to communicate with each other via the Internet.

In May, an Austrian court convicted a 14-year-old boy of downloading bomb-making instructions onto his PlayStation console, according to local media reports.

License this article from Dow Jones Reprint Service

Notes

PUBLISHER: Dow Jones & Company, Inc.

Classification

Language: ENGLISH

Publication-Type: Newspaper

The Attacks in Paris: Islamic State Teaches Tech Savvy

Journal Code: J

Subject: LAW ENFORCEMENT (90%); TERRORISM (90%); MUSLIMS & ISLAM (89%); RELIGION (89%); TERRORIST ORGANIZATIONS (79%); INTELLIGENCE SERVICES (78%); ESPIONAGE (78%); PRIVACY RIGHTS (78%); WRITERS (75%); CRYPTOLOGY (74%); ghome Law Enforcement; gsci Sciences/Humanities; gspy Espionage; gterr Terrorism; gvio Military Action; gcat Political/General News; gcns National Security; gcrim Crime/Courts; gdef Armed Forces; grisk Risk News; ncat Content Types; nfact Factiva Filters; nfcpex C&E Executive News Filter; PROVIDER TERMS: WSJ CRM DJWI GEN LEN SCN TER

Company: GOOGLE INC (54%); FACEBOOK INC (54%); agdirg Islamic State of Iraq and the Levant

Organization: CENTRAL INTELLIGENCE AGENCY (55%)

Ticker: GOOG (NASDAQ) (54%); FB (NASDAQ) (54%)

Industry: SURVEILLANCE TECHNOLOGY (89%); INTERNET SOCIAL NETWORKING (89%); SOCIAL MEDIA (78%); INTERNET & WWW (78%); WRITERS (75%); CRYPTOLOGY (74%); INFORMATION SECURITY & PRIVACY (69%)

Geographic: PARIS, FRANCE (88%); FRANCE (93%); EUROPE (87%); belg Belgium; eurz Europe; fra France; paris Paris; benluxz Benelux Countries; eecz European Union Countries; ilefra Ile-de-France; medz Mediterranean; weurz Western Europe; PROVIDER TERMS: BEL EC EU EZN FR WEU

IP Codes: IGV NND

Load-Date: November 17, 2015

Exhibit F





Operational Technology

Home • About Us • Operational Technology • Going Dark Issue

Going Dark Issue

Law enforcement at all levels has the legal authority to intercept and access communications and information pursuant to court orders, but it often lacks the technical ability to carry out those orders because of a fundamental shift in communications services and technologies. This scenario is often called the "Going Dark" problem.

Law enforcement faces two distinct Going Dark challenges. The first concerns real-time court-ordered interception of data in motion, such as phone calls, e-mail, text messages, and chat sessions. The second challenge concerns "data at rest"—court-ordered access to data stored on devices, like e-mail, text messages, photos, and videos. Both real-time communications and stored data are increasingly difficult for law enforcement to obtain with a court order or warrant. This is eroding law enforcement's ability to quickly obtain valuable information that may be used to identity and save victims, reveal evidence to convict perpetrators, or exonerate the innocent.

Make no mistake, the FBI supports strong encryption, and we know firsthand the damage that can be caused by vulnerable and insecure systems. As such, the Department of Justice, the FBI, and other law enforcement agencies are on the front lines of the fight against cyber crime. The government uses strong encryption to secure its own electronic information, and it encourages the private sector and members of the public to do the same.

However, the challenges faced by law enforcement to lawfully and quickly obtain valuable information are getting worse. The Communications Assistance for Law Enforcement Act (CALEA) was enacted in 1994 and applies only to traditional telecommunications carriers, providers of interconnected Voice over Internet Protocol (VoIP) services, and providers of broadband access services. Currently thousands of companies provide some form of communication service, and most are not required by CALEA to develop lawful intercept capabilities for law enforcement. As a result, many of today's communication services are developed and deployed without consideration of law enforcement's lawful intercept and evidence collection needs.

Of the Going Dark problem, Director James Comey has said, "Armed with lawful authority, we increasingly find ourselves simply unable to do that which the courts have authorized us to do, and that is to collect information being transmitted by terrorists, by criminals, by pedophiles, by bad people of all sorts." And as for a perceived conflict between keeping people safe and protecting their privacy, "it isn't a question of conflict," according to Comey. "We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve—in every investigation."

To help address the challenges posed by advancing communications services and technologies, the Department of Justice's National Domestic Communications Assistance Center (NDCAC) leverages and shares the law enforcement community's collective technical knowledge, solutions, and resources. NDCAC also works on behalf of federal, state, local, and tribal law enforcement agencies to strengthen law enforcement's relationships with the communications industry.

Additional resources:

- Congressional testimony of Director James Comey
- Congressional testimony of Director James Comey and Deputy Attorney General Sally Quillian Yates
- Acting Deputy Attorney General Sally Q. Yates' speech at the Association of State Criminal Investigative Agencies' Spring Conference
- Congressional testimony of Executive Assistant Director Amy Hess
- Director James Comey's speech at the Brookings Institution
- National Domestic Communications Assistance Center

Operational Technology Links

Operational Technology Home

Inside OTD

- Overview
- Capabilities
- News and Stories

Student Opportunities

- Internships

Other Resources

- RCFL News

Accessibility | eRulemaking | Freedom of Information Act | Legal Notices | Legal Policies and Disclaimers | Links | Privacy Policy | USA.gov | White House FBI.gov is an official site of the U.S. government, U.S. Department of Justice

Close

Exhibit G

MENU LAWFARE Q

ENCRYPTION

Encryption, Public Safety, and "Going Dark"

By James Comey Monday, July 6, 2015, 10:38 AM



David Bruce

I am worried we are talking past each other with respect to "Going Dark," so let me try to frame it in a way that I hope is fair-minded and provides a basis for healthy discussion:

These are things I believe to be true:

1. The logic of encryption will bring us, in the not-todistant future, to a place where devices and data in motion are protected by universal strong encryption. That is, our conversations and our "papers and effects" will be locked

in such a way that permits access only by participants to a conversation or the owner of the device holding the data.

- 2. There are many benefits to this. 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 lock-boxes 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.
- 3. There are many costs to this. Public safety in the United States has relied for a couple centuries on the ability of the government, with predication, to obtain permission from a court to access the "papers and effects" and communications of Americans. The Fourth Amendment reflects a trade-off inherent in ordered liberty: To protect the public, the government sometimes needs to be able to see an individual's stuff, but only under appropriate circumstances and with appropriate oversight.
- 4. These two things are in tension in many contexts. When the government's ability—with appropriate predication and court oversight—to see an individual's stuff goes away, it will affect public safety. That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment. But the tension could as well be illustrated in

criminal investigations all over the country. There is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption.

5. Democracies resolve such tensions through robust debate. I really am not a maniac (or at least my family says so). But my job is to try to keep people safe. In universal strong encryption, I see something that is with us already and growing every day that will inexorably affect my ability to do that job. It may be that, as a people, we decide the benefits here outweigh the costs and that there is no sensible, technically feasible way to optimize privacy and safety in this particular context, or that public safety folks will be able to do their job well enough in the world of universal strong encryption. Those are decisions Americans should make, but I think part of my job is make sure the debate is informed by a reasonable understanding of the costs.

Topics: Surveillance

Tags: Encryption



James Comey is director of the Federal Bureau of Investigation.

MORE ARTICLES ≥

RELATED ARTICLES

Trust, Apple, and the First Amendment

Andrew Keane Woods _Tue, Feb 23, 2016, 5:44 PM

Apple's Challenge to Magistrate's Order for Assisting the FBI

Herb Lin Wed, Feb 17, 2016, 7:52 PM

Not a Slippery Slope, but a Jump off the Cliff

Nicholas Weaver Wed, Feb 17, 2016, 4:51 PM

NSA IG Report Reveals New Information on Section 702 Collection

Cody M. Poplin Wed, Feb 17, 2016, 4:11 PM

PCLOB Releases Recommendations Assessment Report

Cody M. Poplin _Mon, Feb 8, 2016, 4:49 PM

SUPPORT LAWFARE

Exhibit H

MENU LAWFARE Q

ENCRYPTION

We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead

By **James Comey** Sunday, February 21, 2016, 9:03 PM

The San Bernardino litigation isn't about trying to set a precedent or send any kind of message. It is about the victims and justice. Fourteen people were slaughtered and many more had their lives and bodies ruined. We owe them a thorough and professional investigation under law. That's what this is. The American people should expect nothing less from the FBI.

The particular legal issue is actually quite narrow. The relief we seek is limited and its value increasingly obsolete because the technology continues to evolve. We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. We don't want to break anyone's encryption or set a master key loose on the land. I hope thoughtful people will take the time to understand that. Maybe the phone holds the clue to finding more terrorists. Maybe it doesn't. But we can't look the survivors in the eye, or ourselves in the mirror, if we don't follow this lead.

Reflecting the context of this heart-breaking case, I hope folks will take a deep breath and stop saying the world is ending, but instead use that breath to talk to each other. Although this case is about the innocents attacked in San Bernardino, it does highlight that we have awesome new technology that creates a serious tension between two values we all treasure: privacy and safety. That tension should not be resolved by corporations that sell stuff for a living. It also should not be resolved by the FBI, which investigates for a living. It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before. We shouldn't drift to a place—or be pushed to a place by the loudest voices—because finding the right place, the right balance, will matter to every American for a very long time.

So I hope folks will remember what terrorists did to innocent Americans at a San Bernardino office gathering and why the FBI simply must do all we can under the law to investigate that. And in that sober spirit, I also hope all Americans will participate in the long conversation we must have about how to both embrace the technology we love and get the safety we need.

Topics: Encryption, Going Dark

Tags: Apple, San Bernadino



James Comey is director of the Federal Bureau of Investigation.

MORE ARTICLES ≥

RELATED ARTICLES

Trust, Apple, and the First Amendment

Andrew Keane Woods _Tue, Feb 23, 2016, 5:44 PM

We Enter the Lion's Den: Join Us as We Get Flayed in a Reddit AMA on Apple and the FBI

Susan Hennessey, Benjamin Wittes _Tue, Feb 23, 2016, 3:28 PM

Apple's Letters to the Public are Slightly Disingenuous but Opposing the FBI Request is the Right Outcome For Now

Herb Lin _Tue, Feb 23, 2016, 11:31 AM

Apple in China, Part I: What Does Beijing Actually Ask of Technology Companies?

Samm Sacks Mon, Feb 22, 2016, 7:30 AM

We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead - Lawfare Page 3 of 3 Case 5:16-cm-00010-SP Document 16-9 Filed 02/25/16 Page 4 of 4 Page ID #:170

The Government Strikes Back: DOJ takes off its gloves with Apple

Robert Loeb Fri, Feb 19, 2016, 7:12 PM

SUPPORT LAWFARE

Exhibit I

THE WALL STREET JOURNAL

Investing in the Future of Energy

APRIL 6-8, 2016 SANTA BARBARA, CA REQUEST AN INVITATION

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit http://www.djreprints.com.

http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153

BUSINESS | JOURNAL REPORTS: LEADERSHIP

Gen. Michael Hayden Gives an Update on the Cyberwar

Former head of the CIA and NSA says government moves to protect cyberspace are too little, too late

Feb. 9, 2016 10:49 p.m. ET

We're in a global cyberwar in which our corporate secrets are our chief prize. Are we up for the fight?

To get a clearer answer, The Wall Street Journal's John Bussey spoke with Gen. Michael Hayden, principal of Chertoff Group and former director of the Central Intelligence Agency and National Security Agency. Here are edited excerpts of the discussion.

It's up to you

MR. BUSSEY: We got some news last month. There's some legislation meant to increase cooperation between the government and business. Tell us about the bill and whether or not it helps CIOs protect corporate secrets.

GEN. HAYDEN: We're talking about CISA, the Cybersecurity Information Sharing Act. Good news, a step in the right direction. But it's too long in coming, it's too small a step. And it reveals that within any realistic planning horizon, you are largely responsible for your own defense in the cyber domain.

JOURNAL REPORT

Read more at WSJ.com/LeadershipReport (http://www.wsj.com/public/page/journal-report-leadership.html)

MORE IN CIO NETWORK

- Hilary Mason, Andreas Weigend on the Mistakes Companies Make With Big Data (http://www.wsj.com/articles/the-mistakes-companies-make-with-big-data-1455075886)
- Dawn Lepore Discusses the Path from CIO to CEO (http://www.wsj.com/articles/dawn-lepore-discussesthe-path-from-cio-to-ceo-1455076044)
- Andy Ozment on the Cybersecurity Information Sharing Act (http://www.wsj.com/articles/andy-ozment-on-information-sharing-and-cybersecurity-1455082611)
- Jeremy Bailenson Peers Into the Future of Virtual Reality (http://www.wsj.com/articles/jeremy-bailenson-peers-into-the-future-of-virtual-reality-1455082679)
- Andy Bryant Says CIOs Need Better Communications Skills (http://www.wsj.com/articles/andy-bryant-says-cios-need-better-communications-skills-1455083007)

The government, our government will be permanently late for your cybersecurity. Look, your armed forces view cyber as a domain. Land, sea, air, space, cyber. It's a new domain. You and I have decided that this domain is so wonderful, empowering, we're going to take things we used to keep down here in a safe, in a drawer, in a wallet, and put it up here where it's largely undefended. This is the largest ungoverned space in recorded human history. There is no rule of law up here.

As taxpayers, you and I are going to want our government to defend us up here the way we have become accustomed to relying on the government for defending us down here. But there's the general sclerosis of government, and the technology is going to move much faster than any government can move. Then we have not yet decided what it is we want or what it is we will allow the government to keep us safe. You're going to have to be responsible for your safety [in the cyber domain] in a way in which you have not been required to be responsible for your safety [in the physical domain] since the closing of the American frontier in 1890.

Who follows whom?

MR. BUSSEY: It does seem that before the war on cybersecurity can be fought as a nation, we have to resolve the civil war internally over privacy.

GEN. HAYDEN: Yeah. And that's a multigenerational thing. We haven't arrived at a national consensus. In the American system, when the government doesn't show up, we generally pick up the burden ourselves. So, the good news is there's a lot of private-sector activity designed to keep us safe.

Let me explain this another way. When I think about a national-security problem, generally my instincts are the government is the prime mover. If you're into Civil War history, Gen. Grant or Gen. Lee says, "You, sir, your corps is the main body. And you, gentlemen, you will conform your movements to the movements of the main body." In government, I assumed that in cyberdefense, the main body was the government, and you shall conform your movements with the movements of the main body. In the cyber domain, you are the main body. What our government has to teach itself is that the government needs, in all but a few exceptional cases, to conform its movements to the movements of the main body, you.

MR. BUSSEY: One of the things that the private sector is doing is to look again at encryption.

GEN. HAYDEN: The issue here is end-to-end unbreakable encryption, should American firms be allowed to create such a thing. You've got Jim Comey, the director of the FBI, saying, "I am really going to suffer if I can't read Tony Soprano's email or if I've got to ask Tony for the PIN number before I get to read Tony's emails." I get it. There is an unarguable downside to unbreakable encryption. On the other side is the question: On balance, is America more or less secure with unbreakable end-to-end encryption, regardless of whether Jim can read Tony's emails?

I think Jim Comey's wrong. Jim's logic is based on the belief that he remains the main body and you should accommodate your movements to the movements of him, which is the main body. And I'm telling you, with regard to the cyber domain, he's not. You are.

MR. BUSSEY: *Tell us how the landscape of threat is evolving or changing.*

GEN. HAYDEN: The stealing-your-data stuff is there, and it's getting worse. Beyond that, [people are trying] not just to steal data, but to create effects. So you've got Stuxnet, which is the destruction of a thousand centrifuges at Natanz in Iran. I view it as an unalloyed good, but it was done using a weapon comprised of ones and zeros to create physical destruction.

Leon Panetta spent a lot of time in his last year or two in government talking about cyber Pearl Harbor, digital 9/11, catastrophic attack. I don't think that's what we have to worry about. I'm not frightened about the Chinese turning out all the lights east of the Mississippi. I'm not worried about that superpower, catastrophic attack.

I'm worried about the isolated, nothing to lose, "Ah, what the hell? Let's go see what happens," nation state who goes after a North American enterprise to create physical destruction to show that they can. The Sony attack is the poster child for that.

Concerns and Constraints

Where companies are focusing their information-security efforts and what's holding them back, according to an Ernst & Young survey



Percentage who ranked each of the following a high, medium or low priority for their organization over the coming 12 months



Percentage who said each of the following was among the main obstacles or challenges for their information-security operations

62%Budget constraints

57%

Lack of skilled resources

32%

Lack of executive awareness or support

28%

Lack of quality tools for managing information security

28%

Management and governance issues

23%

Fragmentation of compliance/regulation

Source: Ernst & Young's Global Information Security Survey 2015, a survey of 1,755 CIOs and other executives involved in information security in 67 countries, conducted in person and online between June and September 2015.

THE WALL STREET JOURNAL.

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

Exhibit J

THE WALL STREET JOURNAL

ECO:NOMICS

Investing in the Future of Energy

APRIL 6-8, 2016 SANTA BARBARA, CA REQUEST AN INVITATION

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit http://www.djreprints.com.

http://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096

U.S.

How the U.S. Fights Encryption—and Also Helps Develop It

Agencies are developing encryption tools for secure communications, even as the FBI battles for access to an encrypted iPhone



Nathan Freitas works on ChatSecure at his home office in Boston, Mass. PHOTO: SHIHO FUKADA FOR THE WALL STREET JOURNAL

By DAMIAN PALETTA

Updated Feb. 22, 2016 12:31 a.m. ET

Researchers in London last year discovered an online jihadi handbook with instructions on sending encrypted instant messages that would be indecipherable to law enforcement. The tools it recommended—ChatSecure and Cryptocat—are popular throughout the Middle East, making them easily available to extremists from that part of the world.

They were also developed largely with money from the U.S. government.

The U.S. federal government can work at odds with itself, but not often so directly on a topic with such clear national-security implications. Some federal agencies have funded the development of nearly unbreakable encryption software, while others, especially in intelligence and law enforcement, fume over their inability to read protected messages when they have a court order.

The U.S. Justice Department has sought a court order to force Apple Inc. to help the FBI break into the encrypted iPhone of one of the perpetrators of the San Bernardino, Calif., terrorist attack. Apple says it will fight the order. Meanwhile, at least five federal agencies are developing similar encryption tools, with the aim of helping military officers or pro-democracy activists avoid detection overseas.

The encryption battle has often been framed as a fight pitting technology companies pushing encryption to protect customers' privacy against government officials hoping to crack hidden messages in pursuit of wrongdoers. As the examples of ChatSecure, Cryptocat and other tools show, the division is hardly so neat.

RELATED

Apple Fight Gets Technical (http://www.wsj.com/articles/apple-fbi-phone-fight-gets-technical-1456101154)

Within the government "there are clearly tensions, and those reflect institutional perspectives, the same as personal perspectives," said Ryan Henry, a former Pentagon official. "Whether you prioritize security or you prioritize freedom—institutionally, the government is split along those lines." Mr. Henry also served as information-systems architect at the Defense Advanced Research Projects Agency, known as DARPA, which has conducted encryption research.

Instant messaging

Though the U.S. government has worked in the field of encryption technology for decades, its push into instant-messaging software—useful to anyone from human-rights activists to terrorist plotters—took off just a few years ago.

The process received a boost from Libby Liu, president of the U.S.-funded Radio Free Asia. She was frustrated that reporters and contacts for her news organization were being arrested, harassed and beaten up by some governments' security forces when their messages were intercepted. She felt nothing was secure and worried that spies had penetrated her global newsroom.

Colleagues view Ms. Liu, a former San Francisco prosecutor whose parents immigrated from China, as deeply focused on security and constantly looking for ways to challenge foreign governments that suppress journalists and free speech. She wanted a new way to protect her staff and contacts from spies and hackers, but felt she lacked the tools.

"We want people to be able to talk freely and share ideas that authoritarian governments won't tolerate," Ms. Liu said in an interview.

Congress came to her rescue. Radio Free Asia, founded in 1996, is funded by the Broadcasting Board of Governors, a little-known federal agency that supports international broadcasting with a pro-democracy mission. In 2011, Congress directed \$10 million to the Broadcasting Board of Governors, which advanced \$7 million to Radio Free Asia and Ms. Liu.

Ms. Liu assembled a small team and in 2012 launched the Open Technology Fund, which looked for projects to finance.

It didn't take long for the team to back Nathan Freitas, a technologist and coder. In 2008, he worked on communication security for a group of "Free Tibet" activists traveling to the 2008 Beijing Olympics, but a number of people in the group were arrested and interrogated by the Chinese Public Security Bureau.

After the Olympics, Mr. Freitas convened a group of like-minded coders to work on an encryption tool, which they called Gibberbot, allowing two people to communicate securely through encrypted text messages. They called themselves the Guardian Project.

The Open Technology Fund provided \$388,500 to help Mr. Freitas and his colleagues, with roughly \$100,000 of that going to the encrypted texting program. Gibberbot combined with ChatSecure, an encryption tool in development for Apple iPhones, creating a unified encryption app. Mr. Freitas's team worked to educate people in the Middle East and elsewhere to explain how to use it.

It caught on quickly, in part because ChatSecure is free, simple to use and can be downloaded to smartphones. Users only need to install it and connect with a contact. Their messages are instantly encrypted.

Users don't need to understand the technology, but it works like this: Two people who agree to communicate with each other connect through the application, exchanging (even if they don't realize it) two electronic keys, which are long, unique codes.

If used correctly, the messages can be decoded only by the devices that originated the conversation and contain separate, undiscoverable keys. The key that locks a message is called the "public" key—essentially a digital fingerprint that can be known and shared. The key that unlocks the messages is called the "private" one, and it is implanted securely in each smartphone. No one else has access to that key, not even the device's manufacturer.

Many new smartphones have built-in encryption tools, which is why the Justice Department is pressing Apple to comply in the San Bernardino case. But users often prefer to use tools that aren't designed by large companies, fearful the firms could be compelled to cooperate in decrypting a message.

ChatSecure spread quickly. Democracy activists began using it in Iran, Egypt, Libya, Tibet and elsewhere, to the delight of its creators. Mr. Freitas and his colleagues published blueprints for ChatSecure online so hackers and others could try to find faults with it. Each time a weakness was discovered, they strengthened the program.

Jihadists take it up

It didn't take long for militants to discover ChatSecure. In addition to the jihadi handbook found by the London researchers for Demos, which is a British think tank, another jihadist guide was discovered by SITE Intelligence Group, an American organization that tracks the activity of extremist groups.

This guide listed as the "safest" encryption tools ChatSecure, RedPhone, Signal and two other tools. RedPhone and Signal have since unified. Like ChatSecure, they were financed in part by the Open Technology Fund with money from the U.S. government.

Developers of both ChatSecure and Cryptocat said they have been approached by federal agencies and asked for help in deciphering messages from specific people, reflecting concerns about how the tools were being used. The experience was jarring to coders and developers who had toiled over mathematical formulas and software codes with a vision of helping people thousands of miles away spread democracy.

In an interview, Mr. Freitas initially dismissed the notion of terrorists seizing on his creation. "The content is out there, and for people to copy and paste 'ISIS training manual' on it takes two seconds," he said recently in Brooklyn, N.Y., standing in the Guardian Project's sparse and chilly office beneath the Manhattan Bridge.

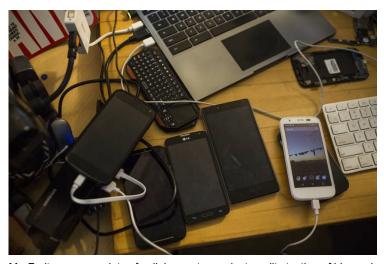
He acknowledged he occasionally second-guesses the motives of some ChatSecure users, who send him questions with Twitter photographs that could resemble jihadists.

"We don't want bad people to use this," said Mr. Freitas. "It makes me sick. I'm a father. I don't want criminals who are hurting children, who are blowing things up or breaking laws to use the tools."

Beyond his work with the Guardian Project, Mr. Freitas is a fellow at Harvard University's Berkman Center for Internet & Society, and he was recently asked to join the technology advisory board at the International Court of Justice in The Hague.

The Broadcasting Board of Governors, which funds several of these initiatives, is adopting a new policy in hopes of inhibiting criminals and terrorists from using them, officials said. A new director for this effort could be in place within weeks.

Other people who have worked on federally funded encryption technology agonized over its potential misuse, though they ultimately defended it. Many described the tools as a natural evolution, like the telephone or automobile, that can be used for good or bad purposes.



Mr. Freitas owns variety of cellphones to conduct quality testing of his product. PHOTO: SHIHO FUKADA FOR THE WALL STREET JOURNAL

Paul Syverson, a mathematician at the U.S. Naval Research Laboratory's Center for High Assurance Computer Systems, was part of a small team that developed Tor, a ground-breaking method of secure communications that enables people to access the Internet anonymously.

Tor was designed in part to help military personnel and U.S. officials communicate overseas, but it now is used for everything from shopping to email. It is credited with helping people avoid surveillance and ensure privacy.

Prosecutors have said drug dealers and child-pornography suspects have used Tor, leading the FBI to hunt for criminals on the routing system.

Mr. Syverson said he worries about that. "I don't care what you are doing—you're driving a taxi, you're cleaning toilets, you're catching cicadas on the end of a sticky pole—whatever you are doing, I think it behooves you to examine the potential implications ... and to try to do the right thing," he said.

The clash between beneficial uses of encryption and problems flowing from it is frustrating to many policy makers. "Encryption is a good thing for all kinds of reasons, for security and privacy and all that," U.S. Director of National Intelligence James Clapper told the Senate Intelligence Committee at a Feb. 9 Senate hearing. "But at the same time, it is enabling nefarious activity of all sorts—whether it's law enforcement or in the national security arena—to go on, and we're losing information because of it."

The State Department, National Security Agency and DARPA are among the agencies that have devoted resources to developing encryption tools. A spokesman for the State Department said its "Internet freedom" effort has a budget of about \$25 million, with an unspecified portion going toward developing secure communication tools.

DARPA spent several years constructing the Safer Warfighter Communications system to help U.S. troops communicate overseas in ways that couldn't be intercepted. An NSA team works on "information assurance" to protect U.S. secrets from spies or adversaries. These programs are highly secretive and aren't available for public use.

The Open Technology Fund set up by Ms. Liu of Radio Free Asia is the only government-funded effort that provides details of its projects.

Despite its relatively small budget, a combined \$21 million in the past two years, the group estimates that a billion people have used technologies it helped create, many of them for encrypted communications.

"While any technology can be misused by bad actors, we focus on protecting some of the world's most vulnerable and repressed," Ms. Liu said. "The program is committed to Congress's goal of making the Internet open, safe and accessible around the world."

FBI push

While government agencies work to develop encryption, the FBI pushes equally hard for technology companies to retain ways to retrieve encrypted messages if presented with a court order. The FBI this month asked Congress for \$69 million to "counter the threat of Going Dark"—being unable to access data because of encryption and other techniques. The bureau currently devotes 39 people and \$31 million to this effort.

Encryption "affects cops and prosecutors and sheriffs and detectives trying to make murder cases, car-accident cases, kidnapping cases, drug cases," the FBI's James Comey said at the hearing with Mr. Clapper. "It has an impact on our national-security work, but overwhelmingly this is a problem that law enforcement sees."

Perhaps no program financed by the Open Technology Fund exhibits the government's push-and-pull more than Cryptocat, which permits secure communications and file-sharing between individuals and groups.

The program was created in 2011 by Nadim Kobeissi, a Lebanese activist and code-writer who was living in Canada at the time. It became popular among Middle Eastern activists during that year's Arab Spring rebellions, according to Mr. Kobeissi, who said Open Technology Fund officials advanced him funding so they could help him strengthen it.

Mr. Kobeissi, now 25 years old, said he was virtually broke at the time, and the \$93,000 the fund offered him in 2012 was enough to support his efforts for two years.

Federal agencies have approached Mr. Kobeissi three times, he said, asking for his help in cracking messages. He said the exchanges have been polite, but he has always said no.

On Friday, Mr. Kobeissi announced he was taking Cryptocat offline until he could make a number of changes to it. He also plans to discontinue its use on smartphones and program it so it can only be used on desktop computers. He said the current debate about encryption had nothing to do with his decision. Rather, he cited his workload as a graduate student and the fact that he likes programming for desktops more than for mobile devices. Still, the change would terminate access to a smartphone tool that has been used throughout the Middle East and elsewhere.

"The thing with bad people using encryption had absolutely nothing at all to do with my decision," he wrote to the Wall Street Journal. "This is purely a major engineering shift in the project. There's nothing political behind it at all. And the thing is, even if Cryptocat ceased to exist, that wouldn't do anything to stop anyone from using encryption. There's still a sea of encrypted services out there. It would've been a pretty pointless move on my behalf."

Write to Damian Paletta at damian.paletta@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

Exhibit K



iOS Security iOS 9.0 or later

September 2015

Contents

Page 4 Introduction

Page 5 System Security

Secure boot chain

System Software Authorization

Secure Enclave

Touch ID

Page 10 Encryption and Data Protection

Hardware security features

File Data Protection

Passcodes

Data Protection classes

Keychain Data Protection

Access to Safari saved passwords

Keybags

Security Certifications and programs

Page 18 App Security

App code signing

Runtime process security

Extensions

App Groups

Data Protection in apps

Accessories

HomeKit

HealthKit

Apple Watch

Page 27 Network Security

TLS

VPN

Wi-Fi

Bluetooth

Single Sign-on

AirDrop security

Page 31 Apple Pay

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

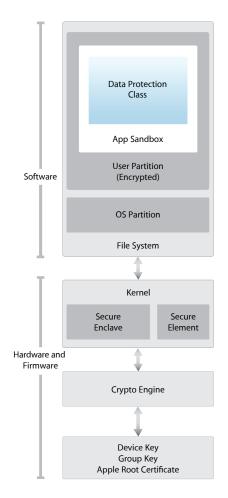
Page 57 Conclusion

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 subdermal 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.

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.

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.

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.

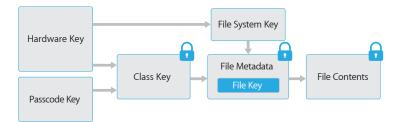
Architecture overview

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 Effaceable 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

- c.a, s . c	assesses arreinb
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	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
While locked	NSFileProtectionCompleteUnlessOpen	N/A
After first unlock	NSFile Protection Complete Until First User Authentication	k Sec Attr Accessible After First Unlock
Always	NSFileProtectionNone	kSecAttrAccessibleAlways
Passcode enabled	N/A	kSecAttrAccessible- WhenPasscodeSetThisDeviceOnly

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 alsosends 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 standardsfor 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.

TIS

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. Certificated-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 CW 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.

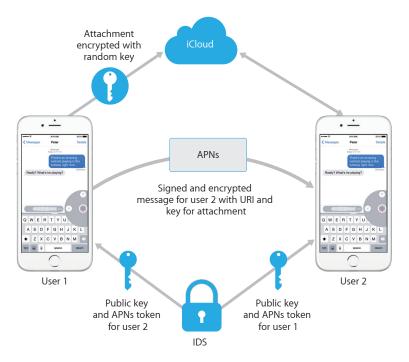
As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which will be verified by sending a confirmation link. Phone numbers are verified 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.

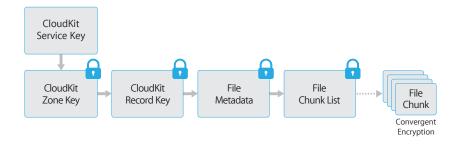
iCloud Drive

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 reguest 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.

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.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

Microphone

Calendars

Camera

Reminders

HomeKit

Photos

- HealthKit
- Motion activity on iPhone 5s or later
- Bluetooth sharing
- Social media accounts, such as Twitter and Facebook

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.

Glossary

Address space layout randomization (ASLR)	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.
Apple Push Notification service (APNs)	A worldwide service provided by Apple that delivers push notifications to iOS devices.
Boot ROM	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.
Data Protection	File and keychain protection mechanism for iOS. It can also refer to the APIs that apps use to protect files and keychain items.
Device Firmware Upgrade (DFU)	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."
ECID	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.
Effaceable Storage	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.
File system key	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.
Group ID (GID)	Like the UID but common to every processor in a class.
Hardware security module (HSM)	A specialized tamper-resistant computer that safeguards and manages digital keys.
iBoot	Code that's loaded by LLB, and in turn loads XNU, as part of the secure boot chain.
Identity Service (IDS)	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.
Integrated circuit (IC)	Also known as a microchip.
Joint Test Action Group (JTAG)	Standard hardware debugging tool used by programmers and circuit developers.
Keybag	A data structure used to store a collection of class keys. Each type (system, backup, escrow, or iCloud Backup) has the same format:
	A header containing:
	– Version (set to 3 in iOS 5)
	– Type (system, backup, escrow, or iCloud Backup)
	– Keybag UUID
	 An HMAC if the keybag is signed The method used for wrapping the class keys: tangling with the UID or PBKDF2, along
	with the salt and iteration count
	• A list of class keys:
	– Key UUID
	- Class (which file or keychain Data Protection class this is)
	- Wrapping type (UID-derived key only; UID-derived key and passcode-derived key)
	– Wrapped class key
	– Public key for asymmetric classes

Keychain	The infrastructure and a set of APIs used by iOS and third-party apps to store and retrieve passwords, keys, and other sensitive credentials.
Key wrapping	Encrypting one key with another. iOS uses NIST AES key wrapping, as per RFC 3394.
Low-Level Bootloader (LLB)	Code that's invoked by the Boot ROM, and in turn loads iBoot, as part of the secure boot chain.
Per-file key	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.
Provisioning Profile	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.
Ridge flow angle mapping	A mathematical representation of the direction and width of the ridges extracted from a portion of a fingerprint.
Smart card	An integrated, embedded circuit that provides secure identification, authentication, and data storage.
System on a chip (SoC)	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.
Tangling	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.
Uniform Resource Identifier (URI)	A string of characters that identifies a web-based resource.
Unique ID (UID)	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.
XNU	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	Updated for iOS 9
	Apple Watch activation lock
	Passcode policies
	• Touch ID API support
	• Data Protection on A8 uses AES-XTS
	Keybags for unattended software update
	Certification updates
	Enterprise app trust model
	Data protection for Safari bookmarks
	App Transport Security
	• VPN specifications
	• iCloud Remote Access for HomeKit
	Apple Pay Rewards cards
	Apple Pay card issuer's app
	Spotlight on-device indexing
	• iOS Pairing Model
	Apple Configurator
	• Restrictions
	 For more information about the security contents of iOS 9 see: support.apple.com/HT205212

^{© 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 L





Testimony

Home • News • Testimony • Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy



James B. Comey Director Federal Bureau of Investigation

Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee Washington, D.C.

July 08, 2015

Good morning, Chairman Grassley, Ranking Member Leahy, and members of the Judiciary Committee. Thank you for the opportunity to testify today about the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as "Going Dark"

We would also like to thank this committee more generally for its continued support for the mission of the Department of Justice. We know that you, like us, take very seriously the role of the Department in protecting the public in a manner that upholds the Constitution and the rule of law.

Introduction

In recent years, new methods of electronic communication have transformed our society, most visibly by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security. The Department is on the frontlines of the fight against cyber crime, and we know first-hand the damage that can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety.

American citizens care deeply about privacy, and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance—not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private communications contain evidence of a crime, then the government can conduct a limited search for that evidence. For example, by having a neutral arbiter—the judge—evaluate whether the government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' Constitutional rights.

The Department of Justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly-authorized warrant issued by a federal

indge. For example, many communications services now encrypt certain communications by default

Recent Testimonies

12.09.15 Law Enforcement Implications of Illegal Online Gambling

Joseph S. Campbell, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Statement Before the House Committee on Oversight and Government Reform, Washington, D.C.

12.09.15 Oversight of the Federal Bureau of Investigation James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary

Committee, Washington, D.C.

10.22.15 Oversight of the Federal Bureau of Investigation
James B. Comey, Director, Federal Bureau of

10.21.15 Worldwide Threats and Homeland Security Challenges

Committee, Washington, D.C.

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the House Committee on Homeland Security, Washington, D.C.

Investigation, Statement Before the House Judiciary

10.08.15 Threats to the Homeland

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C.

08.05.15 Inspector General Access

Kevin L. Perkins, Associate Deputy Director, Federal Bureau of Investigation, Joint Statement with Department of Justice Associate Deputy Attorney General Carlos Uriarte Before the Senate Judiciary Committee, Washington, D.C.

07.08.15 Counterterrorism, Counterintelligence, and the Challenges of Going Dark

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Select Committee on Intelligence, Washington, D.C.

07.08.15 Going Dark: Encryption, Technology, and the Balances Between Public Safety ...

James B. Comey, Director, Federal Bureau of Investigation, Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, Washington, D.C.

06.18.15 FBI's Plans for the Use of Rapid DNA Technology in CODIS

Amy S. Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Washington, D.C.

06.03.15 Terrorism Gone Viral: The Attack in Garland, Texas and Beyond

Michael B. Steinbach, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, Statement Before the House Homeland

Security Committee, Washington, D.C.

with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is "in motion" over electronic networks, or "at rest" on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party.

Threats

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case—from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation—where critical evidence came from smart phones, computers, and online communications.

When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence.

These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from state to state and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker.

In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully authorized access to their data, the jury would not have been able to consider that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

Legal Framework

We would like to emphasize that the Going Dark problem is, at base, one of technological choices and capability. We are not asking to expand the government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the Department of Justice fully complies with those protections. The core question is this: Once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?

We would like to describe briefly the law and the extensive checks, balances, and safeguards that it contains. In addition to the Constitution, two statutes are particularly relevant to the Going Dark problem. Generally speaking, in order for the government to conduct real-time—i.e., data in motion—electronic surveillance of the content of a suspect's communications, it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as "Title III" or the "Wiretap Act") or the Foreign Intelligence Surveillance Act of 1978 (or "FISA"). Title III authorizes the government to obtain a court order to conduct surveillance of wire, oral, or electronic communications when it is investigating federal felonies. Generally speaking, FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court

(FISC), to approve surveillance directed at foreign intelligence and international terrorism threats.

More

Case 5:16-cm-00010-SP Document 16-13 Filed 02/25/16 Page 4 of 5 Page ID #:248

Regardless of which statute governs, however, the standards for the real-time electronic surveillance of United States persons' communications are demanding. For instance, if federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a federal district court judge must find:

- That there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;
- That alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and
- That there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

The law also requires that before an application is even brought to a court, it must be approved by a high-ranking Department of Justice official. In addition, court orders allowing wiretap authority expire after 30 days; if the government seeks to extend surveillance beyond this period, it must submit another application with a fresh showing of probable cause and investigative necessity. And the government is required to minimize to the extent possible its electronic interceptions to exclude non-pertinent and privileged communications. All of these requirements are approved by a federal court.

The statutory requirements for electronic surveillance of U.S. persons under FISA are also demanding. To approve that surveillance, the FISC, must, among other things, find probable cause to believe:

- That the target of the surveillance is a foreign power or agent of a foreign power; and
- That each of the facilities or places at which the electronic surveillance is directed is being used
 or is about to be used by a foreign power or an agent of a foreign power.

Similarly, when law enforcement investigators seek access to electronic information stored-i.e., data at rest—on a device, such as a smartphone, they are likewise bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

Collectively, these statutes reflect a concerted Congressional effort, overseen by an independent judiciary, to validate the principles enshrined in our Constitution and balance several sometimes competing, yet equally legitimate social interests: privacy, public safety, national security, and effective justice. The evolution and operation of technology today has led to recent trends that threaten this time-honored approach. In short, the same ingenuity that has improved our lives in so many ways has also resulted in the proliferation of products and services where providers can no longer assist law enforcement in executing warrants.

Provider Assistance

BothTitle III and FISA include provisions mandating technical assistance so that the government will be able to carry out activities authorized by the court. For example, Title III specifies that a "service provider, landlord...or other person shall furnish [the government]...forthwith all...technical assistance necessary to accomplish the interception." As the communications environment has grown in volume and complexity, technical assistance has proven to be essential for interception to occur. These provisions alone, however, have not historically been sufficient to enable the government to conduct electronic surveillance in a timely and effective manner.

In the early 1990s, the telecommunications industry was undergoing a major transformation and the government faced a similar problem: determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA requires "telecommunications carriers" to develop and deploy intercept solutions in their networks to ensure that the government is able to intercept electronic communications when lawfully authorized, although it does not require a carrier to decrypt communications encrypted by the customer unless the carrier provided the encryption and possesses the information necessary to decrypt. Specifically, it requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as "pen register information" or "dialing and signaling information"). CALEA regulates the capabilities that covered entities must have and does not affect the process or the legal standards that the government must meet in order to obtain a court order to collect communications or related data.

While CALEA was intended to keep pace with technological changes, its focus was on telecommunications carriers that provided traditional telephony and mobile telephone services, not Internet-based communications services. Over the years, through interpretation of the statute by the Federal Communications Commission, the reach of CALEA has been expanded to include facilities-based broadband Internet access and Voice over Internet Protocol (VoIP) services that are fully interconnected with the public switched telephone network. Although that expansion of coverage has been extremely helpful, CALEA does not cover popular Internet-based communications services such as e-mail, Internet messaging, social networking sites, or peer-to-peer services.

At the time CALEA was enacted, Internet-based communications were in a fairly early stage of development, and digital telephony represented the greatest challenge to law enforcement. However, due to the revolutionary shift in communications technology in recent years, the government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.

The harms resulting from the inability of companies to comply with court-ordered surveillance

warrants are not abstract, and have very real consequences in different types of criminal and national security investigations.

Going Forward

Mr. Chairman, The Department of Justice believes that the challenges posed by the Going Dark problem are grave, growing, and extremely complex. At the outset, it is important to emphasize that we believe that there is no one-size-fits-all strategy that will ensure progress. We have been asked what we should do going forward. We believe we will need to pursue multiple paths:

All involved must continue to ensure that citizens' legitimate privacy interests can be effectively secured, including through robust technology and legal protections.

We must continue the current public debate about how best to ensure that privacy and security can coexist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe. The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently implemented poses real barriers to law enforcement's ability to seek information in specific cases of possible national security threat.

We also cannot lose sight of the international implications of this issue. It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection. It is also true that other countries—particularly those without our commitment to the rule of law—are using this debate as a cynical means to create trade barriers, impose undue burdens on our companies, and undermine human rights. We should be clear that any steps that we take here in the United States may impact the decisions that other nations take—both our closest democratic allies and more repressive regimes. In addition, any next steps we identify will be more effective if we are working together with our allies, and made more difficult if we are isolated.

We should also continue to invest in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the Going Dark problem. In limited circumstances, this investment may help mitigate the risks posed in high priority national security or criminal cases, although it will most likely be unable to provide a timely or scalable solution in terms of addressing the full spectrum of public safety needs.

We don't have any silver bullet, and the discussions within the Executive Branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with Congress, industry, academics, privacy groups and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

Conclusion

Mr. Chairman and Ranking Member Leahy, we would like to thank you and the members of this committee again for your attention to this subject of national importance. While technology may change, our basic commitment at the Department to upholding the rule of law and our constitutional traditions does not. Our goal at the Department is to work collaboratively and in good faith with interested stakeholders to explore approaches that protect the integrity of technology and promote strong encryption to protect privacy, while still allowing lawful access to information in order to protect public safety and national security.

We would be happy to answer any questions that you may have.

Accessibility | eRulemaking | Freedom of Information Act | Legal Notices | Legal Policies and Disclaimers | Links | Privacy Policy | USA.gov | White House FBI.gov is an official site of the U.S. government, U.S. Department of Justice

Close

Exhibit M

DON'T PANIC.

Making Progress on the "Going Dark" Debate



Foreword

Just over a year ago, with support from the William and Flora Hewlett Foundation, the Berkman Center for Internet & Society at Harvard University convened a diverse group of security and policy experts from academia, civil society, and the U.S. intelligence community to begin to work through some of the particularly vexing and enduring problems of surveillance and cybersecurity.

The group came together understanding that there has been no shortage of debate. Our goals were to foster a straightforward, non-talking-point exchange among people who do not normally have a chance to engage with each other, and then to contribute in meaningful and concrete ways to the discourse on these issues.

A public debate unfolded alongside our meetings: the claims and questions around the government finding a landscape that is "going dark" due to new forms of encryption introduced into mainstream consumer products and services by the companies who offer them. We have sought to distill our conversations and some conclusions in this report. The participants in our group who have signed on to the report, as listed on the following page, endorse "the general viewpoints and judgments reached by the group, though not necessarily every finding and recommendation." In addition to endorsing the report, some signatories elected to individually write brief statements, which appear in Appendix A.

Our participants who are currently employed full-time by government agencies are precluded from signing on because of their employment, and nothing can or should be inferred about their views from the contents of the report. We simply thank them for contributing to the group discussions.

Matt Olsen, Bruce Schneier, and Jonathan Zittrain
 Project Conveners

Signatories

Urs Gasser Matthew G. Olsen

Nancy Gertner Daphna Renan

Jack Goldsmith Julian Sanchez

Susan Landau Bruce Schneier

Joseph Nye Larry Schwartztol

David R. O'Brien Jonathan Zittrain



Don't Panic

Making Progress on the "Going Dark" Debate

February 1, 2016

Introduction

In the last year, conversations around surveillance have centered on the use of encryption in communications technologies. The decisions of Apple, Google, and other major providers of communications services and products to enable end-to-end encryption in certain applications, on smartphone operating systems, as well as default encryption of mobile devices, at the same time that terrorist groups seek to use encryption to conceal their communication from surveillance, has fueled this debate.

The U.S. intelligence and law enforcement communities view this trend with varying degrees of alarm, alleging that their interception capabilities are "going dark." As they describe it, companies are increasingly adopting technological architectures that inhibit the government's ability to obtain access to communications, even in circumstances that satisfy the Fourth Amendment's warrant requirements. Encryption is the hallmark of these architectures. Government officials are concerned because, without access to communications, they fear they may not be able to prevent terrorist attacks and investigate and prosecute criminal activity. Their solution is to force companies to maintain access to user communications and data, and provide that access to law enforcement on demand, pursuant to the applicable legal process. However, the private sector has resisted. Critics fear that architectures geared to guarantee such access would compromise the security and privacy of users around the world, while also hurting the economic viability of U.S. companies. They also dispute the degree to which the proposed solutions would truly prevent terrorists and criminals from communicating in mediums resistant to surveillance.

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 6 of 38 Page ID #:255

Berkman Center for Internet & Society at Harvard University

Leading much of the debate on behalf of the U.S. government is the Department of Justice, including the Federal Bureau of Investigation, whose leaders have commented on the matter in numerous public statements, speeches, and Congressional testimony throughout 2014 and 2015. After nearly a year of discourse, which included numerous statements critical of the government's position from former U.S. intelligence officials and security technologists, the White House declared in October 2015 it would not pursue a legislative fix in the near future.¹

However, this decision has not brought closure. The FBI has since focused its energy on encouraging companies to voluntarily find solutions that address the investigative concerns. Most recently, terrorist attacks in San Bernardino, Paris, and elsewhere around the world, along with rising concern about the terrorist group ISIS, have focused increased attention on the issues of surveillance and encryption. These developments have led to renewed calls, including among U.S. Presidential candidates, for the government and private sector to work together on the going dark issue and for the Obama administration to reconsider its position.

Findings

Although we were not able to unanimously agree upon the scope of the problem or the policy solution that would strike the best balance, we take the warnings of the FBI and others at face value: conducting certain types of surveillance has, to some extent, become more difficult in light of technological changes. Nevertheless, we question whether the "going dark" metaphor accurately describes the state of affairs. Are we really headed to a future in which our ability to effectively surveil criminals and bad actors is impossible? We think not.

Short of a form of government intervention in technology that appears contemplated by no one outside of the most despotic regimes, communication channels resistant to surveillance will always exist. This is especially true given the generative nature of the modern Internet, in which new services and software can be made available without centralized vetting. However, the question we explore is the significance of this lack of access to communications for legitimate government interests. We argue that communications in the future will neither be eclipsed into darkness nor illuminated without shadow. Market forces and commercial interests will likely limit the circumstances in which companies will offer encryption that obscures user data from the companies themselves, and the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will "go dark" and beyond reach.

Berkman Center for Internet & Society at Harvard University

In short, our findings are:

- End-to-end encryption and other technological architectures for obscuring user data are
 unlikely to be adopted ubiquitously by companies, because the majority of businesses that
 provide communications services rely on access to user data for revenue streams and
 product functionality, including user data recovery should a password be forgotten.
- Software ecosystems tend to be fragmented. In order for encryption to become both
 widespread and comprehensive, far more coordination and standardization than currently
 exists would be required.
- Networked sensors and the Internet of Things are projected to grow substantially, and
 this has the potential to drastically change surveillance. The still images, video, and audio
 captured by these devices may enable real-time intercept and recording with after-thefact access. Thus an inability to monitor an encrypted channel could be mitigated by the
 ability to monitor from afar a person through a different channel.
- Metadata is not encrypted, and the vast majority is likely to remain so. This is data that needs to stay unencrypted in order for the systems to operate: location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before these systems became widespread.
- These trends raise novel questions about how we will protect individual privacy and security in the future. Today's debate is important, but for all its efforts to take account of technological trends, it is largely taking place without reference to the full picture.

A Catalyst: Apple, Google, and Others Introduce Easy-to-Use, Built-In Encryption

In September 2014, about a year and a half after the disclosures by former NSA contractor Edward Snowden, Apple announced its decision to include default encryption of the password-protected contents of its devices in the then-next version of its mobile operating systems, iOS 8.² Indeed, data generated by many of the system apps on iOS 8 and later versions are encrypted when data is stored locally on the phone, in transit, and stored on Apple's servers.³ The decryption keys are tied to the device password and only stored locally on the phone.

Not long after Apple's announcement, Google followed suit by announcing that Lollipop, its next version of Android OS, would enable device encryption by default.⁴ Then, in November 2014, WhatsApp, the

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 8 of 38 Page ID #:257

Berkman Center for Internet & Society at Harvard University

popular instant messaging service for smartphones now owned by Facebook, announced it would support TextSecure, an end-to-end encryption protocol.⁵ In March 2015, Yahoo introduced source code for an extension that encrypts messages in Yahoo Mail, though it requires users to run a key exchange server.⁶ These steps bring to the appliance-style mobile world some of the technologies that have long been available – if not enabled by default – for personal computing operating systems, such as Apple's FileVault and Microsoft's Bitlocker.

The most significant aspects of these announcements are that the encryption takes place using keys solely in the possession of the respective device holders, and it is enabled by default.

While the going dark problem encompasses a range of architectural changes that impede government access, the adoption of encryption of data at rest, and end-to-end encryption in some common communications applications, by companies has become a focal point in the current debate, particularly those in which service providers do not have access to the keys. For example, *end-to-end* encryption is being used to describe scenarios in which information is being encrypted at the end points of a communication channel, and only the original sender and intended recipient possess the keys necessary to decrypt the message. In other words, the information is (in theory, and as advertised) not capable of being read by anyone who sees it traverse a network between the sender and the receiver, including an intermediary service provider, such as Apple. Similarly, *device* encryption – in which the keys exist only on locked devices – prevents the contents from being read by anyone who does not possess the keys.

The distinction is important because an overwhelming percentage of Internet users communicate through web-based services, such as webmail, instant messages, and social networking websites that are not end-to-end encrypted. In the course of an investigation, government officials can intercept communications and seek access to stored communications held by these intermediaries by obtaining a warrant, court order, or subpoena, provided that the company is capable of producing the information sought. However, without access to the keys, a company like Apple is incapable of providing a means to access communications in transit or stored on the company's services, regardless of whether law enforcement presents a valid warrant or court order.⁷

The role of default options and native support for encryption is also important. As with Filevault and Bitlocker for their data at rest, individuals have been able to use encryption software to send and receive end-to-end encrypted messages for a long time. For example, the first widely available public-key crypto software, Pretty Good Privacy (PGP), was made available to the public in the early 1990s. However, for the average computer user, e-mail encryption software has proven difficult to use, especially when it is not supported natively by communication software.⁸ There is a well-documented learning curve to using the

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 9 of 38 Page ID #:258

Berkman Center for Internet & Society at Harvard University

software and it adds several steps to sending messages – both the sender and the recipient need to understand the encryption process, possess the software, generate a key pair, share the public keys, and encrypt and decrypt the messages. Much of this adds complexity and friction that is simply too much for most users to bother.

The complexity is substantially reduced when encryption is supported natively by communication software. When encryption is seamlessly integrated, a user does not have to take any affirmative actions to encrypt or decrypt messages, and much of the process occurs on the back end of the software. In fact, an average user might not be able to tell the difference between an encrypted message and an unencrypted message. When these options are enabled by default on popular devices and platforms, like the iPhone, a large swath of communications is encrypted. Up to this point, government officials have not had to worry about the widespread use of such encryption, but the default nature of these schemes could alter the landscape. To be sure, in the past there was simply less data for government officials to seek in the first place – the amount of digital communications taking place in the PC-only era from 1977 to 2007 – even with the rise of the Internet in between – is dwarfed by the communications facilitated by mobile devices.

Despite all the noise, few of the headline-grabbing and anxiety-provoking (for government, at least) moves by device and operating system makers from 2014 have materialized into real-world default encryption that is beyond the reach of government actors. ¹⁰ Moreover, as we explore below, for a variety of reasons, it is not clear that the wave of encryption introduced in recent years will continue.

The "Going Dark" Debate Begins (Again)

This is not the first debate about the public's ability to use encryption and the government's ability to access communications. Often recounted as the "crypto wars," government access to encrypted communications has been the subject of hot debate and restrictive policy since the 1970s, with the government ultimately relaxing many export-control restrictions on software containing strong cryptographic algorithms in 2000. The roles and obligations of telecommunications companies in providing a means for government actors to wiretap voice communications – in particular on the legacy telephone system that predated the PC and Internet era – have also been debated extensively over these decades. This was framed in the U.S. by the Communications Assistance to Law Enforcement Act – CALEA – which required telephone companies and others to ensure that their networks could be wiretapped, with appropriate legal process, as network technologies moved from analog to digital. The communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the process of the communications are not provided to the

The FBI has led the government's participation in the current debate. The Bureau started publicly raising concerns in 2010 about its ability to capture online communications.¹³ The FBI's then-General Counsel,

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 10 of 38 Page ID #:259

Berkman Center for Internet & Society at Harvard University

Valerie Caproni, appeared before the Senate Judiciary Committee and used the phrase "going dark" to characterize the concern, citing a widening gap between law enforcement's legal privilege to intercept electronic communications and its practical ability to actually intercept those communications. ¹⁴ Her testimony emphasized that many Internet-based communications services have not only become more complex but have also deployed in modalities that are not subject to the Communications Assistance to Law Enforcement Act. ¹⁵ Other reports with similar accounts surfaced during this time period as well, including a declassified FBI situational report on cyber activity that described how data can be "hidden" from law enforcement by using encryption and the end points of communications channels can be obfuscated through use of proxies such as the Tor network. ¹⁶

While the FBI has been the most vocal government agency about this issue, 17 foreign intelligence agencies such as the Central Intelligence Agency and National Security Agency also face obstacles due to encryption and other architectures that impede their access. The government is not a monolithic organization, and the encryption debate is not viewed the same way across governmental organizations or among the individuals within these organizations. The needs and resources of government organizations differ, as do their jurisdictional ambits. For instance, the resources available to the FBI for defeating encryption may be fewer than those available to the NSA. Likewise, state and local authorities have access to fewer resources than law enforcement operating at the federal level. However, while the degree of concern and operational value may not be shared across different agencies and levels of government, there is a general sense by actors within both the intelligence and law enforcement communities that, were all else equal, they would benefit if technological architectures did not present a barrier to investigations. (To be sure, all else is not equal - for example, if all communications were routinely unencrypted, citizens would be exposed to surveillance from myriad sources, many of whom might be viewed as national security threats by those citizens' governments.) Meanwhile certain agencies, including the Department of State, the Naval Research Laboratories, and the Defense Advanced Research Projects Agency (DARPA) have helped support the development of the Tor network, which hides the transactional information of Web-based communications. There are security reasons as well as human-rights interests for the U.S. government's support of Tor.

Since Caproni's invocation of the going dark metaphor in 2010, the problem, according to government officials, continues to worsen. Encryption has become central to their concerns. FBI Director James Comey, who has perhaps been the most vocal government official on this topic throughout the last year, highlighted his unease in October 2014 shortly after the announcements from Apple and Google:

Berkman Center for Internet & Society at Harvard University

"Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so." ¹⁸

In other public statements and Congressional testimony, Director Comey and others, including Deputy Attorney General Sally Yates, have continued to call attention to the problem. According to these statements, the going dark problem is being fueled by "the advent of default encryption settings and stronger encryption standards on both devices and networks," and, it may have a number of implications. For instance, according to FBI officials, "if there is no way to access the data . . . we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets." ²⁰

According to government officials, use of encryption may inhibit the ability of law enforcement and the intelligence community to investigate and prevent terrorist attacks. More specifically, Director Comey has stated that ISIS operators in Syria are "recruiting and tasking dozens of troubled Americans to kill people, [using] a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment." FBI officials have also emphasized that the FBI does not possess the capability to defeat encryption using brute-force attacks and there is not an easy way to get around strong encryption. Recently, Director Comey in Congressional testimony identified a terrorist attack in Garland, Texas, as an example: "[B]efore one of those terrorists left and tried to commit mass murder, he exchanged 109 messages with an overseas terrorist," Comey told a Senate committee. "We have no idea what he said, because those messages were encrypted."

Others from the U.S. intelligence and law enforcement community, including NSA Director Admiral Michael Rogers, Homeland Security Secretary Jeh Johnson, and Attorney General Loretta Lynch have also voiced concerns about the going dark problem.²⁴ In the wake of the November 2015 ISIS-associated attacks in Paris, even in the absence of an on-the-record assertion that the terrorists used encryption to protect their communications, Central Intelligence Agency Director John Brennan suggested terrorists' use of technology "make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it." Whatever the assessment of the use of

Berkman Center for Internet & Society at Harvard University

encrypted communications to frustrate government investigations, a number of former officials from law enforcement and the intelligence community have disagreed about the need for a policy intervention.²⁶

Although much of the debate in the media has focused on whether Director Comey is asking for companies like Google and Apple to preserve access to user data, no formal proposals have emerged from the FBI or other members of the law enforcement and intelligence communities. In July 2015, Director Comey noted in an appearance before the Senate Judiciary and House Intelligence Committees that "while there has not yet been a decision whether to seek legislation, we must work with Congress, industry academics, privacy groups, and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months." Director Comey has also called on the private sector for help in identifying solutions that provide the public with security without frustrating lawful surveillance efforts. Most recently, in October 2015, Comey confirmed in testimony that the Obama administration will not, for the time being, pursue a legislative mandate, but will instead "continue conversations with industry" to find voluntary solutions. ²⁸

Similar debates are ongoing in other countries.²⁹ In the United Kingdom, Prime Minister David Cameron proposed an outright ban on end-to-end encryption technologies following the January 2015 attacks at the *Charlie Hebdo* offices in Paris.³⁰ The more recent November attacks in Paris have also caused French authorities to question policies surrounding the availability of encryption software.³¹ Other European countries have passed or are considering legislation that would require companies to retain readable user data and provide access to government authorities on request.³² And nation states that recognize fewer constitutional or other legal barriers to generating government demands for data, such as Saudi Arabia, Russia, and the U.A.E., have pioneered the use of pre-emptive legal mandates for data retention and decryption by technology providers.

Before we delve into the issues with the going dark metaphor, a few general observations are worth highlighting in brief.

The debate brings to the fore a number of tensions between security, privacy, economic competitiveness, and government access to information. A rich trove of expert literature explores these issues in detail.³³ Many of the technical and political merits of the debate were the focus of the recently published *Keys Under Doormats* report, authored by several of those who join this paper.³⁴ While these perspectives are out of scope for this paper, we acknowledge their importance for understanding the many dimensions of the going dark debate.

Berkman Center for Internet & Society at Harvard University

The global stage on which this debate is unfolding is worth emphasizing. Many geopolitical partners to the U.S. are actively engaged in discussions about promoting cybersecurity and the appropriate limits of surveillance across borders. For instance, the U.S.-E.U. Data Protection safe harbor, which provided a legal framework since the turn of the century for commercial cross-border data flows, was recently ruled invalid by the Court of Justice of the European Union due to concerns about the U.S. intelligence community's ability to access data. The U.N. has also weighed in to a limited extent on encryption, recently declaring it "necessary for the exercise of the right to freedom of expression."

Meanwhile, many U.S. companies must also answer to governments of foreign countries in which they do business. In this vein, they are increasingly playing a quasi-sovereign role as they face difficult decisions when foreign government agencies pressure them to produce data about citizens abroad. Many companies refuse to change the architecture of their services to allow such surveillance. However, if the U.S. government were to mandate architectural changes, surveillance would be made easier for both the U.S. government and foreign governments, including autocratic regimes known to crack down on political dissidents. The comparatively well-developed legal doctrines, procedural requirements, and redress mechanisms that serve as backstops to the U.S. government's surveillance activities are not mirrored worldwide.

On the subject of surveillance tools and techniques, much has changed over the past twenty years. The digital revolution has proven to be a boon for surveillance – it has become possible to track and learn about individuals at very granular level.³⁷ Although use of encryption may present a barrier to surveillance, it may not be impermeable. There are many ways to implement encryption incorrectly and other weaknesses beyond encryption that are exploitable.³⁸ For example, encryption does not prevent intrusions at the end points, which has increasingly become a technique used in law enforcement investigations.³⁹ Encryption typically does not protect metadata, such as e-mail addresses and mobile-device location information, that must remain in plaintext to serve a functional purpose. Data can also be leaked into unencrypted media, through cloud backups and syncing across multiple devices.⁴⁰

Going Dark is the Wrong Metaphor

The going dark metaphor suggests that communications are becoming steadily out of reach – an aperture is closing, and once closed we are blind. This does not capture the current state and trajectory of technological development.

To be sure, encryption and provider-opaque services make surveillance more difficult in certain cases, but the landscape is far more variegated than the metaphor suggests. There are and will always be pockets of

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 14 of 38 Page ID #:263

Berkman Center for Internet & Society at Harvard University

dimness and some dark spots – communications channels resistant to surveillance – but this does not mean we are completely "going dark." Some areas are more illuminated now than in the past and others are brightening. Three trends in particular facilitate government access. First, many companies' business models rely on access to user data. Second, products are increasingly being offered as services, and architectures have become more centralized through cloud computing and data centers. A service, which entails an ongoing relationship between vendor and user, lends itself much more to monitoring and control than a product, where a technology is purchased once and then used without further vendor interaction. Finally, the Internet of Things promises a new frontier for networking objects, machines, and environments in ways that we just beginning to understand. When, say, a television has a microphone and a network connection, and is reprogrammable by its vendor, it could be used to listen in to one side of a telephone conversation taking place in its room – no matter how encrypted the telephone service itself might be. These forces are on a trajectory towards a future with more opportunities for surveillance.

In this section, we hope to elucidate this counter narrative. We do not suggest that the problem the FBI and others have identified is necessarily solved by the availability of other sources of data, nor do we conflate availability with the government's ability to gain access. Rather, we think that the forces opening new opportunities for government surveillance mean that, whatever the situation with iOS 8 encryption versus its predecessor, "going dark" does not aptly describe the long-term landscape for government surveillance. Any debate about surveillance capabilities today that will result in lasting policy should take into account these larger trends.

Encryption Runs Counter to the Business Interests of Many Companies

Current company business models discourage implementation of end-to-end encryption and other technological impediments to company, and therefore government, access.

For the past fifteen years, consumer-facing Internet companies have relied on advertising as their dominant business model. Ads are frequently used to subsidize free content and services. Internet companies more recently have been shifting towards data-driven advertising, and the technology that facilitates advertising delivery has become more reliant on user data for targeting ads based on demographics and behaviors. Companies seek to make behavioral assessments to match ads to individuals on the fly. Google products display advertising determined by behavioral patterns, search queries, and other signals collected by Google. Similarly, Facebook claims it is capable of reaching narrow audiences in advertising campaigns with S9% accuracy based on location, demographics, interests, and behaviors. Yahoo products are also supported by advertising. And, the list goes on.

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 15 of 38 Page ID #:264

Berkman Center for Internet & Society at Harvard University

To fuel this lucrative market, companies typically wish to have unencumbered access to user data – with privacy assured through either restricting dissemination of identifiable customer information outside the boundaries of the company (and of governments, should they lawfully request the data). Implementing end-to-end encryption by default for all, or even most, user data streams would conflict with the advertising model and presumably curtail revenues. Market trends so far reflect that companies have little incentive to veer from this model, making it unlikely that end-to-end encryption will become ubiquitous across applications and services. As a result, many Internet companies will continue to have the ability to respond to government orders to provide access to communications of users.

Cloud computing entails the movement of data and software to centralized locations operated by companies instead of under direct user custody. This technology, made possible by ubiquitous connectivity, enables businesses and individuals to extend their computing resources through the Internet at remote data centers, much like a utility service. As a result, products are increasingly being offered as services, which in turn marks a shift away from traditional notions of ownership and control, and more towards centralized repositories of user data. Software and data no longer need to be installed and stored locally on an individual's computer – they can be delivered through a cloud service (e.g., Google Apps) or stored remotely in a cloud storage service (e.g., Dropbox) where they can be conveniently accessed from anywhere through a web browser or a smartphone app. Webmail, social networking, word processing, and other common applications are now typically delivered as networked services. These services deliver substantial benefits and convenience to both individuals and companies, and they are often provided free in ad-subsidized models or in economical pay-as-you-go arrangements.

End-to-end encryption is currently impractical for companies who need to offer features in cloud services that require access to plaintext data. For example, Google offers a number of features in its web-based services that require access to plaintext data, including full text search of documents and files stored in the cloud. In order for such features to work, Google must have access to the plaintext. While Apple says that it encrypts communications end-to-end in some apps it develops, the encryption does not extend to all of its services. This includes, in particular, the iCloud backup service, which conveniently enables users to recover their data from Apple servers. iCloud is enabled by default on Apple devices. Although Apple does encrypt iCloud backups,⁴⁸ it holds the keys so that users who have lost everything are not left without recourse. So while the data may be protected from outside attackers, it is still capable of being decrypted by Apple.⁴⁹ Since Apple holds the keys, it can be compelled through legal process to produce user data that resides in iCloud.

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 16 of 38 Page ID #:265

Berkman Center for Internet & Society at Harvard University

There are a number of other reasons why a shift to encryption or other architectures would not appeal to businesses. Encryption schemes often add complexity to the user experience. Former Facebook Chief Security Officer Joe Sullivan observed that Facebook "has been able to deploy end-to-end encryption for a long time," but it has held back due to the added complexity and because "when end-to-end encryption is done right, it's hard for the average person to communicate." Google has also reportedly held off on implementing device encryption by default on locked Android devices due to performance issues, despite its announcements that it would do so in 2014. To date, the latest version of Android does not enable encryption by default.

Fragmentation in software ecosystems can also impede the degree to which new conventions and architectural changes – especially those that would enable user-to-user encryption across different devices and services – become widespread. In these ecosystems, multiple points of control may exist that influence the types of apps and operating system updates that eventually filter down to end users.

For example, in the Android ecosystem, smartphones are controlled by the wireless providers and handset manufacturers who create customized versions of the Android operating systems for the phones they sell. These companies have little incentive to update older phones to the latest versions of Android, because it would require them to invest resources into making the customized features compatible with newer versions of Android. Fact, many older Android smartphones are never updated to newer OS versions. According to Google, as of this writing, approximately 32% of Android devices are running the latest Lollipop, which was released in November 2014. In addition, although the next version of Android released by Google may contain apps that support end-to-end encryption, a manufacturer or wireless provider may modify the software to include its own suite of custom apps that do not support encryption. Some of these companies may have commercial interests in retaining access to plaintext communications. A wide variety of third-party messaging applications are also available on Google Play, and end users can install and use them in place of the pre-installed messaging app that ships on their phones. In order for end-to-end encryption to work properly, both a sender's and receiver's messaging apps must be able to support it, and not all do. If the ecosystem is fragmented, encryption is that much less likely to become all encompassing.

The Internet of Things and Networked Sensors Open Uncharted Paths to Surveillance

A plethora of networked sensors are now embedded in everyday objects. These are prime mechanisms for surveillance: alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark – so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become. To paint an overall picture of going dark

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 17 of 38 Page ID #:266

Berkman Center for Internet & Society at Harvard University

based upon the fact that a number of widely used applications and products have introduced encryption by default risks obscuring this larger trend.

According to analysts and commentators representing the conventional wisdom, the Internet of Things (IoT) is the next revolution in computing. Expert observers have suggested that "the Internet of Things has the potential to fundamentally shift the way we interact with our surroundings," at work, at home, in retail environments, in cars, and on public streets.⁵⁵ The IoT market is forecast to grow into a multi-trillion dollar industry within the next ten years,⁵⁶ and according to a survey of experts, it will have "widespread and beneficial effects by 2025." This will result in significant changes in how members of society interact with one another and the inanimate objects around them.⁵⁸

Appliances and products ranging from televisions and toasters to bed sheets, light bulbs, cameras, toothbrushes, door locks, cars, watches and other wearables are being packed with sensors and wireless connectivity.⁵⁹ Numerous companies are developing platforms and products in these areas.⁶⁰ To name but a few, Phillips, GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all working on products with embedded IoT functionality, with sensors ranging from gyroscopes, accelerometers, magnetometers, proximity sensors, microphones, speakers, barometers, infrared sensors, fingerprint readers, and radio frequency antennae with the purpose of sensing, collecting, storing, and analyzing finegrained information about their surrounding environments. These devices will all be connected to each other via the Internet, transmitting telemetry data to their respective vendors in the cloud for processing.⁶¹

The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications. A ten-year-old case involving an inautomobile concierge system provides an early indication of how this might play out. The system enables the company to remotely monitor and respond to a car's occupants through a variety of sensors and a cellular connection. At the touch of a button, a driver can speak to a representative who can provide directions or diagnose problems with the car. During the course of an investigation, the FBI sought to use the microphone in a car equipped with such a system to capture conversations taking place in the car's cabin between two alleged senior members of organized crime. In 2001, a federal court in Nevada issued ex parte orders that required the company to assist the FBI with the intercept. The company appealed, and though the Ninth Circuit disallowed the interception on other grounds, it left open the possibility of using in-car communication devices for surveillance provided the systems' safety features are not disabled in the process. Such assistance might today be demanded from any company capable of recording conversations or other activity at a distance, whether through one's own smartphone, an Amazon Echo, a

Berkman Center for Internet & Society at Harvard University

baby monitor, an Internet-enabled security camera, or a futuristic "Elf on a Shelf" laden with networked audio and image sensors.⁶³

In February 2015, stories surfaced that Samsung smart televisions were listening to conversations through an onboard microphone and relaying them back to Samsung to automatically discern whether owners were attempting to give instructions to the TV.⁶⁴ A statement published in Samsung's privacy policy instructed users to "be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of the Voice Recognition."⁶⁵

Any given step of Samsung's process makes sense to offer the TV's features. Voice recognition is a computationally intensive task, and the processing capabilities of a modern television would be insufficient to make such a feature work. This is a common challenge for IoT devices that have limited processing power and limited battery capacity. The solution, in this case, was to utilize cloud infrastructure through a network connection to send the voice data to a remote server for processing and interpretations of that data back to the television as machine-actionable commands. Simple commands, such as "switch to channel 13," could be processed locally, but more complex ones, such as "show me a sci-fi movie like last week's, but not with Jane Fonda," would need to be sent to the cloud infrastructure – and in Samsung's case, to a third party, for processing.

Similarly, Google's Chrome browsing software supports voice commands using the onboard microphone in a laptop or desktop computer. The feature is activated when a user states the phrase "OK Google," and the resource intensive voice processing takes place on Google's remote servers. ⁶⁶ Even children's toys are beginning to possess these features. In April 2015, Mattel introduced "Hello Barbie," an interactive doll capable of responsive speech, which is accomplished by recording children's interactions with the doll through a microphone, processing it in the cloud, and sending verbal responses through a speaker on the doll. ⁶⁷ IP video cameras have also risen in popularity in the last several years. Devices like the Nest Cam record high resolution video with a wide-angle lens camera broadcast over the Internet to account holders. ⁶⁸ Users can tune into the recording from Nest's website or through an app on their phone, and a camera will send an alert if it detects motion or an unusual noise. The Nest Cam can also exchange data and interact with other devices, such as Nest's thermostats and smoke detectors, which themselves contain sensors and microphones.

Law enforcement or intelligence agencies may start to seek orders compelling Samsung, Google, Mattel, Nest or vendors of other networked devices to push an update or flip a digital switch to intercept the ambient communications of a target. These are all real products now. If the Internet of Things has as

Berkman Center for Internet & Society at Harvard University

much impact as is predicted, the future will be even more laden with sensors that can be commandeered for law enforcement surveillance; and this is a world far apart from one in which opportunities for surveillance have gone dark. It is vital to appreciate these trends and to make thoughtful decisions about how pervasively open to surveillance we think our built environments should be – by home and foreign governments, and by the companies who offer the products that are transforming our personal spaces.

Concluding Thoughts

The debate over encryption raises difficult questions about security and privacy. From the national security perspective, we must consider whether providing access to encrypted communications to help prevent terrorism and investigate crime would also increase our vulnerability to cyber espionage and other threats, and whether nations that do not embrace the rule of law would be able to exploit the same access. At the same time, from a civil liberties perspective, we must consider whether preventing the government from gaining access to communications under circumstances that meet Fourth Amendment and statutory standards strike the right balance between privacy and security, particularly when terrorists and criminals seek to use encryption to evade government surveillance.

In examining these questions, our group focused on the trajectory of surveillance and technology. We concluded that the "going dark" metaphor does not fully describe the future of the government's capacity to access the communications of suspected terrorists and criminals. The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense, the government is losing some surveillance opportunities. However, we concluded that the combination of technological developments and market forces is likely to fill some of these gaps and, more broadly, to ensure that the government will gain new opportunities to gather critical information from surveillance.

Looking forward, the prevalence of network sensors and the Internet of Things raises new and difficult questions about privacy over the long term. This means we should be thinking now about the responsibilities of companies building new technologies, and about new operational procedures and rules to help the law enforcement and intelligence communities navigate the thicket of issues that will surely accompany these trends.

Appendix A: Individual Statements from Signatories

Three signatories to this report elected to write statements to individually reflect on the report or particular issues discussed within it. The statements listed below are included in this Appendix.

Susan Landau, "The National-Security Needs for Ubiquitous Encryption"

Bruce Schneier, "Security or Surveillance?"

Jonathan Zittrain, "The Good News and the Troubling News: We're not going dark"

Appendix A: Individual Statements from Signatories

The National-Security Needs for Ubiquitous Encryption

Susan Landau

Each terrorist attack grabs headlines, but the insidious theft of U.S. intellectual property – software, business plans, designs for airplanes, automobiles, pharmaceuticals, etc. – by other nations does not. The latter is the real national-security threat and a strong reason for national policy to favor ubiquitous use of encryption.

In 2000, the U.S. government loosened export controls on encryption. In part this was because of pressures from Silicon Valley and Congress,¹ but in large part, the reason for this change was national security. The end of the Cold War led to a temporary decline in military spending. One way to accommodate the shift was to turn to commercial off the shelf (COTS) equipment, a requirement formalized in the 1996 Clinger-Cohen Act.² Another reason for the shift to COTS equipment for communications and computer technology was the speed of innovation in Silicon Valley. The need for ubiquitous security throughout our communications systems represented the third major reason.

There was an era when Blackberrys were the communication device of choice for the corporate world; these devices, unlike the recent iPhones and Androids, can provide cleartext of the communications to the phone's owner (the corporation for whom the user works). Thus businesses favored Blackberrys.

But apps drive the phone business. With the introduction of iPhones and Androids, consumers voted with their hands. People don't like to carry two devices, and users choose to use a single consumer device for *all* communications. We have moved to a world of BYOD (Bring Your Own Device).³ In some instances, e.g., jobs in certain government agencies, finance, and the Defense Industrial Base, the workplace can require that work communications occur only over approved devices. But such control is largely ineffective in most work situations. So instead of Research in Motion developing a large consumer user base, the company lost market share as employees forced businesses to accept their use of personal

¹ For a longer explanation of the confluence of issues, *see*, *e.g.*, Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th Century and the 21st" in Karl De Leeuw and Jan Bergstra (eds.), *The History of Information Security* (Elsevier, 2007), at 733-735.

² 40 U.S.C. § 1401 et seq.

³ Mick Slattery, "How Consumer Technology is Remaking the Workplace," *WIRED*, March 2013, http://www.wired.com/insights/2013/03/how-consumer-technology-is-remaking-the-workplace/.

Appendix A: Individual Statements from Signatories

devices for corporate communications. Thus access to U.S. intellectual property lies not only on corporate servers – which may or may not be well protected – but on millions of private communication devices.

Protecting U.S. intellectual property is crucial for U.S. economic and national security, and given BYOD – a social change that is here to stay – encrypted communications are necessary for national security. In a July 2015 *Washington Post* op-ed former DHS Secretary Michael Chertoff, former NSA Director Mike McConnell, and former Deputy Defense Secretary William Lynn concurred, observing that "Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interest. . . . If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential." They concluded that the security provided by encrypted communications was more important than the difficulties encryption present to law enforcement.

There are, after all, other ways of going after communications content than providing law enforcement with "exceptional access" to encrypted communications. These include using the existing vulnerabilities present in the apps and systems of the devices themselves. While such an approach makes investigations more expensive, this approach is a tradeoff enabling the vast majority of communications to be far more secure.

Exceptional access is dangerous. As my co-authors and I have described in our *Keys under Doormats* paper,⁵ proposals for law-enforcement "exceptional access" ignore the realities of current software. Getting software correct is very difficult. Thus, for example, when NSA tested CALEA-compliant switches,⁶ it discovered security problems with every implementation.⁷ Furthermore, exceptional access

_

⁴ Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear of ubiquitous data encryption is overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

⁵ Hal Abelson et al., "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

⁶ The 1994 Communications Assistance for Law Enforcement Act (CALEA) requires all digitally switched networks be built to accommodate lawful surveillance. Pub. L. 103-414.

⁷ Private communication with Richard George, Former Technical Director for Information Assurance, National Security Agency (Dec. 1, 2011).

Appendix A: Individual Statements from Signatories

prevents the deployment of two extremely useful forms of security: forward secrecy and authenticated encryption.⁸

At a time when nation-state espionage is heavily aimed at business communications and these communications are often found on personal devices, national security dictates that they be secured. And that means policy facilitating the ubiquitous use of uncompromised strong encryption is in our national security interest.

⁸ Hal Abelson et al., "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

Appendix A: Individual Statements from Signatories

Security or Surveillance?

Bruce Schneier

Both the "going dark" metaphor of FBI Director James Comey¹ and the contrasting "golden age of surveillance" metaphor of privacy law professor Peter Swire² focus on the value of data to law enforcement. As framed in the media, encryption debates are about whether law enforcement should have surreptitious access to data, or whether companies should be allowed to provide strong encryption to their customers.

It's a myopic framing that focuses only on one threat – criminals, including domestic terrorists – and the demands of law enforcement and national intelligence. This obscures the most important aspects of the encryption issue: the security it provides against a much wider variety of threats.

Encryption secures our data and communications against eavesdroppers like criminals, foreign governments, and terrorists. We use it every day to hide our cell phone conversations from eavesdroppers, and to hide our Internet purchasing from credit card thieves. Dissidents in China and many other countries use it to avoid arrest. It's a vital tool for journalists to communicate with their sources, for NGOs to protect their work in repressive countries, and for attorneys to communicate with their clients.

Many technological security failures of today can be traced to failures of encryption. In 2014 and 2015, unnamed hackers – probably the Chinese government – stole 21.5 million personal files of U.S. government employees and others. They wouldn't have obtained this data if it had been encrypted. Many large-scale criminal data thefts were made either easier or more damaging because data wasn't encrypted: Target, TJ Maxx, Heartland Payment Systems, and so on. Many countries are eavesdropping on the unencrypted communications of their own citizens, looking for dissidents and other voices they want to silence.

_

¹ James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course," speech at Brookings Institution, October 16, 2014. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

² Peter Swire, testimony at Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," July 8, 2015. https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

Case 5:16-cm-00010-SP Document 16-14 Filed 02/25/16 Page 25 of 38 Page ID #:274

Appendix A: Individual Statements from Signatories

Adding backdoors will only exacerbate the risks. As technologists, we can't build an access system that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document.³ If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists. This is not theoretical; again and again, backdoor accesses built for one purpose have been surreptitiously used for another. Vodafone built backdoor access into Greece's cell phone network for the Greek government; it was used against the Greek government in 2004-2005.⁴ Google kept a database of backdoor accesses provided to the U.S. government under CALEA; the Chinese breached that database in 2009.⁵

We're not being asked to choose between security and privacy. We're being asked to choose between less security and more security.

This trade-off isn't new. In the mid-1990s, cryptographers argued that escrowing encryption keys with central authorities would weaken security.⁶ In 2011, cybersecurity researcher Susan Landau published her excellent book *Surveillance or Security?*, which deftly parsed the details of this trade-off and concluded that security is far more important.⁷

Ubiquitous encryption protects us much more from bulk surveillance than from targeted surveillance. For a variety of technical reasons, computer security is extraordinarily weak. If a sufficiently skilled, funded, and motivated attacker wants in to your computer, they're in. If they're not, it's because you're not high enough on their priority list to bother with. Widespread encryption forces the listener – whether a foreign government, criminal, or terrorist – to target. And this hurts repressive governments much more than it hurts terrorists and criminals.

³ Hal Abelson et al., "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

⁴ Vassilis Prevelakis, Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, June 27, 2007. http://spectrum.ieee.org/telecom/security/the-athens-affair.

⁵ Ellen Nakashima, "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say," *The Washington Post*, May 20, 2013, https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

⁶ Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1998. https://www.schneier.com/paper-key-escrow.html.

⁷ Susan Landau, Surveillance or Security: The Risks Posed by New Wiretapping Technologies (Cambridge: MIT Press, 2011).

Appendix A: Individual Statements from Signatories

Of course, criminals and terrorists have used, are using, and will use encryption to hide their planning from the authorities, just as they will use many aspects of society's capabilities and infrastructure: cars, restaurants, telecommunications. In general, we recognize that such things can be used by both honest and dishonest people. Society thrives nonetheless because the honest so outnumber the dishonest. Compare this with the tactic of secretly poisoning all the food at a restaurant. Yes, we might get lucky and poison a terrorist before he strikes, but we'll harm all the innocent customers in the process. Weakening encryption for everyone is harmful in exactly the same way.

Appendix A: Individual Statements from Signatories

The Good News and the Troubling News: We're not going dark

Jonathan Zittrain

Two trends have dominated the U.S. foreign intelligence landscape for the past fifteen years.

The first arises from the terrorist attacks of 9/11. The attacks reshaped the priorities of the U.S. intelligence community, as extraordinary resources have been allocated to prevent and counter terrorism. Our national security establishment has pioneered new technological tools and new legal authorities (or interpretations of existing ones) in an effort to secure safety.

The second trend is the mainstreaming of the Internet and surrounding technologies built around and upon it, which has led to an unprecedented proliferation of data that can be analyzed by the intelligence services. In late 2001 there were no smartphones and no social media. Facebook and Twitter were still years away from capturing our imagination, our time – and our data. The more bits we generate, actively through typing and talking, and passively by sharing our location, our social relationships, and other information as we go about our lives, the more there is for vendors – and the governments to whom they answer – to potentially review, whether in bulk or individually.

The intersection of these trends led to what Peter Swire and Kenesa Ahmad in 2011 called "the Golden Age of Surveillance." Since then, that high water mark for opportunities for surveillance has receded in places. Some communications and data previously accessible by governments through vendors is no longer so easily obtained, because some vendors have refined the technologies they offer to prevent even themselves from seeing the data the users generate and exchange with one another. Such technologies, including the use of encryption, are not new as a category, but their entry into mainstream usage perhaps is. Losing a tool, rather than never having had it to begin with, is no doubt highly salient for the director of the FBI and others charged with protecting security. They ask: if we have a warrant or other legal authority, why should previously-accessible information now be off-limits to us?

I empathize with the idea that just how much government can learn about us should not depend on the cat and mouse game of technological measure and counter-measure. Ideally, a polity would carefully calibrate its legal authorities to permit access exactly and only where it comports with the imperatives of

¹ Peter Swire and Kenesa Ahmad, "Going Dark' Versus a Golden Age of Surveillance," Center for Democracy & Technology, November 28, 2011.

Appendix A: Individual Statements from Signatories

legitimate security – and with basic human rights as recognized through the protections of conventions and constitutions. For one intriguing attempt to reconcile government use of technological hacking tools with appropriate privacy protections, you might read the proposal for "lawful hacking" that civil liberties—minded computer scientists Steven Bellovin, Matt Blaze, Sandy Clark, and fellow project participant Susan Landau have advocated.²

But it is a very large step – a leap, even – to go beyond the legal demand for information already in a company's possession, and beyond the use of technological tools to reveal what otherwise is obscure, to requirements on how technology must be deployed to begin with. I've written reasons why this leap is ill-advised.³ To try to constrain the generative Internet ecosystem in that way would be either futile or require that we, in the fitting words of the U.S. Supreme Court, "burn the house to roast the pig." That turn of phrase was used by Justice Frankfurter to explain why a Michigan law banning books that could tend to "corruption of the morals of youth" violated the First Amendment, even if it was aimed at a laudable goal. Here, too, there are times we will rue the cleverness or luck of a criminal who benefits first from the Internet's facilitation of communication and organization, and then from encryption to prevent his or her activities from being discovered or investigated. But this is not reason enough to require that foundational technologies be restricted or eliminated in general use – any more than the population of Michigan could rightly be restricted to reading only what is fit for children.

Most of the "Don't Panic" report from our Berklett cybersecurity project isn't about that. Given the spectrum of roles and viewpoints represented in the room, our focus was more on a factual (if speculative) question – are we really "going dark"? – than one of articulating and balancing values. The answer, in the big picture, is no, even as it's small solace to a prosecutor holding both a warrant and an iPhone with a password that can't be readily cracked. (To be sure, many of those situations will also have an owner who could, after process, be ordered by a court to unlock the phone on pain of contempt.)

² See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," 12 Northwestern Journal of Technology & Intellectual Property 1 (2014), available at http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1.

³ See Jonathan Zittrain, "An Open Letter to Prime Minister Cameron: 20th-Century Solutions Won't Help 21st-Century Surveillance," (2015), https://medium.com/message/dear-prime-minister-cameron-20th-century-solutions-wont-help-21st-century-surveillance-ff2d7a3d300c.

⁴ Butler v. Michigan, 352 U.S. 380, 383 (1957).

Appendix A: Individual Statements from Signatories

As data collection volume and methods proliferate, the number of human and technical weaknesses within the system will increase to the point that it will overwhelmingly likely be a net positive for the intelligence community. Consider all those IoT devices with their sensors and poorly updated firmware. We're hardly going dark when – fittingly, given the metaphor – our light bulbs have motion detectors and an open port. The label is "going dark" only because the security state is losing something that it fleetingly had access to, not because it is all of a sudden lacking in vectors for useful information.

But exactly what should reassure government officials, and stay the momentum for major policy interventions into Internet technology development, is what should also trouble everyone: we are hurtling towards a world in which a truly staggering amount of data will be only a warrant or a subpoena away, and in many jurisdictions, even that gap need not be traversed. That's why this report and the deliberations behind it are genuinely only a beginning, and there's much more work to do before the future is upon us.

Appendix B: Berklett Cybersecurity Project Group Members and Guests

Appendix B: Berklett Cybersecurity Project Group Members and Guests

More information about the Berkman Center's Berklett Cybersecurity Project can be found here: http://brk.mn/cybersecurity.

At the heart of the project is an extremely diverse group of experts who regularly convene, approximately every three months, to discuss enduring problems of surveillance and cybersecurity. As part of the meetings, special guests are occasionally invited to join these meetings for the opportunity to share unique perspectives on specific topics of discussion.

The core members of the group are:

John DeLong: the Director of the Commercial Solutions Center at the National Security Agency. Formerly he was the Director of Compliance at the NSA and previously served as the Deputy Director of the National Cyber Security Division at the Department of Homeland Security. He has also developed classes and taught at the National Cryptologic School in areas of compliance, computer science, and cybersecurity.

Urs Gasser: the Executive Director of the Berkman Center for Internet & Society and a Professor of Practice at Harvard Law School. His research includes activities focused on information law, policy, and society with projects in collaboration with leading international research institutions exploring regulation, ICT interoperability, cybersecurity, and the law's impact on innovation and risk in the ICT space. Urs is the author of several books, including, with John Palfrey, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books, 2012).

Hon. Nancy Gertner (ret.): a former U.S. federal judge for the U.S. District Court for the District of Massachusetts. She was appointed to the federal bench by President Bill Clinton in 1994,

^{*}This publication would not have been possible without contributions from the project's talented team members and collaborators, in particular Samantha Bates, Tiffany Lin, Shailin Thomas, and Jordi Weinstock, who contributed research, editing, and inspiration throughout the writing process. A number of the Berkman Center's summer interns, research assistants, and Harvard Law School students also contributed to the report, including Abby Colella, David Eichert, Lydia Lichlyter, and Grant Nelson. We are also indebted to many other staff members at the Center and Harvard Law School who supported the project and the report, including Carey Andersen, Ryan Budish, Rob Faris, Dan Jones, Sue Kriegsman, Amanda McMahan, Annie Pruitt, Daniel Oyolu, Gretchen Weber, and Amy Zhang.

Appendix B: Berklett Cybersecurity Project Group Members and Guests

holding the position for 17 years. She has written and spoken widely on various legal issues concerning civil rights and liberties, criminal justice, and procedural issues. Currently, she is a Senior Lecturer on Law at Harvard Law School.

Jack Goldsmith: formerly served as Assistant Attorney General, Office of Legal Counsel, and Special Counsel to the Department of Defense for the Bush Administration. He is the Henry L. Shattuck Professor of Law at Harvard Law School and a Senior Fellow at the Hoover Institution at Stanford University. He is also the co-founder of Lawfareblog.com, and focuses on national security, international, and Internet law, and cybersecurity.

Susan Landau: a professor of cybersecurity policy at Worcester Polytechnic Institute and a visiting professor in computer science at University College London. She works at the intersection of cybersecurity, national security, law, and policy, and is the author of numerous books, including Surveillance or Security?: Risks Posed by New Wiretapping Technologies (MIT Press, 2011) and, with Whitfield Diffie, Privacy on the Line: The Politics of Wiretapping and Encryption (MIT Press, rev. ed. 2007). Susan has previously served as a senior staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems.

Anne Neuberger: the Chief Risk Officer at the National Security Agency, responsible for the implementation of the risk management process. She is also a member of the NSA's Senior Leadership team. Previously she served as the Director of NSA's Commercial Solutions Center, and as Special Assistant to the Director for the Enduring Security Framework.

Joseph Nye: formerly served as the Assistant Secretary of Defense for International Security Affairs, Chair of the National Intelligence Council, and was the Deputy Under Secretary of State for Security Assistance, Science and Technology. Ranked as the most influential scholar on American foreign policy, he has written extensively on international relations and power. He was formerly the Dean of the Harvard Kennedy School of Government and is currently a University Distinguished Service Professor at Harvard.

David R. O'Brien: a Senior Researcher at the Berkman Center for Internet & Society at Harvard University, where he leads research initiatives on privacy and cybersecurity. He formerly practiced intellectual property and technology law in Boston.

Matthew G. Olsen: former Director of the U.S. National Counterterrorism Center appointed by President Obama in 2011. Prior to that position, he served as General Counsel for the National Security Agency, in leadership positions at the Department of Justice, and as a federal prosecutor. Currently, he is a president and co-founder of IronNet Cybersecurity, a lecturer at Harvard Law School, and a national security analyst for ABC News.

Appendix B: Berklett Cybersecurity Project Group Members and Guests

Daphna Renan: served as an Attorney Advisor in the Justice Department's Office of Legal Counsel as well as Counsel to the Deputy Attorney General. She is currently an Assistant Professor of Law at Harvard Law School where her research examines surveillance as ongoing and routinized domestic administration, and explores mechanisms for its systematic governance.

Julian Sanchez: a Senior Fellow at the Cato Institute who studies technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance. He was formerly the Washington editor for Ars Technica, and was a writer for The Economist's Democracy in America. He is also a founding editor of the policy blog, Just Security.

Bruce Schneier: a renowned security technologist who has written extensively on security issues, both academically and within the public. He is the Chief Technology Officer of Resilient Systems, a fellow at the Berkman Center for Internet & Society, a program fellow at the Open Technology Institute, and a board member of the Electronic Frontier Foundation. He is also the author of numerous books on security, surveillance, and cryptography, including the New York Times Bestseller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton and Company, 2015).

Larry Schwartztol: formerly worked as a staff attorney at the American Civil Liberties Union's National Security project, litigating cases involving foreign intelligence surveillance. He was also a staff attorney in the ACLU's Racial Justice Program, litigating cases at the intersection of racial and economic justice. He is currently the executive director of the Criminal Justice Program of Study, Research & Advocacy at Harvard Law School.

Jonathan Zittrain: is the George Bemis Professor of International Law at Harvard Law School and the Harvard Kennedy School of Government, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, and co-founder and Faculty Director of the Berkman Center for Internet & Society. He is a member of the Board of Directors of the Electronic Frontier Foundation and also contributes to the advisory board of the National Security Agency.

Meeting guests have included:

James Baker, Federal Bureau of Investigation

James Burell, Federal Bureau of Investigation

Janice Gardner, Office of the Director of National Intelligence

Melissa Hathaway, Harvard Kennedy School's Belfer Center; Hathaway Global Strategies

Eli Sugarman, William and Flora Hewlett Foundation

Ben Wittes, Lawfare; Brookings Institution

-

- ⁸ Alma Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in Lori Cranor and Simpson Garfinkel, *Security and Usability: Designing Systems that People Can Use* (O'Reilly: Sebastapol, 2005).
- ⁹ In early 2014, more than 600 million individuals worldwide were estimated to use iPhones and more than 1.9 billion individuals were estimated to use phones running Android. *See* Dawiderpal Sahota, "Android Domination to continue in 2014; iPhone loses ground," *Telecoms.com*, January 2014, http://telecoms.com/210391/android-domination-to-continue-in-2014-iphone-loses-ground/.
- ¹⁰ See, e.g., Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," MIT Technology Review, November 24, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark," Lawfare, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark; Jan Willem Aldershoff, "Users shouldn't trust WhatsApp's end-to-end encryption," MYCE.com, May 1, 2015, http://www.myce.com/news/users-shouldnt-trust-on-whatsapps-end-to-end-encryption-75939/.

¹ See Ellen Nakashima and Andrea Peterson, "Obama administration opts not to force firms to decrypt data – for now," *The Washington Post*, October 8, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

² David Sanger, "Signaling Post-Snowden Era, New iPhone Locks Out NSA," *The New York Times*, September 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era.html.

² Apple, Inc., "iOS Security Guide: iOS 8.1 or later," October 2014.

³ Ihid

⁴ Craig Timberg, "Newest Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, September 18, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

⁵ Andy Greenberg, "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," WIRED, November 18, 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

⁶ Alex Stamos, "User-Focused Security: End-to-End Encryption Extension for Yahoo Mail," *Yahoo Blog*, March 15, 2015, http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption.

⁶ Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *The New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.

⁷ See filings related to In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court, No. 15-MC-1902 (EDNY October 9, 2015).

¹¹ For a thorough history, see Whitfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption (MIT Press: Cambridge, 2007).

- ¹² See Ben Adida, Collin Anderson, Annie Anton, et al., "CALEA II: Risks of Wiretap Modifications to Endpoints," (May 17, 2013).
- ¹³ Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *The New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.
- ¹⁴ "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," Before the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, United States House of Representatives, 112th Cong. (2011), http://judiciary.house.gov/_files/hearings/printers/112th/112-59 64581.PDF.
- ¹⁵ Enacted in 1994, CALEA required require telecommunications companies to modify their digital infrastructure so that law enforcement agencies would be able to conduct lawful surveillance activities. Pub. L. 103-414, 108 Stat. 4279 (October 5, 1994) (codified at 47 USC §§ 1001-1010).
- ¹⁶ Federal Bureau of Investigation, Situational Information Report, Cyber Activity Alert, "Going Dark: Law Enforcement Problems in Lawful Surveillance," June 29, 2011, http://info.publicintelligence.net/FBI-GoingDark.pdf.
- ¹⁷ State and local government agencies have also issued reports and statements on the debate. *See*, *e.g.*, "Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety," November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20P ublic%20Safety.pdf.
- ¹⁸ James B. Comey, Federal Bureau of Investigation Director, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech delivered to Brookings Institution, October 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
 ¹⁹ Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, "Encryption and Cyber Security for Mobile Electronic Communication Devices," Encryption Technology and Potential U.S. Policy Responses, Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, April 29, 2015, http://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.
- ²⁰ Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, "Encryption and Cyber Security for Mobile Electronic Communication Devices," Encryption Technology and Potential U.S. Policy Responses, Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, April 29, 2015.
- ²¹ James B. Comey, "Counter Intelligence and the Challenges of Going Dark," Statement Before the Senate Select Committee on Intelligence, July 8, 2015, https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark; https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy; James Comey, "Encryption, Public Safety, and 'Going Dark," *Lawfare*, July 6, 2015, https://www.lawfareblog.com/encryption-public-safety-and-going-dark. *See also* Michael Steinbach, "ISIL in America: Domestic Terror and Radicalization," Statement Before

the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, February 26, 2015, https://www.fbi.gov/news/testimony/isil-in-america-domestic-terror-and-radicalization.

- ²² James B. Comey, Federal Bureau of Investigation Director, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech delivered to Brookings Institution, October 2014.
- ²³ James Comey, Oral Testimony Before the U.S. Senate Committee on the Judiciary, "Oversight of the Federal Bureau of Investigation," December 9, 2015.
- ²⁴ John Reed, "Transcript: NSA Director Mike Rogers vs Yahoo! on Encryption Backdoors," Just Security, February 23, 2015, http://justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/; Nick Gass, "Jeh Johnson warns of post-Snowden encryption frenzy," *Politico*, May 15, 2015, http://www.politico.com/story/2015/05/jeh-johnson-edward-snowden-fallout-117986.html.
- ²⁵ See Damian Paletta, "Paris Attack Reopens U.S. Privacy vs Security Debate," *The Wall Street Journal*, November 16, 2015, http://blogs.wsj.com/washwire/2015/11/16/paris-attack-reopens-u-s-privacy-vs-security-debate/.
- ²⁶ Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear of ubiquitous data encryption is overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.
- ²⁷ James B. Comey, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption," Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, July 8, 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.
- ²⁸ Ellen Nakashima and Andrea Peterson, "Obama administration opts not to force firms to decrypt data for now," *The Washington Post*, October 8, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.
- ²⁹ Cyrus Vance, Fraçois Molins, Adrian Leppard, and Javier Zaragoza, "When Phone Encryption Blocks Justice," *The New York Times*, August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.
- ³⁰ See Rowena Mason, "U.K. spy agencies need more powers, says Cameron," *The Guardian*, January 12, 2015, http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-parisattacks; Rob Price, "The U.K. government insists it's not going to try and ban encryption," *Business Insider*, July 14, 2015, http://www.businessinsider.com/uk-government-not-going-to-ban-encryption-2015-7.
- ³¹ See David Sanger and Nicole Perlroth, "Encrypted Messaging Apps May Face New Scrutiny Over Possible Role in Paris Attacks," The New York Times, November 16, 2015,
- http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html.
- ³² See Paul Mozur, "New Rules in China Upset Western Tech Companies," *The New York Times*, January 28, 2015, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-

companies.html; Zack Whittaker, "E.U wants to force Internet, phone companies to turn over encryption keys," ZDNet, January 22, 2015, http://www.zdnet.com/article/eu-wants-internet-phone-companies-to-hand-overencryption-keys/; Paul Hockenos, "Europe Considers Surveillance Expansion After Deadly Attacks," The Intercept, January 20, 2015, https://firstlook.org/theintercept/2015/01/20/europe-considers-surveillance-expansion/. ³³ To give but a few examples, see Hal Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," Journal of Cybersecurity, Vol.1(1) (2015); Kenneth Dam and Herbert Lin, eds., Cryptography's Role in Securing the Information Society (National Academies Press: Washington, DC, 1996); Hal Abelson, Ross Anderson, et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," (1997); Peter Swire and Kenesa Ahmad, "Encryption and Globalization," 13 Columbia Science & Technology Review 416 (September 2012); Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th Century and the 21st" in Karl De Leeuw and Jan Bergstra (eds.), The History of Information Security (Elsevier, 2007). Technology companies have also joined members of civil society, academics, and security technologists in recent public statements concerning the debate. See Kevin Bankston, "Massive Coalition of Security Experts, Tech Companies and Privacy Advocates Presses Obama to Oppose Surveillance Backdoors," New America Foundation, Open Technology Institute, May 19, 2015, https://www.newamerica.org/oti/massive-coalition-of-security-expertstech-companies-and-privacy-advocates-presses-obama-to-oppose-surveillance-backdoors/.

- ³⁴ Hal Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).
- ³⁵ Maximillian Schrems v. Data Protection Commissioner, C-362/14 (CJEU October 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.
- ³⁶ David Kaye, Human Rights Council, United Nations, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," May 22, 2015. *See also* David Kravets, "U.N. says encryption 'necessary for the exercise of the right to freedom'," *Ars Technica*, May 28, 2015, http://arstechnica.com/tech-policy/2015/05/un-says-encryption-necessary-for-the-exercise-of-the-right-to-freedom/.
- ³⁷ See Peter Swire and Kenesa Ahmad, "Going Dark' Versus a Golden Age of Surveillance," Center for Democracy & Technology, November 28, 2011.
- ³⁸ Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," *MIT Technology Review*, November 24, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.
- ³⁹ See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," 12 Northwestern Journal of Technology and Intellectual Property 1 (April 2014).
- ⁴⁰ See, e.g., Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," MIT Technology Review, November 24, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-

can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.

- ⁴¹ See, e.g., Google, "Showing Gmail ads," https://support.google.com/adwords/answer/6105478.
- ⁴² Facebook, "How to target Facebook Ads," https://www.facebook.com/business/a/online-sales/ad-targeting-details.
- ⁴³ Yahoo, "Advertising," https://advertising.yahoo.com/.
- ⁴⁴ Michael Ambrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
- ⁴⁵ See, e.g., Dropbox, http://dropbox.com/.
- ⁴⁶ See, e.g., Janna Anderson and Lee Rainie, "The future of cloud computing," Pew Research Center, June 11, 2010, http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/.
- ⁴⁷ See Quentin Hardy, "The Era of Cloud Computing," *The New York Times*, June 11, 2014, http://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/.
- ⁴⁸ Apple, "iOS Security," September 2015, https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- ⁴⁹ Nicholas Weaver, "iPhones, the FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.
- ⁵⁰ Zach Miners, "End-to-end encryption needs to be easier for users before Facebook embraces it," *PC World*, March 19, 2014, http://www.pcworld.com/article/2109582/end-to-end-encryption-needs-to-be-easier-for-users-before-facebook-embraces-it.html.
- ⁵¹ Andrew Cunningham, "Google quietly backs away from encrypting new Lollipop devices by default," *Ars Technica*, March 2, 2015, http://arstechnica.com/gadgets/2015/03/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/; Timothy J. Seppala, "Google won't force Android encryption by default," *Engadget*, March 2, 2015, http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/.
- ⁵² Alex Dobie, "Why you'll never have the latest version of Android," *Android Central*, September 6, 2012, http://www.androidcentral.com/why-you-ll-never-have-latest-version-android.
- ⁵³ Android Developer Dashboards, http://developer.android.com/about/dashboards/index.html (visited January 27, 2016).
- ⁵⁴ See, e.g., Anton Troianovski, "Phone Firms Sell Data on Customers," *The Wall Street Journal*, May 21, 2013, http://www.wsj.com/articles/SB10001424127887323463704578497153556847658; Julianne Pepitone, "What your wireless carrier knows about you," *CNN Money*, December 16, 2013,

http://money.cnn.com/2013/12/16/technology/mobile/wireless-carrier-sell-data/; Declan McCullagh, "Verizon draws fire for monitoring app usage, browsing habits," *CNET*, October 16, 2012,

http://www.cnet.com/news/verizon-draws-fire-for-monitoring-app-usage-browsing-habits/.

⁵⁵ McKinsey, "Unlocking the Potential of the Internet of things," June 2015. http://www.mckinsey.com/insights/business_technology/The_Internet_of_Things_The_value_of_digitizing_the_p hysical_world.

- ⁵⁸ See Kelsey Finch and Omer Tene, "Welcome to the Metropicon: Protecting Privacy in a Hyperconnected Town," 41 Fordham Law Review 1581 (October 2014).
- ⁵⁹ See, e.g., "Discover the internet of things," http://iolist.co.

as-service-and-perfect-enforcement/.

- 60 See, e.g., https://aws.amazon.com/iot/; http://www.apple.com/ios/homekit/; https://developers.google.com/brillo/.
- ⁶¹ See David Linthicum, "Thank the cloud for making big data and IoT possible," *InfoWorld*, January 16, 2015, http://www.infoworld.com/article/2867978/cloud-computing/thank-the-cloud-for-making-big-data-and-internet-of-things-possible.html.
- ⁶² The Company v. United States, 349 F.3d 1132 (9th Cir. 2003). See also Adam Liptak, "Court Leaves the Door Open For Safety System Wiretaps," The New York Times, October 21, 2003, http://www.nytimes.com/2003/12/21/automobiles/court-leaves-the-door-open-for-safety-system-wiretaps.html, and Jonathan Zittrain, The Future of the Internet And How to Stop It (2008), "Tethered Appliances, Software as Service, and Perfect Enforcement," http://yupnet.org/zittrain/2008/03/14/chapter-5-tethered-appliances-software-
- ⁶³ There are numerous consumer products including baby monitors, security cameras, and even children's toys with networked sensors that rely telemetry and other data to third-party intermediaries for processing and other purposes. *See*, *e.g.*, "Amazon Echo," http://www.amazon.com/gp/product/B00X4WHP5E/; Nest, "Meet Nest Cam," https://nest.com/camera/meet-nest-cam/; Phillips, "In.Sight Wireless HD Baby Monitor," http://www.usa.philips.com/c-p/B120_37/in.sight-wireless-hd-baby-monitor.
- ⁶⁴ See Shane Harris, "Your Samsung SmartTV Is Spying on You, Basically," *The Daily Beast*, February 5, 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.
- ⁶⁵ Samsung, "Samsung Privacy Policy SmartTV Supplement," http://www.samsung.com/sg/info/privacy/smarttv.html (accessed October 26, 2015).
- ⁶⁶ Samuel Gibbs, "Google eavesdropping tool installed on computers without permission," *The Guardian*, June 23, 2015, http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission.
- ⁶⁷ Ariella Brown, "Smart Barbie Puts Child's Play in the Cloud," *Information Week*, April 5, 2015, http://www.informationweek.com/cloud/smart-barbie-puts-childs-play-in-the-cloud/a/d-id/1319779.
- ⁶⁸ Nest, "Meet Nest Cam," https://nest.com/camera/meet-nest-cam/.

⁵⁶ See McKinsey, "Unlocking the Potential of the Internet of things," June 2015.

⁵⁷ See Janna Anderson and Lee Rainie, "The Internet of Things Will Thrive by 2025," Pew Research Center, March 14, 2014, http://www.pewinternet.org/2014/05/14/internet-of-things/.

Exhibit N

Apple Inc. and Apple Distribution International—written evidence (IPB0093)

- 1. The world today faces security threats from criminals and terrorists who threaten our shared commitment to a peaceful and productive future. Apple has a long history of cooperating with the UK government on a wide range of important issues, and in that tradition, thanks the Committee for the opportunity to share our views on this topic.
- 2. Apple is deeply committed to protecting public safety and shares the Government's determination to combat terrorism and other violent crimes. Strong encryption is vital to protecting innocent people from malicious actors. While the Government has said it does not intend to weaken encryption, its representatives have made clear if, "the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear."
- 3. The fact is to comply with the Government's proposal, the personal data of millions of law-abiding citizens would be less secure.

Summary

- 4. Hundreds of millions of people depend on Apple's products and services. Our customers trust Apple and their Apple devices with some of their most personal information their financial data, health data, family photos, videos and messages.
- 5. Two things have changed in a short period of time: 1) the amount of sensitive information innocent individuals put on their devices; and 2) the sophistication and determination of malicious cyber-attackers. Governments, businesses, and individuals have all been victims, and we've all been surprised by the successful implementation of exploits the experts viewed as still merely theoretical.
- 6. Increasingly sophisticated hacking schemes and cyber-attacks have become the new normal as individuals live more of their lives on their devices and online. Without strong defense, these attacks have the potential to impose chaos, and threaten our way of life, economic stability and infrastructure.
- 7. We owe it to our customers to protect their personal data to the best of our ability. Increasingly stronger not weaker encryption is the best way to protect against these threats.
- 8. The bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks. The creation of backdoors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers. A key left under the doormat would not just be there for the good guys. The bad guys would find it too.

- 9. Encryption today is as ubiquitous as computing itself and we are all the better for it. There are hundreds of products that use encryption to protect user data, many of them open-source and beyond the regulation of any one government. By mandating weakened encryption in Apple products, this bill will put law-abiding citizens at risk, not the criminals, hackers and terrorists who will continue having access to encryption.
- 10. Some would portray this as an all-or-nothing proposition for law enforcement. Nothing could be further from the truth. Law enforcement today has access to more data data which they can use to prevent terrorist attacks, solve crimes and help bring perpetrators to justice than ever before in the history of our world.
- 11. If the UK Government forces these capabilities, there's no assurance they will not be imposed in other places where protections are absent.
- 12. On the pages that follow, our submission will also take exception to the fact the bill would attempt to force non-UK companies to take actions that violate the laws of their home countries. This would immobilize substantial portions of the tech sector and spark serious international conflicts. It would also likely be the catalyst for other countries to enact similar laws, paralyzing multinational corporations under the weight of what could be dozens or hundreds of contradictory country-specific laws.
- 13. Finally, the bill would also force companies to expend considerable resources hacking their own systems at the Government's direction. This mandate would require Apple to alter the design of our systems and could endanger the privacy and security of users in the UK and elsewhere.
- 14. We are committed to doing everything in our power to create a safer and more secure world for our customers. But it is our belief this world cannot come by sacrificing personal security.

Encryption

- 15. Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones. Governments like the United States fund sophisticated encryption technology including some of the best end-to-end encryption apps. Encryption, in short, *protects people*.
- 16. Protecting our customers and earning their trust is fundamental to our business model. At Apple, we've been providing customers easy ways to protect their data with strong encryption in our products and services for well over 10 years. In 2003, we launched FileVault to protect data on a user's Mac. In 2010, with iOS 4, we began to encrypt data on iOS devices to keys derived from a user's passcode. We launched FaceTime in 2010 and iMessage in 2011, both with end-to-end encryption. As users increasingly entrust Apple and their devices with sensitive information, we will continue to deploy strong encryption methods because we firmly believe they're in our customers' best interests, and ultimately

in the best interests of humanity. Our job is to constantly stay 10 steps ahead of the bad guys.

- 17. Some have asserted that, given the expertise of technology companies, they should be able to construct a system that keeps the data of nearly all users secure but still allows the data of very few users to be read covertly when a proper warrant is served. But the Government does not know in advance which individuals will become targets of investigation, so the encryption system necessarily would need to be compromised for everyone.
- 18. The best minds in the world cannot rewrite the laws of mathematics. Any process that weakens the mathematical models that protect user data will by extension weaken the protection. And recent history is littered with cases of attackers successfully implementing exploits that nearly all experts either remained unaware of or viewed as merely theoretical. Every day that companies hold the ability to decrypt their customers' data is more time criminals have to gain that ability. All the while, hacking technology grows more sophisticated. What might have been adequate security for customers two years ago no longer is and that's why we've strengthened our encryption protections.
- 19. Strong encryption does not eliminate Apple's ability to give law enforcement metadata or other categories of data, as outlined in our Law Enforcement Guidelines. The information Apple and other companies provide helps catch criminals and save lives. It is for this reason that UK law enforcement still requests this data from us routinely. Information about our assistance can be found at http://www.apple.com/privacy/government-information-requests/
- 20. We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat. In this rapidly-evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers.

Extraterritoriality

- 21. Apple has been established in Europe for more than 35 years. With the exception of certain limited retail and human resources data, Apple is not established in the UK.
- 22. Under European data protection law, Apple Distribution International established in Cork, Ireland and iTunes S.à.r.l. established in Luxembourg have data controller responsibility for Apple and iTunes user personal data of users located in the EEA and Switzerland.
- 23. We take this responsibility very seriously and face sanction from data protection authorities and/or user litigation if we fail to meet those requirements. Additionally, user content is stored in the United States, and US law controls access to that data by law enforcement. Failure on the part of any relevant US entity to follow those requirements gives rise to criminal and civil liability. Most relevant, Title III of the US Omnibus Crime

Control and Safe Streets Act would subject Apple to criminal sanctions for any unauthorized interception of content in transit.

- 24. As defined in relevant EU Telecommunications Law, Apple is not an electronic communications service provider. The Investigatory Powers Bill seeks to extend definitions in this area to an extent beyond that provided for in relevant EU law.
- 25. The draft bill makes explicit its reach beyond UK borders to, in effect, any service provider with a connection to UK consumers. In short, we believe this will lead to major issues for businesses and could ultimately put UK users at greater risk.
- 26. The first problem with asserting such extraterritorial powers is that there will remain a proportion of service providers which will never assist British law enforcement regardless of threatened sanction because they are underground or in jurisdictions unfriendly to British interests. It is to these providers that dangerous people will gravitate.
- 27. Even leaving that aside, the implications for companies such as Apple who do assist law enforcement will be profound. As well as complying with local law in the countries where we are established for the provision of our services, we will have to attempt to overlay compliance with UK law. On their face, those laws would not be in harmony. Further, we know that the IP bill process is being watched closely by other countries. If the UK asserts jurisdiction over Irish or American businesses, other states will too.
- 28. Those businesses affected will have to cope with a set of overlapping foreign and domestic laws. When these laws inevitably conflict, the businesses will be left having to arbitrate between them, knowing that in doing so they might risk sanctions. That is an unreasonable position to be placed in.
- 29. The Government has partly addressed this by providing a defense for businesses who cannot comply with a warrant because of local laws (although not in all parts of the bill see below). However, once a third jurisdiction is overlaid (home country, UK and one other), the situation soon becomes very difficult for businesses to negotiate.
- 30. This will not just be an issue for companies like Apple: any British business with customers overseas might be faced with having to comply with a warrant from a foreign jurisdiction which poses it ethical problems, or impinges on the privacy of British consumers.
- 31. Clearly this situation could arise regardless of whatever legislation is passed in the UK. But Parliament will be leading the way with this bill and needs to carefully consider the precedent it sets.

Equipment Interference

32. We believe the UK is the first national Government to attempt to provide a legislative basis for equipment interference. Consumer trust in the public and private sectors can benefit from a more concrete understanding of the framework in which these activities can take place. However, it could at the same time be undermined by a blurring of the

boundaries of responsibilities, and the bill as it stands seems to threaten to extend responsibility for hacking from Government to the private sector.

- 33. It would place businesses like Apple whose relationship with customers is in part built on a sense of trust about how data will be handled in a very difficult position. For the consumer in, say, Germany, this might represent hacking of their data by an Irish business on behalf of the UK state under a bulk warrant activity which the provider is not even allowed to confirm or deny. Maintaining trust in such circumstances will be extremely difficult.
- 34. For these reasons, we believe there is a need for much greater clarity as to how the powers in the bill will be applied, not least because, once again, the extension of the powers to overseas providers will set a precedent which, if followed by other countries, could endanger the privacy and security of users in the UK and elsewhere.

Specific Comments on Clauses

Clauses 189, 190 and 191

- 35. These clauses govern the Secretary of State's ability to require businesses to establish a technical capability to comply with warrants.
- 36. Paragraphs (1) to (5) of Clause 189 would authorize the Secretary of State to make regulations imposing specified obligations on an operator. Paragraph (4) states that those obligations could include ones "relating to the removal of electronic protection applied by a relevant operator to any communications or data" in other words, the removal of encryption.
- 37. As set out above, we believe there are significant risks to applying this power to encryption and to extending this power to overseas providers. We therefore do not believe the clause should be retained in its current form and certainly should not extend outside the UK.
- 38. However, this power could have a very profound effect on any business to whom the clauses apply, and the details are worth examining.
- 39. First, the oversight seems less rigorous than other parts of the bill. There is no judicial authorization of the requirements placed on businesses. There is no protection for businesses who cannot comply because of local laws.
- 40. Second, the system does not allow for a full weighing of the costs of compliance. While the clauses require some assessment of compliance cost, it is not clear how this would be calculated. Even if a consensus could be reached on the number of working hours and computing power needed to comply, a proper consideration would need to include the opportunity cost as other projects were put on hold, the knock-on effects for other services and the change in the customer relationship.

- 41. Third, because (as we explain above) any reduction in encryption in the UK will be exploited by regimes and bad actors not subject to the same privacy and civil liberties protections as UK law enforcement, the implications of a Notice under these clauses would go way beyond either the UK or the affected business. The bill at present does not require any consideration of this.
- 42. Fourth, there is no explicit obligation for the requirements on a business to be proportionate. Our reading of the bill is that although the Secretary of State might be required to take into account the benefits, costs and technical feasibility of the notice, and consult the Technical Advisory Board and (in the case of review) the Investigatory Powers Commissioner, it is at best implicit that she must only impose requirements that are proportionate. If there is a review, the bill requires that the Investigatory Powers Commissioner must consider whether the notice is proportionate, but the Secretary of State could still reject this advice.
- 43. The overall effect is a wide ranging power for the Secretary of State to demand a business remove encryption based on an insufficiently robust process and without regard to the full effects, leaving the business with no effective means of appeal.

44. Suggested amendments:

The steps required of a business by a Notice should not include removal of electronic protection.

These powers should not extend to overseas businesses; a conflict of laws exemption should be added.

A notice under s189 should require judicial authorization.

There should be clear and concise definitions for the following terms: "removal of electronic protection", "technical feasibility" and "reasonably practicable". These are key terms that should not be left in the first instance for argument in court. Parliament should define and agree what their intent is.

The criteria by which the assessment is made by the Secretary of State should be made much more explicit.

The Technical Advisory Board advice should be made available to the affected business, and in the case of a review under clause 191, the Interception Commissioner's advice as well.

Before imposing any requirement under s189, the Secretary of State should consider whether the time spent in complying, cost (including opportunity cost), knock-on effects and change in customer relationships are reasonable and proportionate to the expected benefits.

The Secretary of State should also be obliged to consider the impact of a notice on human rights, in the UK and globally.

The Secretary of State should be required only to apply notices that are proportionate as advised by the Commissioner.

- 45. Paragraph (1) of Clause 188 would authorize the Secretary of State to give any telecommunications operator in the UK a national security notice directing the operator to take such steps as the Secretary of State considers necessary in the interests of national security. 188(4) precludes the powers under this clause being used as a shortcut if powers exist elsewhere in the bill.
- 46. While we take the strong view that this bill should not be used to demand the removal of encryption, we would not want to see that clarified only for a catch-all Clause 188 to allow the Secretary of State to demand it unilaterally.

47. Suggested amendment:

The Clause should be amended to clarify that it cannot be used to require businesses to remove electronic protection from their products or services.

Clause 31

- 48. This clause places a duty on an operator to comply with a warrant. Again, in line with our argument above, we continue to believe the duty should not be applied to overseas businesses, but have some more general comments on the clause.
- 49. Clause 31 would require a relevant operator to take all reasonably practicable steps for giving effect to a warrant. Although this is not explicit in the draft bill, our understanding of the government's intention is that this would require us to remove end to end encryption if that was necessary to give effect to the warrant and considered proportionate. The Home Office indicated exactly this in the evidence to your committee we quoted above.
- 50. In other words, the bill as it stands means that whether or not the Secretary of State has served a business with a Clause189 order requiring it to remove electronic protection, a fresh warrant could be served on a business requiring them to provide data in the clear, backed up by the threat of imprisonment. This seems to represent a short cut for the Secretary of State to insist on removal of encryption but of course compliance with a warrant in the timescale required by a criminal investigation is likely to be impossible.

51. Suggested amendments:

This Clause should not apply to overseas providers.

The Clause should be amended to make clear that 'reasonably practicable steps' cannot include removal of electronic protection unless dealt with separately under a Notice under Clause 189, subject to the amendments to that Clause we suggest above

The definition of 'reasonably practicable steps' should be clarified as we set out above to distinguish it from 'technical feasibility.'

Clauses 81 and 135

52. These clauses deal with targeted and bulk equipment interference warrants.

- 53. We are concerned about the way in which the bill could make private companies implicated in the hacking of their customers.
- 54. Clause 81(2) provides that a warrant can be served on a person to require them to assist in hacking.
- 55. Is the intention that persons receiving a warrant would knowingly let the security services break into their equipment or services or allow them to use that equipment to break into equipment used by a third party? Or does the envisaged power go even further and require persons in receipt of a warrant to actively assist in the interference of their own equipment and services?
- 56. These questions become even more pressing when applied to bulk equipment interference warrants. It is extremely difficult to imagine circumstances in which this could be justified, so we believe the bill must spell out in more detail the types of activities required of communications providers and the circumstances in which they are expected to carry them out. Additionally and in line with earlier comments, these clauses should not have extra-territorial effect.

57. Suggested amendments:

The powers in this part of the bill need to be fully understood as to their intent. The bill should set out in much more detail what the requirement on a person served with a warrant will be.

The clauses should not apply to overseas providers who would be put in an impossible conflict of laws position.

21 December 2015

Exhibit O

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 <u>op-ed</u> 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

or deaf. Case 5:16-cm-00010-SP Document 16-16 Filed 02/25/16 Page 4 of 4 Page ID #:300

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 P

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.

Proposal seeks to fine tech companies for noncompliance with wiretap orders - The Wash... Page 2 of 5 Case 5:16-cm-00010-SP Document 16-17 Filed 02/25/16 Page 3 of 6 Page ID #:303

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."

Proposal seeks to fine tech companies for noncompliance with wiretap orders - The Wash... Page 3 of 5 Case 5:16-cm-00010-SP Document 16-17 Filed 02/25/16 Page 4 of 6 Page ID #:304

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-toend 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.

Proposal seeks to fine tech companies for noncompliance with wiretap orders - The Wash... Page 4 of 5 Case 5:16-cm-00010-SP Document 16-17 Filed 02/25/16 Page 5 of 6 Page ID #:305

"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 <u>lost some of its cachet</u> 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.

Proposal seeks to fine tech companies for noncompliance with wiretap orders - The Wash... Page 5 of 5

Case 5:16-cm-00010-SP Document 16-17 Filed 02/25/16 Page 6 of 6 Page ID #:306

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 Q

President Barack Obama The White House 1600 Pennsylvania Avenue NW Washington, DC 20500

May 19, 2015

Dear President Obama,

We the undersigned represent a wide variety of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online, as well as technology companies, trade associations, and security and policy experts. We are writing today to respond to recent statements by some Administration officials regarding the deployment of strong encryption technology in the devices and services offered by the U.S. technology industry. Those officials have suggested that American companies should refrain from providing any products that are secured by encryption, unless those companies also weaken their security in order to maintain the capability to decrypt their customers' data at the government's request. Some officials have gone so far as to suggest that Congress should act to ban such products or mandate such capabilities.

We urge you to reject any proposal that U.S. companies deliberately weaken the security of their products. We request that the White House instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology. Such policies will in turn help to promote and protect cybersecurity, economic growth, and human rights, both here and abroad.

Strong encryption is the cornerstone of the modern information economy's security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, repressive governments trying to stifle dissent, or foreign intelligence agencies trying to compromise our and our allies' most sensitive national security secrets.

Encryption thereby protects us from innumerable criminal and national security threats. This protection would be undermined by the mandatory insertion of any new vulnerabilities into encrypted devices and services. Whether you call them "front doors" or "back doors", introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government's own experts.

In addition to undermining cybersecurity, any kind of vulnerability mandate would also seriously undermine our economic security. U.S. companies are already struggling to maintain international trust in the wake of revelations about the National Security Agency's surveillance programs. Introducing mandatory vulnerabilities into American products would further push many customers—be they domestic or international,

individual or institutional—to turn away from those compromised products and services. Instead, they—and many of the bad actors whose behavior the government is hoping to impact—will simply rely on encrypted offerings from foreign providers, or avail themselves of the wide range of free and open source encryption products that are easily available online.

More than undermining every American's cybersecurity and the nation's economic security, introducing new vulnerabilities to weaken encrypted products in the U.S. would also undermine human rights and information security around the globe. If American companies maintain the ability to unlock their customers' data and devices on request, governments other than the United States will demand the same access, and will also be emboldened to demand the same capability from their native companies. The U.S. government, having made the same demands, will have little room to object. The result will be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes. That's not a future that the American people or the people of the world deserve.

The Administration faces a critical choice: will it adopt policies that foster a global digital ecosystem that is more secure, or less? That choice may well define the future of the Internet in the 21st century. When faced with a similar choice at the end of the last century, during the so-called "Crypto Wars", U.S. policymakers weighed many of the same concerns and arguments that have been raised in the current debate, and correctly concluded that the serious costs of undermining encryption technology outweighed the purported benefits. So too did the President's Review Group on Intelligence and Communications Technologies, who unanimously recommended in their December 2013 report that the US Government should "(1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

We urge the Administration to follow the Review Group's recommendation and adopt policies that promote rather than undermine the widespread adoption of strong encryption technologies, and by doing so help lead the way to a more secure, prosperous, and rights-respecting future for America and for the world.

Thank you,

Civil Society Organizations

Access
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee (ADC)
American Civil Liberties Union
American Library Association
Benetech
Bill of Rights Defense Committee

Center for Democracy & Technology

Committee to Protect Journalists

The Constitution Project

Constitutional Alliance

Council on American-Islamic Relations

Demand Progress

Defending Dissent Foundation

DownsizeDC.org, Inc.

Electronic Frontier Foundation

Electronic Privacy Information Center (EPIC)

Engine

Fight for the Future

Free Press

Free Software Foundation

Freedom of the Press Foundation

GNOME Foundation

Human Rights Watch

The Media Consortium

New America's Open Technology Institute

Niskanen Center

Open Source Initiative

PEN American Center

Project Censored/Media Freedom Foundation

R Street

Reporters Committee for Freedom of the Press

TechFreedom

The Tor Project

U.S. Public Policy Council of Association for Computing Machinery

World Privacy Forum

X-Lab

Companies & Trade Associations

ACT | The App Association

Adobe

Apple Inc.

The Application Developers Alliance

Automattic

Blockstream

Cisco Systems

Coinbase

Cloud Linux Inc.

CloudFlare

Computer & Communications Industry Association

Consumer Electronics Association (CEA)

Context Relevant

The Copia Institute

CREDO Mobile

Data Foundry

Dropbox

Evernote

Facebook

Gandi.net

Golden Frog

Google

HackerOne

Hackers/Founders

Hewlett-Packard Company

Internet Archive

Internet Association

Internet Infrastructure Coalition (i2Coalition)

Level 3 Communications

LinkedIn

Microsoft

Misk.com

Mozilla

Open Spectrum Inc.

Rackspace

Rapid7

Reform Government Surveillance

Sonic

ServInt

Silent Circle

Slack Technologies, Inc.

Symantec

Tech Assets Inc.

TechNet

Tumblr

Twitter

Wikimedia Foundation

Yahoo

Security and Policy Experts*

Hal Abelson, Professor of Computer Science and Engineering, Massachusetts Institute of Technology

Ben Adida, VP Engineering, Clever Inc.

Jacob Appelbaum, The Tor Project

Adam Back, PhD, Inventor, HashCash, Co-Founder & President, Blockstream

Alvaro Bedoya, Executive Director, Center on Privacy & Technology at Georgetown Law

Brian Behlendorf, Open Source software pioneer

Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University

Matt Bishop, Professor of Computer Science, University of California at Davis

Matthew Blaze, Director, Distributed Systems Laboratory, University of Pennsylvania

Dan Boneh, Professor of Computer Science and Electrical Engineering at Stanford University

Eric Burger, Research Professor of Computer Science and Director, Security and Software Engineering Research Center (Georgetown), Georgetown University Jon Callas, CTO, Silent Circle

L. Jean Camp, Professor of Informatics, Indiana University

Richard A. Clarke, Chairman, Good Harbor Security Risk Management

Gabriella Coleman, Wolfe Chair in Scientific and Technological Literacy, McGill University

Whitfield Diffie, Dr. sc. techn., Center for International Security and Cooperation, Stanford University

David Evans, Professor of Computer Science, University of Virginia

David J. Farber, Alfred Filter Moore Professor Emeritus of Telecommunications, University of Pennsylvania

Dan Farmer, Security Consultant and Researcher, Vicious Fishes Consulting

Rik Farrow, Internet Security

Joan Feigenbaum, Department Chair and Grace Murray Hopper Professor of Computer Science Yale University

Richard Forno, Jr. Affiliate Scholar, Stanford Law School Center for Internet and Society

Alex Fowler, Co-Founder & SVP, Blockstream

Jim Fruchterman, Founder and CEO, Benetech

Daniel Kahn Gillmor, ACLU Staff Technologist

Robert Graham, creator of BlackICE, sidejacking, and masscan

Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society

Matthew D. Green, Assistant Research Professor, Johns Hopkins University Information Security Institute

Robert Hansen. Vice President of Labs at WhiteHat Security

Lance Hoffman, Director, George Washington University, Cyber Security Policy and Research Institute

Marcia Hofmann, Law Office of Marcia Hofmann

Nadim Kobeissi, PhD Researcher, INRIA

Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology

Nadia Heninger, Assistant Professor, Department of Computer and Information Science, University of Pennsylvania

David S. Isenberg, Producer, Freedom 2 Connect

Douglas W. Jones, Department of Computer Science, University of Iowa

Susan Landau, Worcester Polytechnic Institute

Gordon Fyodor Lyon, Founder, Nmap Security Scanner Project

Aaron Massey, Postdoctoral Fellow, School of Interactive Computing, Georgia Institute of Technology

Jonathan Mayer, Graduate Fellow, Stanford University

Jeff Moss, Founder, DEF CON and Black Hat security conferences

Peter G. Neumann, Senior Principal Scientist, SRI International Computer Science Lab, Moderator of the ACM Risks Forum

Ken Pfeil, former CISO at Pioneer Investments

Ronald L. Rivest, Vannevar Bush Professor, Massachusetts Institute of Technology

Paul Rosenzweig, Professorial Lecturer in Law, George Washington University School of Law

Jeffrey I. Schiller, Area Director for Security, Internet Engineering Task Force (1994-2003), Massachusetts Institute of Technology

Bruce Schneier, Fellow, Berkman Center for Internet and Society, Harvard Law School

Micah Sherr, Assistant Professor of Computer Science, Georgetown University

Adam Shostack, author, "Threat Modeling: Designing for Security"

Eugene H. Spafford, CERIAS Executive Director, Purdue University

Alex Stamos, CISO, Yahoo

Geoffrey R. Stone, Edward H. Levi Distinguished Service Professor of Law, The University of Chicago

Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology

C. Thomas (Space Rogue), Security Strategist, Tenable Network Security

Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute of Public Policy

Nicholas Weaver, Researcher, International Computer Science Institute

Chris Wysopal, Co-Founder and CTO, Veracode, Inc.

Philip Zimmermann, Chief Scientist and Co-Founder, Silent Circle

^{*}Affiliations provided only for identification purposes.

Exhibit R

Home » News

Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption

FEB 18, 2016 Issues: Civil Justice, Government Oversight

Washington, D.C.—Earlier this week, through a court order, the United States government demanded that Apple Inc. help the Federal Bureau of Investigation (FBI) develop software in an effort to break the encryption on an iPhone that was recovered after the recent shootings in San Bernardino, California. The government cited the "All Writs Act," enacted in 1789, to demand that the technology company create a new version of the iPhone operating system to circumvent several security features on the device. Apple has five days to respond to the court's order. The House Judiciary Committee will hold an oversight hearing on the encryption debate on March 1.

Senior Democratic Members of the House Judiciary Committee, Reps. Conyers, Nadler, Lofgren and Jackson Lee, released the following statement in response:

"The terrorist attack in San Bernardino was a tragic event. We agree that heightened vigilance is necessary to combat the threat of home grown extremism in all of its forms. In this effort, we commit our full support to law enforcement agencies at the local, state, and federal levels and hope to

provide them with the resources and tools they require to perform their jobs.

"But there is little reason for the government to make this demand on Apple—except to enact a policy proposal that has gained no traction in Congress and was <u>rejected by the White House</u>.

"Properly understood, strong encryption is our best defense against online criminals—including terrorist organizations. It is the backbone of the Internet economy and vital for the protection of both free expression and privacy. The government's demand on Apple would coerce a private U.S. company to hack its own device, threatening the trust of millions of customers and placing our technology industry at a significant disadvantage abroad.

"In a September 2015 article, the <u>Washington Post</u> cited an email from a top intelligence community official which stated: 'the legislative environment is very hostile today . . . it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement.' We are concerned that the heartbreaking event in San Bernardino is being exploited to undertake an end-run around the legislative process in just this fashion."

Exhibit S

Home • News • Testimony • Threats to the Homeland



James B. Comey Director Federal Bureau of Investigation

Statement Before the Senate Committee on Homeland Security and Governmental Affairs Washington, D.C.

October 08, 2015

Good afternoon Chairman Johnson, Ranking Member Carper, and members of the committee. Thank you for the opportunity to appear before you today to discuss the current threats to the homeland and our efforts to address new challenges, including terrorists' use of technology to communicate—both to inspire and recruit. The widespread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the homeland or abroad. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our federal, state, local, and international partnerships. Our successes depend on interagency cooperation. We work closely with our partners within the Department of Homeland Security and the National Counterterrorism Center to address current and emerging threats.

Counterterrorism

Counterterrorism remains the FBI's top priority, however, the threat has changed in two significant ways. First, the core al Qaeda tumor has been reduced, but the cancer has metastasized. The progeny of al Qaeda—including AQAP, al Qaeda in the Islamic Maghreb, and the Islamic State of Iraq and the Levant (ISIL)—have become our focus

Secondly, we are confronting the explosion of terrorist propaganda and training on the Internet. It is no longer necessary to get a terrorist operative into the United States to recruit. Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they can't travel, they motivate them to act at home. This is a significant change from a decade ago.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI and the Intelligence Community as a

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. We estimate approximately 250 Americans have traveled or attempted to travel to Syria to participate in the conflict. While this number is lower in comparison to many of our international partners, we closely analyze and assess the influence groups like ISIL have on individuals located in the United States who are inspired to commit acts of violence. Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the United States and U.S. persons.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al Qaeda or other foreign terrorist organizations, ISIL has persistently used the Internet to communicate. From a homeland perspective, it is ISIL's widespread reach through the Internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life—from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred when an individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

There is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise—the inspired youth. We've seen certain children and young adults drawing deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks.

Recent Testimonies

12.09.15 Law Enforcement Implications of Illegal Online Gambling

Joseph S. Campbell, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Statement Before the House Committee on Oversight and Government Reform, Washington, D.C.

12.09.15 Oversight of the Federal Bureau of Investigation

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Washington, D.C.

10.22.15 Oversight of the Federal Bureau of Investigation

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the House Judiciary Committee, Washington, D.C.

10.21.15 Worldwide Threats and Homeland Security Challenges

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the House Committee on Homeland Security, Washington, D.C.

10.08.15 Threats to the Homeland

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C.

08.05.15 Inspector General Access

Kevin L. Perkins, Associate Deputy Director, Federal Bureau of Investigation, Joint Statement with Department of Justice Associate Deputy Attorney General Carlos Uriarte Before the Senate Judiciary Committee, Washington, D.C.

07.08.15 Counterterrorism, Counterintelligence, and the Challenges of Going Dark

James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Select Committee on Intelligence, Washington, D.C.

07.08.15 Going Dark: Encryption, Technology, and the Balances Between Public Safety ...

James B. Comey, Director, Federal Bureau of Investigation, Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, Washington, D.C.

06.18.15 FBI's Plans for the Use of Rapid DNA Technology in CODIS

Amy S. Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Washington, D.C.

06.03.15 Terrorism Gone Viral: The Attack in Garland, Texas and Beyond

Michael B. Steinbach, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, Statement Before the House Homeland Security Committee, Washington, D.C.

More

Case 5:16-cm-00010-SP Document 16-20 Filed 02/25/16 Page 3 of 4 Page ID #:319

Following other groups, ISIL has advocated for lone offender attacks. In recent months ISIL released a video, via social media, reiterating the group's encouragement of lone offender attacks in Western countries, specifically advocating for attacks against soldiers and law enforcement, intelligence community members, and government personnel. Several incidents have occurred in the United States and Europe over the last few months that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

In one case, a New York-based male was arrested in September after he systematically attempted to travel to the Middle East to join ISIL. The individual, who was inspired by ISIL propaganda, expressed his support for ISIL online and took steps to carry out acts encouraged in the ISIL call to arms.

The targeting of U.S. military personnel is also evident with the release of names of individuals serving in the U.S. military by ISIL supporters. The names continue to be posted to the Internet and quickly spread through social media, depicting ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

Social media has allowed groups, such as ISIL, to use the Internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

In other examples of arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland.

We live in a technologically driven society, and just as private industry has adapted to modern forms of communication, so, too, have terrorists. Unfortunately, changing forms of Internet communication and the use of encryption are posing real challenges to the FBI's ability to fulfill its public safety and national security missions. This real and growing gap, to which the FBI refers as "Going Dark," is an area of continuing focus for the FBI; we believe it must be addressed given the resulting risks are grave both in both traditional criminal matters as well as in national security matters. The United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time.

The FBI is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage robust information sharing; in partnership with our many federal, state, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the homeland.

Intelligence

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken two steps to improve this integration. First, we have established an Intelligence Branch within the FBI headed by an executive assistant director (EAD). The EAD looks across the entire enterprise and drives integration. Second, we now have special agents and new intelligence analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better prepared to work well together in the field. Our goal every day is to get better at using, collecting and sharing intelligence to better understand and defeat our adversaries.

The FBI cannot be content to just work what is directly in front of us. We must also be able to understand the threats we face at home and abroad and how those threats may be connected. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps in what we know about these threats. We then seek to fill those gaps and learn as much as we can about the threats we are addressing and others on the threat landscape. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to organize threats into priority for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

Cybei

An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to strike our critical infrastructure and to harm our economy.

We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. For example, as the committee is aware, the Office of Personnel Management (OPM) discovered earlier this year that a number of its systems were compromised. These systems included those that contain information related to the background Case 5:16-cm-00010-SP Document 16-20 Filed 02/25/16 Page 4 of 4 Page ID #:320

individuals for whom a federal background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques—such as sources, court-authorized electronic surveillance, physical surveillance, and forensics—to fight cyber threats. We are working side-by-side with our federal, state, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF), which serves as a coordination, integration, and information sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations. Through CyWatch, our 24-hour cyber command center, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

* * *

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States from all of those threats and the men and women of the Bureau continue to meet—and exceed—those expectations, every day. I want to thank them for their dedication and their service.

Chairman Johnson, Ranking Member Carper, and committee members, I thank you for the opportunity to testify concerning the threats to the homeland and terrorists' use of the Internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the homeland, and the impact of the Going Dark problem on mitigating their efforts. I am happy to answer any questions you might have.

Accessibility | eRulemaking | Freedom of Information Act | Legal Notices | Legal Policies and Disclaimers | Links | Privacy Policy | USA.gov | White House FBI.gov is an official site of the U.S. government, U.S. Department of Justice

Close

Exhibit T





News Blog

Home • News • News Blog • Director Discusses Encryption, Patriot Act Provisions

May 20, 2015 04:45 PM

Director Discusses Encryption, Patriot Act Provisions



FBI Director James Comey discusses cyber threats with interviewer Benjamin Powell at the Cybersecurity Law Institute at Georgetown Law Center on May 20, 2015.

FBI Director James Comey spoke to legal professionals and scholars this week about cyber threats and the FBI's abilities to counter and investigate those evolving threats.

In remarks at the American Law Institute on Tuesday and at a cyber security summit on Wednesday at Georgetown University Law Center, Comey said the group calling itself the Islamic State, or ISIL, represents the FBI's most urgent threat. He described the organization's use of social media to motivate troubled people in the United States to engage in acts of violence—either by traveling to the so-called caliphate or killing where they are. Comey said ISIL reaches out to individuals on Twitter and elsewhere, then moves their more sensitive communications to encrypted platforms.

"The threat we face has morphed," Comey said on Wednesday. "It's a chaotic spider web through social media—increasingly invisible to us because the operational communications are happening in an encrypted channel."

Comey later elaborated on the issue of encryption, which is a process of encoding messages—on mobile phones for example—that only authorized parties can access. While it can be effective at thwarting digital thieves, strong encryption also limits the amount of information—or evidence—that law enforcement can effectively gather from a device.

"Increasingly we're finding ourselves unable to read what we find, or unable to open a device," Comey said, "and that is a serious concern."

The issue of "going dark," as the Bureau calls it, is worthy of a larger public conversation about the balance between privacy and public safety, Comey said. Momentum toward universal encryption, he explained, may have unintended consequences.

"As all of our lives become digital, the logic of encryption is all of our lives will be covered by strong encryption, and therefore all of our lives—including the lives of criminals and terrorists and spies—will be in a place that is utterly unavailable to court-ordered process," he said. "And that, I think, to a democracy should be very, very concerning."

The Director also pointed to provisions of the Patriot Act of 2001 that, if allowed to expire on June 1, could hobble the FBI's investigative abilities. One of the provisions is Section 215, which authorized the National Security Agency's database of telephony records and metadata.

Comey said the FBI relies on that provision fewer than 200 times a year—in particular cases to get particular records. "If we lose that authority," Comey said, "we can't get information that I think everybody wants us to attain."

Two other provisions include:

■ Poving wiretane. The FRI has had authority since the 1080s to use legally authorized roving

More News & Information

- Field Press Releases

- Stories

- National Press Releases

- Testimony

- Photo Gallery

- Speeches

- Podcasts & Radio Shows

- Video

News by Subject

- Terrorism

- Foreign Counterintelligence

- Organized Crime - White-Collar Crime

Cubo

- Cyber

- Major Thefts/

- Public Corruption

Violent Crime

- Civil Rights

- More

Connect & Subscribe



Facebook



YouTube



Twitter



iTunes



E-mail Updates



News Feeds



Case 5:16-cm-00010-SP Document 16-21 Filed 02/25/16 Page 3 of 3 Page ID #:323

- wiretaps in criminal cases—allowing authorities to follow surveillance targets rather than their phones, which can be easily trashed and replaced. The Patriot Act extended that authority to terrorism and counterintelligence cases.
- The Lone Wolf provision. In 2004, Congress amended the Foreign Intelligence Surveillance Act to authorize intelligence gathering on individuals not affiliated with any known terrorist organization.

"These three are going to go away June 1," Comey said, "and I don't want them to get lost in the conversation about metadata."

 $Accessibility \mid eRule making \mid Freedom \ of \ Information \ Act \mid Legal \ Notices \mid Legal \ Policies \ and \ Disclaimers \mid Links \mid Privacy \ Policy \mid USA.gov \mid White \ House \ FBI.gov \ is \ an official \ site of the U.S. \ government, U.S. \ Department \ of \ Justice \$

Close

Exhibit U



LAW

< It's Not Just The iPhone Law Enforcement Wants To Unlock

Updated February 22, 2016 · 1:50 PM ET Published February 21, 2016 · 7:57 AM ET

RACHEL MARTIN, HOST:

We've been hearing a lot about the tension right now between privacy rights and law enforcement's need for information to solve crimes. All of this stems from last year's massacre in San Bernardino. On one side, you have the FBI that wants access to the data on one of the shooter's iPhones. On the other side, you have Apple, which says if it develops the software needed to unlock that phone, it will set a dangerous precedent. We're going to hear one legal perspective on this issue now. Cyrus Vance Jr. is a Manhattan district attorney. He joins me on the line. Thanks so much for being with us.

CYRUS VANCE JR.: Good morning, Rachel.

MARTIN: You believe Apple should comply with the court order from the federal government and build the technology needed to open this particular phone. Can you summarize your argument for me?

VANCE: Sure, Rachel. The thing that I believe folks need to understand is that criminals are using their smartphone devices to communicate with each other, to store information about their crimes on their phones. Our inability, as a result of Apple's engineering its phones to make it impossible for them to use a digital key to open a phone, has left us in a place where we are simply unable to perform our function to protect the public.

MARTIN: So you're saying this is bigger than just this one case, that this is a problem you run up against all the time.

VANCE: In fact, Rachel, it's a problem that affects us more than actually I believe it affects the federal government. We started tracking the number of iOS 8 devices that we cannot access as a result of Apple's decision in late 2014. And over that year-and-a-half time period, there are now 175 phones that we cannot access out of a universe of 670 phones that our cyber lab has evaluated. So it's about a quarter of the phones we haven't been able to get into. And...

MARTIN: And what does that mean for those cases? I mean, have you been able to circumvent this in the case and find other ways to prosecute?

VANCE: It varies. In some cases, we can't move at all. We can't establish liability or responsibility because we can't access the phone. In others, it's affecting our ability to gather all the evidence that's needed to make sure that we are making the right judgments. And I think it's very important for people to understand that a prosecutor's job is to investigate, get all the information and then make the right judgment as to whether or not we can go forward. It's also our responsibility to make sure that we are prosecuting the right people. And when we don't have access to digital devices, we don't have all the information that we need to make the best judgment as to how the case should be handled.

MARTIN: So how would this look in practice? I mean, what ideally do you want Apple to do? I mean...

VANCE: What I want to do is something very simple. At the end of 2014, Apple required warrants issued by judges to access evidence on phones that it manufactured. It was not a problem at the time. I honestly don't think it is a problem today. And I think Apple should be directed to be able to unlock its phones when there is a court order by an independent judge proving and demonstrating that there's relevant evidence on that phone necessary for an individual case. Secondly, I think that the United States Congress is going to have to step in here. The importance of accessing digital evidence in criminal cases, from terrorism to sex crimes, is very significant. I

think also, Rachel, that from my perspective, this is also very much about corporate responsibility. Apple and Google are huge companies who own 96.7 percent of the worldwide smartphone market. We know communications exist on these phones, are being used by the criminals to perpetrate the crimes. And that's a fact. Given that that is a fact, I believe these companies have to acknowledge that and strike a balance between public safety and privacy that is not on one extreme or the other. Right now, they have independently struck a balance between privacy and public safety at that point on the spectrum where it coincides perfectly with their economic interests. We need to look at this with independent eyes. And I believe Congress ultimately is going to have to make the judgment call of where we draw that line.

MARTIN: Cyrus Vance Jr., Manhattan district attorney. Thanks so much for talking with us.

VANCE: Rachel, thank you very much.

Copyright © 2016 NPR. All rights reserved. Visit our website terms of use and permissions pages at www.npr.org for further information.

NPR transcripts are created on a rush deadline by a contractor for NPR, and accuracy and availability may vary. This text may not be in its final form and may be updated or revised in the future. Please be aware that the authoritative record of NPR's programming is the audio.

© 2016 npr

Exhibit V





Briefing Room

Your Weekly Address

Speeches & Remarks

Press Briefings

Statements & Releases

White House Schedule

Presidential Actions

Executive Orders

Presidential Memoranda

Proclamations

Legislation

Pending Legislation

Signed Legislation

Vetoed Legislation

Nominations & Appointments

<u>Disclosures</u>

The White House

Office of the Press Secretary

For Immediate Release

January 16, 2015

SHARE THIS:

Remarks by President Obama and Prime Minister Cameron of the United







Kingdom in Joint Press Conference

East Room

12:37 P.M. EST

PRESIDENT OBAMA: Good afternoon, everybody. This month marks a notable anniversary -- 200 years since the Battle of New Orleans. Here in America, we call it a great victory over a mighty United Kingdom. Our British friends call it a technicality. The treaty ending the war was signed weeks before.

Either way, we've long since made up. On this 200th anniversary of a great American victory, we count the United Kingdom as one of our greatest friends and strongest allies. And today it's a great pleasure to welcome Prime Minister David Cameron back to the White House.

Now, as many of you know, David recently noted how comfortable the two of us are working together. This sent some commentators into a tizzy. Some explored the linguistic origins of the word "bro." Others debated its definition. Several analyzed how this term has evolved over time. Some seemed confused and asked -- what does Obama mean?

And so, let me to put this speculation to rest. Put simply, David is a great friend. He's one of my closest and most trusted partners in the world. On many of the most pressing challenges that we face, we see the world the same way. We recognize that, as I've said before, when the United States and United Kingdom stand together, our nations are more secure and our people are more prosperous, and the world is safer and more just. Great Britain is our indispensable partner, and David has been personally an outstanding partner, and I thank you for your friendship.

With both of our economies growing and unemployment falling, we used our working dinner last night to discuss how we can help create more jobs for our people. We believe that this needs to be the year when the United States and the European Union make real progress toward the Transatlantic Trade and Investment Partnership. And we share the view that boosting demand in Europe can also keep our economies growing.

As innovative economies in this information age, we're expanding our collaboration on digital technologies to improve how our governments serve our citizens and businesses. Given the urgent and growing danger of cyber threats, we've decided to expand our cooperation on cybersecurity to protect our critical infrastructure, our businesses and the privacy of our people. And as leaders in the global fight against climate change, we believe that a strong commitment to reducing greenhouse gases will be an essential element of any ambitious climate agreement that we seek in Paris this year and that this actually will help spur the creation of more clean energy jobs on both sides of the Atlantic.

With regard to security, American-British unity is enabling us to meet challenges in Europe and beyond. We agree on the need to maintain strong sanctions against Russia until it ends its aggression in Ukraine, and on the need to support Ukraine as it implements important economic and democratic reforms. We agree that the international community needs to remain united as we seek a comprehensive diplomatic solution to prevent Iran from obtaining a nuclear weapon. And I'd add that additional sanctions on Iran at this time would undermine that international unity and set back our chances for a diplomatic solution. And as the two leading contributors to the global response to Ebola in West Africa, we urge the world to continue stepping up with the resources that are required so that we don't simply stop this disease, we do more to prevent future epidemics.

Now, much of our discussion obviously focused on the continuing threat of terrorism. And in the wake of the vicious attacks in Paris, as well as the news surfacing out of Belgium, today we continue to stand unequivocally not only with our French friends and allies, but with also all of our partners who are dealing with this scourge. I know David joins me when I say that we will continue to do everything in our power to help France seek the justice that is needed and that all our countries are working together seamlessly to prevent attacks and to defeat these terrorist networks.

With our combat mission in Afghanistan over, we're also focused with our NATO allies on advising and assisting and equipping Afghan forces to secure their own country and deny to al Qaeda any safe haven there. We'll continue to count on our British allies as our -- one of our strongest

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 5 of 26 Page ID #:332 counterterrorism partners, whether it's helping countries fight back against al Qaeda affiliates or Boko Haram in Nigeria.

We reviewed our coalition's progress against ISIL. We are systematically taking out their fighters, we're destroying their infrastructure, we are putting them on the defensive and helping local forces in Iraq push these terrorists back. And David and I agree that we need to keep stepping up the training of Iraqi forces, and that we're not going to relent until this terrorist organization is destroyed.

The Paris attacks also underscored again how terrorist groups like al Qaeda and ISIL are actively trying to inspire and support people within our own countries to engage in terrorism. I led a special session of the United Nations Security Council last fall to rally the world to meet the threat of foreign terrorist fighters, including coming from Syria. David and the United Kingdom continue to be strong partners in this work, including sharing intelligence and strengthening border security.

At the same time, we both recognize that intelligence and military force alone is not going to solve this problem. So we're also going to keep working together on strategies to counter the violent extremism that radicalizes, recruits and mobilizes people, especially young people, to engage in terrorism. And local communities -- families, neighbors, faith leaders -- have a vital role to play in that effort.

We also look forward to welcoming our British friends to our summit next month on countering violent terrorism. Because whether in Europe or in America, a critical weapon against terrorism is our adherence to our freedoms and values at home -- including the pluralism and the respect and tolerance that defines us as diverse and democratic societies.

And finally, I want to take this opportunity to publicly congratulate David on last month's Stormont House Agreement. It's a tribute to the courage and determination of everyone involved, especially the leaders of Northern Ireland as well as the governments of Ireland and the United Kingdom. The United States was pleased to play a small role in achieving this agreement, and we're going to keep doing what we need to do to support the peace process and a better future for the people of Northern Ireland.

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 6 of 26 Page ID #:333 So with that, let me turn it over to my good friend, David Cameron.

PRIME MINISTER CAMERON: Well, thank you very much, Barack. And thank you for welcoming me again to the White House. You are a great friend to Britain and to me personally. As leaders, we share the same values and, as you said, on so many issues, we see the world in the same way. And most of the time, we speak the same language. (Laughter.)

In the last six years since you became President, and in the nearly five since I've been Prime Minister, we've faced some big issues on our watch. And those challenges have boiled down to one word: Security. Economic security -- the jobs and the living standards of our citizens -- and national security -- the ability of our peoples to live safely and in peace.

And at the heart of both issues are the values that our countries cherish: Freedom of expression, the rule of law, and our democratic institutions. Those are the things that make both our countries strong and which give us confidence that even in the midst of the most violent storms, with strong leadership, we will come through to safer, to calmer and to brighter days.

During your presidency, you've had to deal with the aftermath of a massive banking crisis and a deep recession. When I became Prime Minister, Britain had the highest budget deficit in its peacetime history, our economy was in grave peril. Five years ago, we had 110,000 troops serving together in Afghanistan. Thanks to their efforts, today it is Afghan forces taking responsibility for security in their country.

But we continue to face difficult times for the world. First and foremost, we have to deal with the warning lights flashing in the global economy. Wheat growth in the eurozone has slowed down in emerging markets. That is why it is vital for our shared prosperity that we both stick to the long-term economic plans that we've set out.

We agreed that 2015 should be a pivotal year for an ambitious and comprehensive EU-U.S. trade deal which could benefit the average household in Britain by 400 pounds a year. The U.K. is now the top destination for American and foreign investment, with 500 projects last year providing 32,000 jobs. And America is the U.K.'s biggest trade partner, with exports worth nearly 90 billion pounds. We want to build on

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 7 of 26 Page ID #:334 this.

So our message on the economy today is simple: We are going to stick to the course. Because seeing through our economic plans is the only sustainable way to create jobs, to raise living standards, and to secure a better future for hardworking people.

Now, Britain and America both face threats to our national security from people who hate what our countries stand for and who are determined to do us harm. In recent weeks, we've seen appalling attacks in Paris, in Peshawar, in Nigeria. The world is sickened by this terrorism, so we will not be standing alone in this fight. We know what we're up against, and we know how we will win.

We face a poisonous and fanatical ideology that wants to pervert one of the world's major religions, Islam, and create conflict, terror and death. With our allies, we will confront it wherever it appears. In Iraq, the U.K. is the second largest contributor to the anti-ISIL coalition. RAF aircraft have conducted over 100 strikes and will continue to play a leading role. We will deploy additional intelligence and surveillance assets to help Iraqi forces on the ground, and we will ensure they are better trained and equipped to counter explosive devices.

But most important of all, we must also fight this poisonous ideology starting at home. In the U.K., we're passing a law so that every public body must combat extremism. And this morning, we have agreed to establish a joint group to identify what more we can do to counter the rise of domestic violent extremism, and to learn from one another.

In Europe, Russia has chosen to tear up the international rulebook and trample over the affairs of a sovereign state. This threatens our stability and our prosperity. It is important that every country understands that, and that no one in Europe forgets our history. We cannot walk on by. So we will continue to put pressure on Russia to resolve this crisis diplomatically, and at the same time, we will continue our efforts to support Ukraine on the path of reform, including with financial assistance. We also reaffirmed our obligations as NATO partners to stand by our allies, and we'll be contributing an additional thousand troops for exercises in Eastern Europe this year.

On Iran, we remain absolutely committed to ensuring that Iran cannot develop a nuclear weapon. The best way to achieve that now is to create the space for negotiations to succeed. We should not impose further sanctions now; that would be counterproductive and it could put at risk the valuable international unity that has been so crucial to our approach.

We also have to keep pace with new threats, such as cyber attacks. We've discussed that in the last two days, and we've today agreed to deepen our cybersecurity cooperation to better protect ourselves.

Finally, we face -- the entire world faces a growing threat from diseases. Today, our fight is against Ebola. In the future, it could be against a global flu pandemic. Through our action in Sierra Leone, the U.S. action in Liberia, France and Guinea, we are beginning to turn the corner, but we must get better at responding to these global health emergencies and make sure we can master them before they master us.

So reforming the WHO, the World Health Organization; establishing a team of experts to be on standby to deploy anywhere in the world; a new international platform to stimulate the design and development of new drugs -- all of these things are needed. And let 2015, the year we must crack Ebola, also be the year we tackle extreme poverty and climate change.

On poverty, we must set new, clear goals to eradicate extreme poverty, to fight corruption and to build strong institutions. And on climate change, we want an outcome in Paris that keeps our goal of limiting global warming by 2050 to two degrees within reach. These two things -- and they go together -- have the potential to give security to future generations to come.

For almost two centuries, after those little difficulties we were discussing earlier, America and Britain have stood as kindred spirits in defending our freedoms and advancing our shared prosperity. Today, as we survey a world in flux, our alliance stands strong, rooted in its long history, and reinvigorated by the challenges we face today. If our forebears could join us here in the White House today, they might find the challenges that we're facing from ISIL to Ebola, from cyberterrorism to banking crises, they might find those hard to comprehend, but they would

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 9 of 26 Page ID #:336 surely recognize the ties that bind us across the Atlantic and the values that our peoples hold so dear.

We've stood together so often, not just because we faced common threats but because we fundamentally believe in the same things. That is as true today as it has always been, and it hugely benefits our countries and the people that we're here to serve.

Thank you very much.

PRESIDENT OBAMA: Thank you, David. We're going to take a few questions. We're going to start with Jonathan Karl of ABC.

Q Thank you, Mr. President. You mentioned your opposition to the sanctions bill on Iran, and this is obviously a bipartisan bill supported by some very senior top members of your own party in Congress. Why do you oppose a bill that would only impose sanctions if you fail to reach an agreement? And if the Iranians fail to agree to take steps to curtail their nuclear program, would you go so far as to veto a bill supported by top Democrats in Congress on this issue?

And to Mr. Prime Minister, I understand you've been making phone calls to senators on this issue of the Iran sanctions bill, is that correct? Are you actually lobbying the U.S. Congress on this?

And if I may, Mr. President, I'd really like to hear your reaction to the news that Mitt Romney is thinking about running for President again. (Laughter.)

PRESIDENT OBAMA: On your last question -- (laughter) -- I have no comment. (Laughter.)

O None at all?

PRESIDENT OBAMA: On your first question, when I came into office, I made a commitment that Iran would not obtain a nuclear weapon, that we would do everything we could to prevent that. And that is important for our security and it's important for the world's security. If Iran obtained a nuclear weapon, then it would trigger an arms race in the Middle East, make our job in terms of preventing the proliferation of nuclear materials much more difficult. Given their missile capabilities, it

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 10 of 26 Page ID #:337 would threaten directly our closest allies, including Israel, and ultimately could threaten us.

And so what we did was systematically, with the help of Congress, construct the most forceful, most effective sanctions regime in modern history. And what was remarkable was that when I came into office, the world was divided around this issue, and Iran was united. And through some very strong diplomatic work, we united the world and isolated Iran. And it's because of that work that we brought them to the negotiating table -- not for posturing, not for meetings that lead nowhere, but to a very hard-nosed, nuts-and-bolt discussion of their nuclear program.

Now, the interim deal that we entered into also froze progress on their nuclear program, rolled back in some cases the stockpiles of material that they had already accumulated, and provided us insight into their program that was unprecedented. We have people on the ground who are able to verify and inspect and tell us what exactly is going on. That's not just our assessment, that's the assessment of intelligence services around the world, including the Israelis.

So the agreement has held, and the negotiations have been serious. We have not lost ground. Iran has not accelerated its program during the time these negotiations have taken place. In fact, Iran's program has not only been in abeyance, but we've actually made gains in rolling back some of the stockpiles that they had.

Now, we have on the table currently a series of negotiations over the next several months to determine whether or not Iran can get to yes. And what's been remarkable is the unity that we have maintained with the world in isolating Iran and forcing them to negotiate in a serious way. The P5-plus-1 includes not only China, but also includes Russia. And they have continued to cooperate with us in setting forth positions that would give us assurances that Iran was not developing a nuclear weapon.

Now, I've always said that the chances that we can actually get a diplomatic deal are probably less than 50/50. Iran is a regime that is deeply suspicious of the West, deeply suspicious of us. In the past, they have surreptitiously and secretly advanced aspects of this program. We have huge differences with them on a whole range of issues. But if, in

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 11 of 26 Page ID #:338 fact, we still have an opportunity to get a diplomatic deal that provides us verifiable assurances that they are not developing a nuclear weapon, that is the best possible outcome that we can arrive at right now.

And the question I had for members of Congress, including those folks in my own party is: Why is it that we would have to take actions that might jeopardize the possibility of getting a deal over the next 60 to 90 days? What is it precisely that is going to be accomplished?

I can tell you what the risks are, and I think David shares my assessment here. Under the interim deal that brought Iran to the table, we were not supposed to initiate new sanctions. Now, you'll hear arguments -- well, these technically aren't new sanctions, they're simply laws putting in place the possibility of additional sanctions. I assure that is not how Iran would interpret it or our partners would interpret it.

So the likelihood of the entire negotiations collapsing is very high. And if that happens, there is no constraint on Iran at that point going back and doing exactly what it had been doing before they came to the table: Developing a heavy water reactor that, once built, is extraordinarily difficult to dismantle and very difficult to hit military; going back at underground facilities that are very hard to reach militarily; accelerating advanced centrifuges that shorten the time span in which they can achieve breakout capacity.

And they would be able to maintain that the reason that they ended negotiations was because the United States was operating in bad faith and blew up the deal, and there would be some sympathy to that view around the world -- which means that the sanctions that we have in place now would potentially fray, because imposing these sanctions are a hardship on a number of countries around the world. They would love to be able to buy Iranian oil. And the reason that they've hung in there, despite it being against their economic interest, is because we have shown that we are credibly trying to solve this problem and avert some sort of military showdown.

Now, in that context, there is no good argument for us to try to undercut, undermine the negotiations until they've played themselves

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 12 of 26 Page ID #:339

out. Now, if Iran ends up ultimately not being able to say yes, if they cannot provide us the kind of assurances that would lead myself and David Cameron and others to conclude that they are not obtaining a nuclear weapon, then we're going to have to explore other options. And I will be the first one to come to Congress and say we need to tighten the screws.

And, by the way, that's not the only options that are going to be available. I've consistently said we leave all options on the table. But Congress should be aware that if this diplomatic solution fails, then the risks and likelihood that this ends up being at some point a military confrontation is heightened, and Congress will have to own that as well, and that will have to be debated by the American people. And we may not be able to rebuild the kind of coalition we need in that context if the world believes that we were not serious about negotiations.

So I take this very seriously. And I don't question the good faith of some folks who think this might be helpful. But it's my team that's at the table. We are steeped in this stuff day in, day out. We don't make these judgments blindly. We have been working on this for five, six, seven years. We consult closely with allies like the United Kingdom in making these assessments. And I am asking Congress to hold off, because our negotiators, our partners, those who are most intimately involved in this, assess that it will jeopardize the possibility of resolving -- providing a diplomatic solution to one of the most difficult and long-lasting national security problems that we've faced in a very long time. And Congress needs to show patience.

So with respect to the veto, I said to my Democratic caucus colleagues yesterday that I will veto a bill that comes to my desk, and I will make this argument to the American people as to why I'm doing so. And I respectfully request them to hold off for a few months to see if we have the possibility of solving a big problem without resorting potentially to war. And I think that's worth doing. We'll see how persuasive I am, but if I'm not persuading Congress, I promise you I'm going to be taking my case to the American people on this.

PRIME MINISTER CAMERON: I think the big picture is very clear. The sanctions that America and the European Union put in place have had an

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 13 of 26 Page ID #:340 effect. That has led to pressure. That pressure has led to talks. And those talks at least have a prospect of success. And I would argue with the President, how much better is that than the other potential outcomes? And that is what we should be focusing on.

But to answer you very directly, yes, I have contacted a couple of senators this morning and I may speak to one or two more this afternoon -- not in any way as British Prime Minister to tell the American Senate what it should or shouldn't do; that wouldn't be right -- but simply to make the point as a country that stands alongside America in these vital negotiations, that it's the opinion of the United Kingdom that further sanctions or further threat of sanctions at this point won't actually help to bring the talks to a successful conclusion and they could fracture the international unity that there's been, which has been so valuable in presenting a united front to Iran.

And I say this as someone who played quite, I think, a strong role in getting Europe to sign up to the very tough sanctions, including oil sanctions, in the first place. And I would just simply make this point: Those sanctions have had an effect. And to those who said, if you do an interim deal, if you even start discussing with the Iranians any of these things, the sanctions will fall apart, the pressure will dissipate, no one will be able to stick at it. That has demonstrably been shown not to be true.

So the pressure is still there. And as the President says, if the Iranians say no and there is no deal, then by all means let's sit down and work out what extra sanctions to put in place. Because I think we're absolutely united in a simple thought, which is a deal that takes Iran away from a nuclear weapon is better than either Iran having a nuclear weapon or military action to prevent it. In the end, it comes down to that simple choice. And so will I do what I can to help as one of the country's negotiating? Sure I will.

Q Do you acknowledge a less than 50/50 --

PRIME MINISTER CAMERON: I think the way the President put it, I wouldn't disagree with. It's very hard to know what the Iranian thinking is about this. I'm the first British Prime Minister in 35 years I think to meet with an Iranian President, and it's very hard to know what their thinking

But there is a very clear offer there, which is to take Iran away from a nuclear weapon and to conclude an agreement with them which would be mutually beneficial. That's what should happen.

I think we've got a question from Nick Robinson at the BBC.

Q Mr. Nick Robinson, BBC News. Prime Minister, with extra security being put in place today for the Jewish community and also for police officers, would people be right to conclude that the threat of an attack on the streets of Britain is now all but imminent?

And, Mr. President, you've spoken of the threat posed by fighters coming back from Syria. Do you ever worry that this is a legacy of the decision of the United States and the United Kingdom to in effect stand on the sidelines during Syria's bloody civil war?

And if I may briefly, if you'll forgive me, on the economy, you said you agree. Is he right? Is it time to stick to the plan?

PRIME MINISTER CAMERON: Well, first of all, look, we do face a very serious Islamist extremist terrorist threat in Europe, in America, across the world. And we have to be incredibly vigilant in terms of that threat. We've got to strengthen our police and security. We ought to make sure we do everything we can to keep our country safe. And that involves an incredibly long-term, patient, disciplined approach.

There is no single, simple thing that needs to be done. It means closing down the ungoverned spaces that the terrorists operate in. It means working against ISIL in Iraq and Syria. It means countering this poisonous, fanatical death cult of a narrative that is perverting the religion of Islam. It means working together with our oldest and best partners so that we share intelligence and security and we try and prevent terrorist atrocities from taking place. It means all of these things, and it is going to be a long, patient and hard struggle.

I'm quite convinced we will come through it and we will overcome it, because in the end, the values that we hold to of freedom, of democracy, of having open and tolerant societies -- these are the strongest values

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 15 of 26 Page ID #:342 there can be. And in the end, we will come through. But like some of the challenges our countries have faced together in the past, it will take great discipline, great patience, great, hard work.

You asked specifically the question about imminence. We have a system in the United Kingdom where threat levels are set by the Joint Terrorism Assessment Centre. They're not set by politicians. They have judged that the threat we face is severe. That means, in their words, that an attack is highly likely. If ever there is an imminent threat of attack, it goes to the next level up, which is critical. But it's their decision, not mine. My responsibility is to make sure we marshal everything we have as a country in order to defeat the threat.

Q On the Jewish community?

PRIME MINISTER CAMERON: And on the Jewish community, I think it's good that the metropolitan police have announced that they'll be stepping up on patrols. I met with the Jewish Leadership Council earlier this week. We already provide through their security organization, the Community Security Trust, we already provide government money to help protect Jewish schools. But I think this is -- we have to recognize in fighting terrorism, as we found in Britain before, you cannot simply rely on policing and security. This is a job for everyone. This is a role that we're all going to have to play in the vigilance and in making sure that we keep our community safe.

PRESIDENT OBAMA: With respect to Syria and the connection to foreign fighters, there is no doubt that in the chaos and the vacuum that's been created in big chunks of Syria, that that's given an opportunity for foreign fighters to both come in and come back out. And I chaired a U.N. Security Council meeting, and we are now busy working with our partners to implement a series of actions to identify who may be traveling to Syria in order to get trained, to fight, or to hatch plots that would be activated upon return to their home countries. So it's a very serious problem.

The notion that this is occurring because the United States or Great Britain or other countries stood on the sidelines I think is -- first of all, mischaracterizes our position. We haven't been standing on the sidelines; it's true we did not invade Syria. If the assertion is, is that had Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 16 of 26 Page ID #:343 we invaded Syria we would be less prone to terrorist attacks, I'll leave it to you to play out that scenario and whether that sounds accurate.

We've been very active in trying to resolve a tragic situation in Syria -diplomatically; through humanitarian efforts; through the removal of
chemical weapons from Syria that had been so deadly. And now as ISIL
has moved forward, we've been very active in degrading their capabilities
inside of Syria, even as we're working with partners to make sure that the
foreign fighter situation is resolved.

But I think David's point is the key one. This phenomenon of violent extremism -- the ideology, the networks, the capacity to recruit young people -- this has metastasized and it is widespread, and it has penetrated communities around the world.

I do not consider it an existential threat. As David said, this is one that we will solve. We are stronger, we are representing values that the vast majority of Muslims believe in -- in tolerance and in working together to build rather than to destroy. And so this is a problem that causes great heartache and tragedy and destruction, but it is one that ultimately we're going to defeat. But we can't just defeat it through weapons.

One of the things that we spoke about is how do we lift up those voices that represent the vast majority of the Muslim world so that that counternarrative against this nihilism is put out there as aggressively and as nimbly as the messages coming out from these fanatics. How do we make sure that we are working with local communities and faith leaders and families -- whether in a neighborhood in London or a neighborhood in Detroit, Michigan -- so that we are inoculating ourselves against this kind of ideology. And that's going to be slow, plodding, systematic work, but it's work that I'm confident we're going to be able to accomplish, particularly when we've got strong partners like the United Kingdom doing it.

Q On the economy --

PRESIDENT OBAMA: On the economy, I would note that Great Britain and the United States are two economies that are standing out at a time when a lot of other countries are having problems, so we must be doing something right.

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 17 of 26 Page ID #:344 Major Garrett.

Q Thank you, Mr. President. Good afternoon, Mr. Prime Minister. Good afternoon to you, sir.

Questions for all -- for both of you. I want to make sure we heard what you were trying to say. You clearly are directing a message to Congress in the context of Iranian negotiations. Were you also sending a message -- both of you -- to Iran that if the sanctions talks fail, that war footing is the next most likely alternative for this country and those who are allied with us in this common pursuit?

And atrocities in Paris, raids and threats either in Belgium and Netherlands, I'd like to ask you both: Do you believe Europe is at a turning point now in its recognition of what its threats are and its own mobilization in terms of new laws, security footing, larger budgets? And you both talked about cybersecurity. There is a crucial issue for both countries -- backdoors in encryption to protect people and also privacy. I'd like your comments on that. Thank you.

PRESIDENT OBAMA: I am not -- repeat, not -- suggesting that we are in immediate war footing should negotiations with Iran fail. But as David put it very simply -- if, in fact, our view is that we have to prevent Iran from getting a nuclear weapon, then we have to recognize the possibility that should diplomacy fail, we have to look at other options to achieve that goal.

And if you listen sometimes to the rhetoric surrounding this issue, I think there is sometimes the view that this regime cannot be trusted; that, effectively, negotiations with Iran are pointless. And since these claims are being made by individuals who see Iran as a mortal threat and want as badly as we do to prevent them from getting a nuclear weapon, the question then becomes: Well, what other alternatives exactly are available?

That is part of what we have to consider as to why it's so important for us to pursue every possible avenue to see if we can get a deal. Now, it's got to be good deal, not a bad deal. I've already shown myself willing to walk away from a bad deal. And the P5-plus-1 walked away with us. And so nobody is interested in some document that undermines our sanctions

and gives Iran the possibility of, whether covertly or gradually, building up its nuclear weapons capacity. We're not going to allow that. And anything that we do, any deal that we arrive at -- if we were to arrive at one -- would be subject to scrutiny across the board, not just by members of Congress, but more importantly, by people who actually know how the technical aspects of nuclear programs can advance and how we can effectively verify in the most rigorous way possible that the terms of the deal are being met.

So the bottom line is this: We may not get there, but we have a chance to resolve the nuclear issue peacefully. And I should point out also, by the way, that if -- even if we get a nuclear deal and we are assured that Iran doesn't possess nuclear weapons, we've still got a whole bunch of problems with Iran on state-sponsored terrorism, their rhetoric towards Israel, their financing of Hezbollah. We've got differences with respect to Syria. It's not as if suddenly we've got a great relationship with Iran. It solves one particular problem that is urgent, and it solves it better than the other alternatives that might present themselves.

So my main message to Congress at this point is, just hold your fire. Nobody around the world, least of all the Iranians, doubt my ability to get some additional sanctions passed should these negotiations fail. That's not a hard vote for me to get through Congress. And so the notion that we need to have additional sanctions, or even the possibility of sanctions hanging over their head to force them to a better deal, I think the Iranians know that that is certainly in our back pocket if the negotiations fail.

With respect to violent extremism, my impression is that Europe has consistently taken this seriously. During the course of my presidency, we have worked collaboratively and with great urgency and a recognition that not only do you have foreigners who may be trying to hatch plots in Europe, but that, given large immigrant populations, it's important to reach out to and work with local communities and to have a very effective intelligence and counterterrorism cooperation between countries and between the United States and Europe.

There's no doubt that the most recent events has amplified those concerns. I think one of the things that I've learned over the last six years is that there's always more that we can do. We can always do it better.

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 19 of 26 Page ID #:346 We learn from mistakes. Each incident that occurs teaches our professionals how we might be able to prevent these the next time.

And I'm confident that the very strong cooperation that already exists with Europe will get that much better in the months and years to come.

Q Do you believe that Europe has been as sensitized as the United States and Great Britain has?

PRESIDENT OBAMA: Here's where I actually think that Europe has some particular challenges, and I said this to David. The United States has one big advantage in this whole process, and it's not that our law enforcement or our intelligence services, et cetera, are so much better -- although ours are very, very good, and I think Europeans would recognize that we've got capabilities others don't have. Our biggest advantage, Major, is that our Muslim populations, they feel themselves to be Americans. And there is this incredible process of immigration and assimilation that is part of our tradition that is probably our greatest strength. Now, it doesn't mean that we aren't subject to the kinds of tragedies that we saw at the Boston Marathon. But that, I think, has been helpful.

There are parts of Europe in which that's not the case, and that's probably the greatest danger that Europe faces -- which is why, as they respond, as they work with us to respond to these circumstances, it's important for Europe not to simply respond with a hammer and law enforcement and military approaches to these problems, but there also has to be a recognition that the stronger the ties of a North African -- or a Frenchman of North African descent to French values, French Republic, a sense of opportunity -- that's going to be as important, if not more important, in over time solving this problem. And I think there's a recognition of that across Europe, and it's important that we don't lose that.

The last point I'll make, and then I'll turn it over to David, is with respect to the issue of intelligence-gathering, signal intelligence, encryptions, this is a challenge that we have been working on since I've been President. Obviously, it was amplified when Mr. Snowden did what he did. It's gone off the pages of -- the front pages of the news, but we haven't stopped working on it. And we've been in dialogue with companies and have systematically worked through ways in which we can meet legitimate

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 20 of 26 Page ID #:347 privacy concerns, but also meet the very real concerns that David has identified and my FBI Director, Jim Comey, identified.

Social media and the Internet is the primary way in which these terrorism organizations are communicating. Now, that's no different than anybody else, but they're good at it. And when we have the ability to track that in a way that is legal, conforms with due process, rule of law, and presents oversight, then that's the capability that we have to preserve.

And the biggest damage that was done as a consequence of the Snowden disclosures was I think, in some cases, a complete undermining of trust. Some would say that was justified. I would argue that although there are some legitimate concerns there, overall, the United States government and, from what I've seen, the British government, have operated in a scrupulous and lawful way to try to balance these security and privacy concerns. And we can do better, and that's what we're doing.

But we're still going to have to find ways to make sure that if an al Qaeda affiliate is operating in Great Britain or in the United States, that we can try to prevent real tragedy. And I think the companies want to see that as well. They're patriots. They have families that they want to see protected. We just have to work through in many cases what are technical issues. So it's not so much that there's a difference in intent, but how to square the circle on these issues is difficult. And we're working with partners like Great Britain and the United Kingdom, but we're also going to be in dialogue with the companies to try to make that work.

PRIME MINISTER CAMERON: On the Iranian issue, I won't add much to what the President said. I'd just make this point, that I don't think you can characterize it as, if there's a deal then the pressure is off Iran, and if there isn't a deal, new pressure has to be applied to Iran. I mean, even if there is a deal, the key to that deal will be transparency and verification and making sure that this country isn't developing a nuclear weapon. And that will mean repeated pressure, even after a deal is done. I think that's very important.

And I would absolutely back up what Barack says about recognizing that in so many other ways, we have some major disagreements with what the

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 21 of 26 Page ID #:348

Iranians have been doing. I mean, Britain has suffered particularly from the appalling way that our embassy and our staff were treated in that country. So we approach this with a huge amount of skepticism and concern. But the goal of an Iran without a nuclear weapon makes these talks worthwhile.

On the issue -- your question, has -- is this a turning point for Europe in terms of terrorism, I would argue that we turned some time ago. Maybe Britain in particular because of the appalling attacks that took place in 2005, but there have been attacks elsewhere in Europe. I mean, since I've been Prime Minister, there's probably been at least one major plot every year of quite a significant nature that we have managed to intercept, stop and prevent. So the awareness of the scale of the challenge we face is absolutely there across government, across parliament, across the different political parties in the police and intelligence services.

I think there is an opportunity for countries in Europe, who perhaps up to now have been less affected, to work with them and make sure that we share knowledge and skills. Because when you say, have you -- the turning point is making sure your legislation is up to date, making sure your police and security services have the capabilities they need, making sure you've got programs that can channel extremists away and deradicalize them, making sure that you're better integrating your communities. It means doing all of those things.

I very much agree with what Barack says about the importance of building strong and integrated societies. I made a speech about this at Munich a couple of years ago, saying that it had been a mistake in the past when some countries had treated different groups and different religious groups as sort of separate blocks rather than trying to build a strong, common home together. That is what we should be doing, and that is what our policy is directed to.

And, of course, you need to have -- as I believe we are -- a multiracial, multiethnic society of huge opportunity where in one generation or two generations you can come to our country and you can be in the Cabinet; you can serve at the highest level in the armed forces; you can sit on the bench as a judge. I've got in my Cabinet someone just like that, who in two generations his family has gone from arriving in Britain to sitting --

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 22 of 26 Page ID #:349 that's vitally important, as is combatting unemployment, combatting poverty.

But here's I think the really determining point: You can have, tragically, people who have had all the advantages of integration, who have had all the economic opportunities that our countries can offer, who still get seduced by this poisonous, radical death cult of a narrative. We've seen in recent weeks people who have gone to fight in Syria and who may threaten us here back at home who have had every opportunity and every advantage in life in terms of integration. So let's never lose sight of the real enemy here, which is the poisonous narrative that's perverting Islam. That is what we have to focus on, recognizing that of course we help ourselves in this struggle if we create societies of genuine opportunity, if we create genuine integration between our communities. But let's never lose sight of the real -- the heart of the matter.

As for the issue on the techniques necessary for our intelligence services to help keep us safe, all I would say -- and the President and I had a good discussion about this earlier -- I don't think either of us are trying to annunciate some new doctrine. The doctrine that I approach this -- what?

Q (Off-mic.)

PRIME MINISTER CAMERON: Well, I'm sorry to disappoint you, but I take a very simple approach to this, which is ever since we've been sending letters to each other or making telephone calls to each other, or mobile phone calls to each other, or indeed contacting each other on the Internet, it has been possible in both our countries, in extremis -- in my country by a signed warrant by the Home Secretary -- to potentially listen to a call between two terrorists to stop them in their activity. In your country, a judicial process. We've had our own -- we're not asking for backdoors. We believe in very clear front doors through legal processes that should help to keep our countries safe.

And my only argument is that as technology develops, as the world moves on, we should try to avoid the safe havens that can otherwise be created for terrorists to talk to each other. That's the goal that I think is so important, because I'm in no doubt, as having been Prime Minister for

Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 23 of 26 Page ID #:350 four and a half years, having seen how our intelligence services work, I know that some of these plots that get prevented, the lives that get saved, there is a very real connection between that and the capabilities that our intelligence services within the law use to defend our people.

I think the final question is from Robert Moore from ITN.

Q Thank you. Yes, Robert Moore with the British network, ITV News. Prime Minister, it's clear there is a sort of security alert underway at the moment around the Jewish community in Britain. Can I just be clear, is that based on specific intelligence? Should people be concerned about doing their daily activities this weekend? And do you regard a terrorist attack on British soil as almost inevitable?

And, Mr. President, you say there is a dialogue underway with the big American tech companies, but do you share the Prime Minister's view that the current threat environment is so severe that there does need to be a swing of the pendulum a little bit, maybe from privacy towards counterterrorism, and that this area of private encrypted communications is a very dangerous one, potentially in terms of facilitating dialogue between terrorist groups?

PRIME MINISTER CAMERON: On the issue of the threat that we face, as I said, the level has been set at severe. That is set by an independent expert organization, so people can have full confidence that these things aren't ever done for any other motives than literally to look at the evidence that is there about terrorist threats and to set the level accordingly. When the level, as it is as the moment, is set at severe, that means that the authorities believe an attack is highly likely. If we believed it was imminent, then you would move to the next level, which is critical.

And we clearly do face a very real threat in our country. I mean, in recent months, as I was discussing with the President, we've had a number of potential attacks averted, for instance, on British police officers. So that is the threat picture. It's regularly reviewed, regularly updated, but it shouldn't be moved unless there is real evidence to do so.

In terms of the protection to the Jewish community and indeed other communities, and indeed to police officers themselves, this is based on what has happened in France, on the whole picture that we see. And it is Case 5:16-cm-00010-SP Document 16-23 Filed 02/25/16 Page 24 of 26 Page ID #:351 sensible, precautionary measures to make sure we do what we can to reassure those communities -- communities who are all too aware of the threat that they face. And this is a bigger challenge for us.

I think one of the most moving sights in Paris was to see so many people holding up signs saying "Je suis flic," I'm a cop; "Je suis juif," I'm a Jew. And I thought that was incredibly moving, that people wanted to stand together with one community that had been singled out, and singled out not because of anything other than the fact they were Jewish. So I think it's very important that we speak up and stand up for those communities and give them the protection that they deserve.

PRESIDENT OBAMA: Obviously, in the wake of Paris, our attention is heightened. But I have to tell you, over the last six years threat streams are fairly constant. David deals with them every day, I deal with them every day. Our CT, our counterterrorism professionals deal with them every day. So I don't think there's a situation in which because things are so much more dangerous, the pendulum needs to swing. I think what we have to find is a consistent framework whereby our publics have confidence that their government can both protect them, but not abuse our capacity to operate in cyberspace. And because this is a whole new world, as David said, the laws that might have been designed for the traditional wiretap have to be updated.

How we do that needs to be debated, both here in the United States and in the U.K. I think we're getting better at it. I think we're striking the balance better. I think the companies here in the United States at least recognize that they have a responsibility to the public, but also want to make sure that they're meeting their responsibilities to their customers that are using their products. And so the dialogue that we're engaged in is designed to make sure that all of us feel confident that if there is an actual threat out there, our law enforcement and our intelligence officers can identify that threat and track that threat at the same time that our governments are not going around phishing into whatever text you might be sending on your smartphone. And I think that's something that can be achieved.

There are going to be situations where there are hard cases. But for the most part, those who are worried about Big Brother sometimes obscure or deliberately ignore all the legal safeguards that have been put in place to assure people's privacy and to make sure that government is not abusing these powers. And on the other hand, there are times where law enforcement and those of us whose job it is to protect the public aren't thinking about those problems because we're trying to track and prevent a particular terrorist event from happening. And it's useful to have civil libertarians and others tapping us on the shoulder in the midst of this process and reminding us that there are values at stake as well. And I think that David and I welcome that kind of debate.

The technologies are evolving in ways that potentially make this trickier. If we get into a situation in which the technologies do not allow us at all to track somebody that we're confident is a terrorist; if we find evidence of a terrorist plot somewhere in the Middle East that traces directly back to London or New York, we have specific information and we are confident that this individual or this network is about to activate a plot, and despite knowing that information, despite having a phone number, or despite having a social media address or email address -- that we can't penetrate that, that's a problem.

And so that's the kind of dialogue that we're having to have with these companies. Part of it is a legal issue, part of it is a technical question. But overall, I'm actually confident that we can balance these imperatives, and we shouldn't feel as if because we've just seen such a horrific attack in Paris, that suddenly everything should be going by the wayside. Unfortunately, this has been a constant backdrop and I think will continue to be for any Prime Minister or President for some time to come, and we've got to make sure that we don't overreact but that we remain vigilant and are serious about our responsibilities there.

Thank you very much, everybody. Appreciate it. Thank you.

END 1:39 P.M. EST



Exhibit W

White House. Red Chair. Obama Meets Swisher.

President Barack Obama took his turn in the red hot seat last Friday for a one-on-one interview with **Re/code** co-executive editor Kara Swisher*.

Obama was in Silicon Valley to speak at the White House Summit on Cybersecurity and Consumer Protection, and spoke with Swisher after addressing the audience at Stanford University.

The brisk conversation touched on an array of tech-focused topics, including cyber warfare, diversity in tech hiring, the White House's <u>relationship with Silicon Valley</u> — and the president's own <u>gadgets of choice</u>.

This interview has been edited and condensed for clarity.



Vjeran Pavic for Re/code

Watch the full interview in the video below:

Kara Swisher: Thank you for being here, Mr. President.

President Barack Obama: Great to be here.

Very excited to do an interview with Re/code. And we have a lot of topics to talk about in tech.

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 3 of 13 Page ID #:356 Let's go.

We're going to go from cyber security, your relationship with Silicon Valley, privacy, STEM education.

Got it all covered.

Got it all covered, all right.

Let's go.

"Mr. Tech, okay. So let's talk about cyber security first." — Re/code co-executive editor Kara Swisher

Mr. Tech, okay. So let's talk about cyber security first. This is a cyber security summit. You had Tim Cook talking about it, all kinds of different leaders.

Right.

The dangers of what's happening. Right now, there's been a lot of instances of cyber security breaches, Sony being the most famous.

Right.

The government said North Korea was behind this? Yeah.

Are these acts of war?

I wouldn't consider them acts of war. But I would consider them acts of property damage, commercial theft, that are serious. And whenever a criminal act like that is state-sponsored, it's a problem. I just had a terrific roundtable with CEOs and chief information officers from a whole bunch of different sectors of the economy.

And one of the uniform things they said was state actors are in a different category because of the sophistication and the resources and the patience that they have. That's an area where [the] private sector's going to have to get help immediately from the government in a much more aggressive way, and a lot of what we're doing in terms of information sharing, gathering data, getting it out, disseminating it all throughout the economy much quicker — we've gotten better at that.

Then what you have is a bunch of non-state actors, hackers, criminals, etc., that are just flooding the system, constantly probing for weaknesses. And part of what this summit is about is both making sure that we have mechanisms for government/private sector cooperation, increased consumer awareness of how they can reduce their vulnerabilities, how we can build better defenses, how we can respond better and more resiliently. And one of the big conclusions is this is moving so fast that we've got to have a more nimble system. This isn't a traditional setting where you can just set up a few standards or rules or regulations, and then just sit on our laurels. We have to constantly update all the time.

But what does it have to be to become more serious? Shutting down New York? We're very vulnerable, as we become more digital.

We're hugely vulnerable. We've started with critical infrastructure. That's an area where heavy involvement with those industries — whether it's Wall Street and the financial sector, utilities, our airtraffic control system — all of that, increasingly, is dependent on the digital base that they're working off of.

And so a lot of concentration there first. And one of the challenges is that a lot of this is private sector — the vast bulk of it is private sector. The government has to be able to not only work with each individual company, we've got to be able to pull those companies together so they're working together more effectively. And one of the things that makes this such a challenging problem is, all you need is one weak link. You can have nine companies

Well, in any defense.

Right. You can have nine companies that have great protocols, authentication systems, you name it. You have one that's not doing a good job, and that penetrates the entire system. So I think everybody recognizes now the degree of seriousness.

The key is to coordinate more effectively the legislation that we've put before Congress that, for example, provides companies with some selective liability protections so that when they share information, they're not vulnerable to future lawsuits. Those are the kinds of areas where I would like to see us make a lot of progress this year.

We talk about North Korea being this bad actor ... around "The Interview." Right.

We do our own hacking of other countries. There's been lots of reports about the Iran nuclear system and things like that. Can we make a good argument that we should be protected against them, when we're doing the same thing ourselves?

Obviously, I can't talk about specifics and whether ...

But please do. [Laugh]

... whether confirming or denying whatever you discuss. I mentioned in the CEO roundtable — a comment that was made by one of my national security team. This is more like basketball than football, in the sense that there's no clear line between offense and defense. Things are going back and forth all the time.

We have great capabilities here. But there are other countries that have great capabilities, as well. Eventually, what we're going to need to do is to find some international protocols that, in the same way we did with nuclear arms, set some clear limits and guidelines, understanding that everybody's vulnerable and everybody's better off if we abide by certain behaviors. In the meantime, we have to

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 5 of 13 Page ID #:358 have sufficient capability to defend ourselves.



Vjeran Pavic for Re/code

"What we're going to need to do is to find some international protocols that, in the same way we did with nuclear arms, set some clear limits and guidelines, understanding that everybody's vulnerable and everybody's better off if we abide by certain behaviors." — President Barack Obama

Is that just defense? Or offense?

I won't lie to you, this is a debate that we have internally. Because when you develop sufficient defenses, the same sophistication you need for defenses means that potentially you can engage in offense. Now, there are some things that we're very clear about. For example, we just don't do industrial espionage the way many other countries do, where their state-sponsored operations are going in and stealing information commercially.

Most of the work that we do revolves around threats against us from non-state actors, and obviously terrorism is a huge field. And increasingly, cyber terrorism is going to be something that we're concerned about. But we are going to have to build in a whole set of safeguards to make sure that we are upholding high standards if we expect others to do the same.

I'm going to switch to something else in a second. But should there be a cyber army? Should we — our government — have this dedicated, the way they do in North Korea or China?

Well, what we have is a separate cyber structure, a cyber command that coordinates a lot of this activity, partly because our defense systems today, our armed forces, are dependent on the digital world in the same way that it has penetrated everything else. So this separate cyber command monitors, defends, focuses on protecting not only the Department of Defense and our armed forces, but also critical infrastructure, and is constantly monitoring what other state actors potentially could do. But — just to give you a sense of how challenging this is — it's not as if North Korea is particularly good at this.

They did ... not bad.

But look how much damage they were able to do. Non-state actors can do a lot damage, as well. So we've got to constantly upgrade our game, and that's part of the purpose of this.

Are there any countries you're worried about, comparatively? North Korea, not so good. Who's good?

Well — China and Russia are very good. Iran is good. And we're constantly engaged in a dialogue with these countries in the same way that we engage in a dialogue around nuclear arms, indicating to them that it doesn't serve anybody's purpose for us to attack in ways that may end up eliciting responses, and everybody's worse off.

Let's talk about the relationship between you and Silicon Valley. Lots of discussion about who wasn't here, and tensions, and sort of, "can this marriage be saved?" How do you look at your relationship right now with Silicon Valley? They're nervous about the NSA, they're still hurting about that. Visas, Zero-Day flaws, all kinds of things.

You know, look. It's your job to generate some controversy, but...

Now, some controversy ... [Laugh] Some of those quotes from the Google people are pretty tough.

But I think it's also fair to say that my relationship with Silicon Valley and the tech community has historically been really good. Many of these folks are my friends, and have been supporters, and we interact all the time.

"I think it's also fair to say that my relationship with Silicon Valley and the tech community has historically been really good." — Barack Obama

Well, they're still giving a lot of money to ...

But what is true is that the <u>Snowden disclosures</u> were really harmful in terms of the trust between the government and many of these companies, in part because it had an impact on their bottom lines. When you look back at what we've done, I have constantly tried to update the laws and rules governing how we operate in cyberspace with these new technologies.

In the case of the NSA, we're probably a little slow. The truth is that what we did with respect to U.S. persons, what we did in this country, was strictly circumscribed. And, generally speaking, I can say with almost complete confidence that there haven't been abuses on U.S. soil.

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 7 of 13 Page ID #:360 But it's a global Internet world.

And that's the point.

And they're businesses.

And that has been the challenge. What is true — and I've said this publicly, so I'm not saying anything that's classified in any way — our capacities to scoop up information became so great, and traditionally there haven't been restraints on our intelligence community scooping up information from outside our borders and non-U.S. persons.

So what ended up happening was that, in places like Germany, this had a huge impact — not just on government-to-government relations, but suddenly all the Silicon Valley companies that are doing business there find themselves challenged, in some cases not completely sincerely. Because some of those countries have their own companies who want to displace ours.

I say all this to make the point that I think we have made real progress in narrowing the differences around the national security/privacy balance. There are still some issues like encryption that are challenging.

Let's <u>talk about encryption</u>. What's wrong with what Google and Apple are doing? You have encrypted email — shouldn't everybody have encrypted email, or have their protections? Everybody should. And I'm a strong believer in strong encryption. Where the tension has come up, historically, what has happened, is that — let's say you knew a particular person was involved in a terrorist plot. And the FBI is trying to figure out who else were they communicating with, in order to prevent the plot.

Traditionally, what has been able to happen is that the FBI gets a court order. They go to the company, they request those records the same way that they'd go get a court order to request a wiretap. The company technically can comply. The issue here is that — partly in response to customer demand, partly in response to legitimate concerns about consumer privacy — the technologies may be built to a point where, when the government goes to ...

They can't get the information.

The company says, "Sorry, we just can't pull it. It's so sealed and tight that, even though government has a legitimate request, technologically we cannot do it."



Vieran Pavic for Re/code

Is what they're doing wrong?

No, I think they are properly responding to a market demand. All of us are really concerned about making sure our ...

So what are you going to do?

Well, what we're going to try to do is to see: Is there a way for us to narrow this gap? Ultimately, everybody — and certainly this is true for me and my family — we all want to know that if we're using a smartphone for transactions, sending messages, having private conversations, that we don't have a bunch of people compromising that process.

So there's no scenario in which we don't want really strong encryption. The narrow question is going to be if there is a proper request for ... this isn't bulk collection, this isn't sort of fishing expeditions by government.

Where there is a situation in which we're trying to get a specific case of a possible national security threat — is there a way of accessing it? If it turns out it's not, then we're really gonna have to have a public debate. And, you know, I think some in Silicon Valley would make the argument — which is a fair argument, and I get — that the harms done by having any kind of compromised encryption are far greater ...

That's an argument you used to make.

Well ...

You would have made. Has something changed with ...

No, I still make it. It's just that I am sympathetic to law enforcement.

Because years [ago], you were much stronger on civil liberty.

I'm as strong as I have been. I think the only concern is our law enforcement is expected to stop every plot. Every attack. Any bomb on a plane. The first time that attack takes place in which it turns out that we had a lead and we couldn't follow up on it, the public's going to demand answers.

And this is a public conversation that we should end up having. I lean probably further in the direction of strong encryption than some do inside of law enforcement. But I am sympathetic to law enforcement because I know the kind of pressure they're under to keep us safe. And it's not as black-and-white as it's sometimes portrayed.

Now, in fairness, I think the folks who are in favor of airtight encryption also want to be protected from terrorists.

True.

One of the interesting things about being in this job is [that] it does give you a bird's-eye view. You are smack-dab in the middle of these tensions that exist. But I guess what I would say is, there are times where folks who see this through a civil-liberties or privacy lens reject that there's any trade-offs involved, and in fact there are. And you've got to own the fact that it may be [that] we want to value privacy and civil liberty far more than we do ...

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 9 of 13 Page ID #:362 **Safety.**

The safety issues. But we can't pretend that there are no trade-offs whatsoever.

Let's go quickly into privacy. There's a privacy bill you've all been trying to pass forever, with some teeth in it.

Right.

Who owns their data? And, on the other side of the companies, have you all acquiesced too far to the Facebooks and Googles of the world, when Europe is being much more stringent? I think you own your data, I think I own my data. I think we own our health-care data, I think we own our financial data.

Doesn't feel like it.



Vjeran Pavic for Re/code

"This is an area where, ironically, sometimes I also have tensions with Silicon Valley — because folks are quite keen on talking about government intrusion." — Barack Obama

I think this is an area where, ironically, sometimes I also have tensions with Silicon Valley — because folks are quite keen on talking about government intrusion. [Laugh] But some of the commercial models that are set up obviously ...

A little intrusive.

... are fairly intrusive, as well.

But they're selling us things. So ...

Yeah, exactly. So, I think part of the answer here is just people knowing ahead of time what's going on. People knowing how their data's being used. Much greater transparency in terms of its potential for migrating over into some sales-and-marketing scheme of somebody else's.

And the more transparent we are, the more customers can make a choice. There are circumstances — I'll give one specific example that I talked a while back, about ... educational technologies being sold and put into schools. And then it turns out that some kid who's going online to communicate with their teacher — their data is going to some marketing company that then sells to the kid. I think that's got to be off-limits. So there are going to be some areas where we just say no, even if the consumer is aware of it ahead of time.

But does it have any teeth, really? I mean, Europe is very strong on these things, and doing a lot of investigations into Google and Facebook and other companies.

In defense of Google and Facebook, sometimes the European response here is more commercially

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 10 of 13 Page ID #:363

driven than anything else. As I've said, there are some countries like Germany, given its history with the Stasi, that are very sensitive to these issues. But sometimes their vendors — their service providers who, you know, can't compete with ours — are essentially trying to set up some roadblocks for our companies to operate effectively there.

Interesting.

We have owned the Internet. Our companies have created it, expanded it, perfected it in ways that they can't compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests.

Let's talk about owning it. We have invented the Internet, we have created the most important technology companies. Losing that rapidly to other companies. Education, STEM, visas, all kinds of things, bringing the best talent here. Right now, diversity is another issue, especially women.

Right.

How do you look at this? How do we change the equation here? Because many people feel that, even though we've got this strong industry, we're losing on lots of ground.

First of all, we're not losing it rapidly. But what is true is that our lead will erode if we don't make some good choices now. STEM education, huge priority. Homegrown — we've got to have our kids in math and science, and it can't just be a handful of kids. It's got to be everybody. Everybody's got to learn how to code early.

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 11 of 13 Page ID #:364 I have, and I've said to ...

Do they?

Well, not as much as I would probably like. Although I think they got started a little bit late. Part of what you want to do is introduce this with the ABCs and the colors. And particularly, focusing on girls' participation — math.science.technology — early is important. Underrepresented groups, African Americans, Latinos. We've got to get those kids tapped in. That's the largest-growing part of our population. If they don't have basic digital literacy ...

What's the problem? I mean, because company after company, 70 percent white, 70 percent male ...

I think part of the problem is, just generally, our school systems aren't doing as good of a job on this, period. Full stop. And then part of what's happening is that we are not helping schools and teachers teach it in an interesting way.

And what ends up happening is a certain portion of the population just drifts away. Girls, for example — we don't lift up models of them being successful in STEM. Somebody has talked about the degree to which we very rarely see portrayed on television — female engineers.

And don't have any jobs, actually.

Right. So we just have to — we have to lift that stuff up. So that's the long term, getting that whole pool of talent focused. More immediately, we've got an urgent need right now. Comprehensive immigration reform would revise our system so that the best and the brightest from around the world come here, the ones who are studying here aren't forced to leave. We have been pushing this hard in Congress. So far, Congress has blocked it.

So what do you do?

Well, what I did with the executive action that I announced around immigration. There were some areas where I could help to reduce some of the backlog, some of the bureaucracy, [to] make it somewhat easier for talented foreign students to operate here. But we haven't gone far enough, and the legislation is what's going yo be required. So we've got to keep on pushing on that. You know, overall, though, the good news is that the ecosystem here is so far ahead of anywhere else. There's so much talent, so much brain power, so much financing ...

It still leaves a lot of people out.



Vieran Pavic for Re/code

"There's a huge possibility for talent — not just homegrown — from around the world, continuing to converge here in the United States. Look, what used to be primarily Silicon Valley, now it's also Austin,

Texas." — Barack Obama

But the point is is that there is so much more room to grow, I guess. It's not as if this is a mature, finite industry where it's a zero-sum game in terms of how many people can be participating. There's a huge possibility for talent — not just homegrown — from around the world, continuing to converge here in the United States. Look, what used to be primarily Silicon Valley, now it's also Austin, Texas.

Well, they're trying. Yeah.

Yeah. I mean, there are a bunch of other places around the country — in Utah and others — where people are coalescing. I was at Boise State, and they're doing all kinds of interesting stuff in the digital space, connecting universities with companies.

So this is something that we want to democratize and see spread all across the country. We are putting together public/private partnerships around, for example, just getting more engineers. You know, we partnered with Intel and a bunch of companies.

Are you worried that China and others are graduating more engineers?

Yes. Although our engineers are still better. But we don't always need the absolute top MIT engineer. Part of what we also need is the standard engineer who can help on a production facility.

Because, ironically, part of the reason that some tech production jobs have gone overseas is not so much in search of low wages as it is that there are just more engineers at this production level that can really help.

Wrapping up, I want to ask you something about your personal tech habits. Go ahead.

I know you watch a lot of sports.

I do.Where are you watching things now? Are you watching it on your phone, or do you watch it on television?

You know, I'll be honest with you ...

When it comes to ballgames, I'm still usually watching it on TV — DVR. But when it comes to highlights, I'm usually watching it on an iPad.



Vjeran Pavic for Re/code

"When it comes to ballgames, I'm still usually watching it on TV — DVR. But when it comes to highlights, I'm usually watching it on an iPad." — Barack Obama

Case 5:16-cm-00010-SP Document 16-24 Filed 02/25/16 Page 13 of 13 Page ID #:366

And you're still with the BlackBerry, right?

I use a BlackBerry mainly because I'm so restricted in what I can do that it's basically just messages, and it's still easier for me to tap off the [BlackBerry]. But basically most of my non-work-related stuff, I'm working off the iPad. And the girls all have iPhones, so I can get around an iPhone pretty good.

Do you wear any "wearable shirts" or health devices, or things like that?

Not yet. I think ...

You missed the whole Google Glass thing, by the way.

Well, [laugh] no comment.

And what devices do you think you would use once you leave office? I know you like a selfie stick.

Well, right. As BuzzFeed showed. Actually, the first time I used that was when we were in Hawaii for vacation. My photographer, Pete Souza, had a GoPro, and folks were starting to use selfie sticks.

But do you use any other technology? It's just basically the iPad?

It's basically the iPad, although ... I don't have a Fitbit yet, but I work out hard. Word is that these <u>Apple watches</u> might be a good companion for my workout. So I'm going to see. I'm going to test it out. I don't want to give Tim Cook too big of a plug here ...

Yeah. But you just did. [Laugh]

... until I've actually seen the product. But he tells me it's pretty good.

Kara Swisher: "If there was a hashtag for your administration, what would it be?"

Barack Obama: "#YesWeCan."

Absolutely. Last question: If there was a hashtag for your administration, what would it be? #YesWeCan.

Naturally. Thank you so much.

Great to talk to you. Thank you so much.

* Kara Swisher is married to but separated from Megan Smith, chief technology officer for the Obama administration. See her ethics statement here.

Exhibit X

iCloud: Back up your iOS device to iCloud

anguages	English	▼

iCloud automatically backs up your iOS device information daily over Wi-Fi when your device is turned on, locked, and connected to a power source.

Back up automatically

On your iOS 9 or iOS 8 device: Go to Settings > iCloud > Backup, then turn on iCloud Backup.

On your iOS 7 device: Go to Settings > iCloud > Storage & Backup, then turn on iCloud Backup.

Back up manually

On your iOS 9 or iOS 8 device: Go to Settings > iCloud > Backup, then tap Back Up Now.

On your iOS 7 device: Go to Settings > iCloud > Storage & Backup, then tap Back Up Now.

For information about messages that may appear while backing up, see the Apple Support article Get help backing up your device in iCloud.

Important: If you don't back up your iOS device to iCloud for 180 days or more, Apple reserves the right to delete your device's iCloud backups. For information, see iCloud Terms and Conditions.

Last Modified: Feb 11, 2016

Helpful? Yes No

74% of people found this helpful.

Additional Product Support Information



Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.

Get started >



ightharpoonup Support

Exhibit Y

Case 5:16-cm-00010-SP Document 16-26 Filed 02/25/16 Page 2 of 2 Page ID #:370

From: Wert, David (CAO) dwert@cao.sbcounty.gov

Subject: Re: Media inquiry: Ars Technica Date: February 20, 2016 at 8:26 PM

To: Cyrus Farivar cyrus.farivar@arstechnica.com



Statement from the FBI:

STATEMENT TO ADDRESS MISLEADING REPORTS THAT THE COUNTY OF SAN BERNARDINO RESET TERROR SUSPECT'S IPHONE WITHOUT CONSENT OF THE FBI

Recent media reports have suggested that technicians in the county of San Bernardino independently conducted analysis and took steps to reset an iPhone 5C that was recovered during a federal search following the attack in San Bernardino that killed 14 people and wounded 22 others on December 2, 2015. This is not true. FBI investigators worked cooperatively with the county of San Bernardino in order to exploit crucial data contained on a county-issued iPhone that was assigned to the suspected terror suspect, Syed Rizwan Farook.

Since the iPhone 5C was locked when investigators seized it during the lawful search on December 3rd, a logical next step was to obtain access to iCloud backups for the phone in order to obtain evidence related to the investigation in the days following the attack. The FBI worked with San Bernardino County to reset the iCloud password on December 6th, as the county owned the account and was able to reset the password in order to provide immediate access to the iCloud backup data. The reset of the iCloud account password does not impact Apple's ability to assist with the the court order under the All Writs Act.

The last iCloud data backup to the iPhone 5C was 10/19 and, based on other evidence, investigators know that Syed Rizwan Farook had been using the phone after 10/19. It is unknown whether an additional iCloud backup to the phone after that date -- if one had been technically possible -- would have yielded any data.

Through previous testing, we know that direct data extraction from an iOS device often provides more data than an iCloud backup contains. Even if the password had not been changed and Apple could have turned on the auto-backup and loaded it to the cloud, there might be information on the phone that would not be accessible without Apple's assistance as required by the All Writs Act order, since the iCloud backup does not contain everything on an iPhone. As the government's pleadings state, the government's objective was, and still is, to extract as much evidence as possible from the phone.

Laura Eimiller FBI Press Relations Los Angeles Field Office

Sent from my iPhone

On Feb 20, 2016, at 11:16 AM, Cyrus Farivar < cyrus.farivar@arstechnica.com> wrote:

Cyrus Farivar here, a journalist with Ars Technica. I'd like confirmation that this is indeed the case, that a county employee reset the iCloud account at the request of the FBI. Is there any way that you or someone else from the county can help us piece together a timeline as to what was attempted when? http://mobile.reuters.com/article/idUSKCN0VS2GC Best,

Hello.

Sent from my iPhone

Cyrus Fariyar

http://arstechnica.com/author/cyrus-farivar/

Exhibit Z

No Smartphone Lies Beyond the Reach of a Judicial Search Warrant



Cyrus R. Vance Jr. is the Manhattan district attorney.

Updated February 18, 2016, 3:21 AM

iPhones are the first warrant-proof consumer products in American history. They compel law enforcement to deploy extraordinarily creative prosecutorial strategies – and obtain state-of-the-art tools – to carry out even the most basic steps of a criminal investigation. I applaud our federal colleagues for their commitment to justice for the 14 killed in San Bernardino and their families.

The magistrate judge's order rests firmly on centuries of jurisprudence holding that no item – not a home, not a file cabinet and not a smartphone – lies beyond the reach of a judicial search warrant. It affirms the principle that decisions about who can access key evidence in criminal investigations should be made by courts and legislatures, not by Apple and Google. And it provides the highest-profile example to date of how Silicon Valley's decisions inhibit real investigations of real crimes, with real victims and real consequences for public safety.

Decisions about who can access key evidence in criminal investigations should be made by courts and legislatures, not by Apple and Google.

Our coalition – comprising local law enforcement, crime victims' advocates and concerned community leaders – will be watching with great interest.

But as the encryption debate zeroes in on the cowardly terrorist acts committed in San Bernardino, we should also remember that Apple's switch to default device encryption affects virtually all criminal investigations, the overwhelming majority of which are handled by state and local law enforcement. Our agencies do not have the same resources as the federal Justice Department, which is why a national, legislative solution is so urgently needed.

The line between privacy and security in our society should not be drawn unilaterally by two of the world's most powerful companies – especially when that line coincides with their own economic interests. It should be drawn by Congress and courts, as our Report on Smartphone Encryption and Public Safety makes clear.



Cyrus Vance Jr., Manhattan district attorney

Exhibit AA

Privacy

Our Approach to Privacy

Manage Your Privacy

Government Information Requests Our Privacy Policy

We believe security shouldn't come at the expense of individual privacy.

We regularly receive requests for information about our customers and their Apple devices from law enforcement. We want to explain how we handle these requests.

When we receive information requests, we require that it be accompanied by the appropriate legal documents such as a subpoena or search warrant. We believe in being as transparent as the law allows about what information is requested from us. We carefully review any request to ensure that there's a valid legal basis for it. And we limit our response to only the data law enforcement is legally entitled to for the specific investigation.

Apple has never worked with any government agency from any country to create a "backdoor" in any of our products or services. We have also never allowed any government access to our servers. And we never will.

What we're most commonly asked for and how we respond.

The most common requests we receive for information from law enforcement are in relation to devices and/or accounts. Device Requests generally seek information in relation to Apple devices, such as an iPhone, iPad, or Mac. Account Requests generally seek information in regard to an Apple ID account and/or related Apple services or transactions. We also respond to emergency requests worldwide where Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires immediate disclosure.

All content requests require a search warrant. Only a small fraction of requests from law enforcement seek content such as email, photos, and other content stored on users' iCloud accounts. National security-related requests are not considered Device Requests or Account Requests and are reported in a separate category.

On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices

2/23/2016 6:28 PM 1 of 3

running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

Information Requests

94*

Device RequestsLaw enforcement seeking a stolen device.

6%

Account Requests

Law enforcement seeking personal information.

Read Apple's transparency reports >

Read Apple's guidelines for law enforcement requests US > EMEIA > Japan and APAC >

Device Requests

The vast majority of the requests Apple receives from law enforcement come from an agency working on behalf of a customer who has requested assistance locating a stolen device. We encourage any customer who suspects their device is stolen to contact their respective law enforcement agency.

Account Requests

Responding to an Account Request most often involves providing information about a customer's iCloud account. If we are legally compelled to divulge any information for an Account Request, we provide notice to the customer when allowed and deliver the narrowest set of information possible in response. Not only are a minuscule number of accounts actually affected by information requests, but our stringent review meant Apple only disclosed content in response to 27% of the total U.S. account requests we received during the period from July 1st, 2014 to June 30th, 2015.

Less than

0.00673% of customers have been affected by government information requests.

National Security Orders from the U.S. government.

A tiny percentage of our millions of accounts is affected by national security–related requests. In the first six months of 2015, we received between 750 and 999 of these requests. Though we would like to be more specific, by law this is the most precise information we are currently allowed to disclose.

from the Electronic Frontier Foundation

In its latest "Who Has Your Back?" report, once again the EFF awarded Apple 5 out of 5 stars "commend[ing] Apple for its strong stance regarding user rights, transparency, and privacy."

2 of 3 2/23/2016 6:28 PM

We're always working for greater transparency and protections on behalf of our customers.

We believe transparency and dialogue are the best ways for finding solutions to the overarching impact from surveillance laws and practices. We are continuing to engage with the White House, government regulators, legislators, and courts around the world regarding the importance of protecting customer data and security.

Shop and Learn	Apple Store	For Education	Account	About Apple
Mac	Find a Store	Apple and Education	Manage Your Apple ID	Apple Info
Pad	Genius Bar	Shop for College	Apple Store Account	Job Opportunities
Phone	Workshops and Learning		iCloud.com	Press Info
Watch	Youth Programs	For Business		Investors
ΓV	Apple Store App	IPhone In Business	Apple Values	Events
Music	Refurbished	IPad in Business	Environment	Hot News
Tunes	Financing	Mac in Business	Supplier Responsibility	Legal
Pod	Reuse and Recycling	Shop for Your Business	Accessibility	Contact Apple
Accessories	Order Status		Privacy	
ift Cards	Shopping Help		Inclusion and Diversity	
			Education	
Age wave to shop Visit an	Apple Store, call 1-800-MY-APPLE, or find a	receller		

3 of 3 2/23/2016 6:28 PM

Exhibit BB

BuzzFeedNews

News

Buzz

Life Quizzes

Videos

More ~

Get Our App!







Watch the Try Guys on the new **BuzzFeed VIDEO** app.

Get The App

















FBI Admits It Urged Change Of Apple ID Password For Terrorist's iPhone

Apple executives face a court order to help create what the company calls a "backdoor" to the phone. [Update: San Bernardino County officials said the FBI had requested the Apple ID password reset of Syed Farook's phone, which the FBI acknowledged Saturday night.]

Originally posted on Feb. 19, 2016, at 5:49 p.m. Updated on Feb. 21, 2016, at 2:01 a.m.



John Paczkowski Managing Editor, BuzzFeed San Francisco



Chris Geidner BuzzFeed News Reporter















Andrew Burton / Getty Images

The Apple ID password linked to the iPhone belonging to one of the San Bernardino terrorists was changed soon after the government took possession of the device, Apple, San Bernardino County, and federal officials have acknowledged over the past 48 hours. If that password change hadn't happened, senior Apple executives said on Friday afternoon, a backup of the information the government was seeking may have been accessible.

BuzzFeednews

In The News Today

- Donald Trump is marching toward the U.S. Republican presidential nomination: He won last night's Nevada caucuses us
- A small plane carrying 23 people has crashed in Nepal due to bad weather.
 There are no survivors, police say.
- And do you want to give something more than just a like? Facebook is rolling out five new reactions today in the form of emojis (a)

Get The News App

BuzzFeednews



German Refugee Camp Accused Of Sexual Assault

by Jina Moore

Connect With BuzzFeed USNews

f Like Us On Facebook

Follow Us On Twitter



News moves fast. Keep up with the BuzzFeed News daily email. The dispute over retrieving the contents from Syed Rizwan Farook's phone broke into the open earlier this week, part of the government's investigation into the Dec. 2, 2015, attacks that left 14 dead.

Your Email Address

Sign up



Syed Rizwan Farook FBI Handout / Getty Images

Now, the government, through a court order, is demanding Apple build what the company considers a special backdoor way into the phone — an order that Apple is challenging. The government argues Apple would not be creating a backdoor.

The Apple executives said the company had been in regular discussions with the government since early January, and that it proposed four different ways to recover the information the government is interested in without building a backdoor. One of those methods would have involved connecting the iPhone to a known Wi-Fi network and triggering an iCloud backup that might provide the FBI

with information stored to the device between the October 19th and the date of the incident.

Apple sent trusted engineers to attempt that method, the executives said, but they were unable to do it. It was then that they discovered that the Apple ID password associated with the iPhone had been changed sometime after the terrorist's death — within 24 hours of the government taking possession of the phone. By changing the password, the government foreclosed its ability to obtain a fresh copy of the most recent device data via this back-up-to-known-wifi method.

The FBI had claimed in a court filing on Friday that the password was changed by someone at the San Bernardino Health Department, writing, "[T]he owner, in an attempt to gain access to some information in the hours after the attack, was able to reset the password remotely."

On Friday night, however, the San Bernardino County's official Twitter account stated, "The County was working cooperatively with the FBI when it reset the iCloud password at the FBI's request."



County spokesman David Wert told BuzzFeed News on Saturday afternoon the tweet was an authentic statement, but he had nothing further to add.

The Justice Department did not initially respond to repeated requests for comment.

More News



Quinton Tellis Indicted For Capital Murder In Burning Death Of Jessica Chambers



Kalamazoo Shooting Suspect Admits To Deadly Spree, Prosecutor Says



Arizona To Death Row Inmates: You Don't Have A Right To Go Viral



3 Dead, States Of Emergency Declared As Tornadoes Sweep Southeast



Republicans Vow To Not Hold Hearings On Obama's Supreme Court Nominee



Lark & Ro. Ava & Viv. Here's Why So Many Fashion Labels Sound The Same

Late Saturday night, more than 24 hours after Apple's Friday briefing, the FBI confirmed the county's account in a statement. "The FBI worked with San Bernardino County to reset the iCloud password on December 6th, as the county owned the account and was able to reset the password in order to provide immediate access to the iCloud backup data," the agency said in a statement.

The FBI downplayed the effect of the password reset, however, claiming that it "[does] not impact Apple's ability to assist with the the court order under the All Writs Act," and adding that "the government's objective was, and still is, to extract as much evidence as possible from the phone."

A senior Apple engineer countered the FBI's assertions late Saturday night telling BuzzFeed News that the agency's explanation acknowledged that its changing of the Farook's Apple ID password prevented the auto backup and that such backups do indeed have value. As such, the engineer continued, the reset closed off an avenue through which the FBI might have been able to gather information.

Had this password not been changed, Apple senior executives said Friday, the government might not have needed to demand the company create a "backdoor" to access the iPhone used by Farook, who died in a shootout with law enforcement after the attack. Following up on a court order that had been granted earlier in the week, the Department of Justice filed a motion to compel Apple to create the backdoor earlier Friday.

The Apple senior executives spoke with reporters on Friday afternoon to respond to the government's filing, noting that the government had opened the door to discussion of Apple's prior efforts in the case by disclosing those actions in its Friday filing.

Creating backdoor access to Farook's iPhone, the executives said, would put at risk the privacy of millions of users. It would not only serve to unlock one specific phone, they said, but create a sort of master key that could be used to access any number of devices. The government says the access being sought could only be used on Farook's device, but Apple's executives said that there is widespread interest in an iPhone backdoor, noting that Manhattan District Attorney Cyrus Vance said Thursday that his office has 175 Apple devices he'd like cracked. Apple's executives also claimed that no other government in the world — China included — has ever asked the company for the sort of FBiOS the government is demanding that it build now.

Asked why the company is pushing back so hard against this particular FBI request when it has assisted the agency in the past, Apple executives noted that the San Bernadino case is fundamentally different from others in which it was involved. Apple has never before been asked to build an entirely new version of its iOS operating system designed to disable iPhone security measures.

The Apple senior executives also pushed back on the government's arguments that Apple's actions were a marketing ploy, saying they were instead based on their love for the country and desire not to see civil liberties tossed aside.

The U.S. Department of Justice has not yet responded to a request for comment.

UPDATE

This story was updated on Saturday to include information regarding a statement issued by San Bernardino County. Feb. 20, 2016, at 2:51 p.m.



Kesha's Attorney Says Dr. Luke Is "Out To Destroy Her"



This Woman Is Fighting Zika By Dumping Mutant Mosquitoes Out Of A Van



Utah Senate Committee, Led By Republicans, Passes Bill To End The Death Penalty

More News >

Now Buzzing



21 Things Every Couple Who Really Loves Food Will Understand



These Two Tests Will Reveal Your Sex Strength And Weakness



25 Adorable Pairs Of Rain Boots That You Could Wear All Day

UPDATE

This story was updated early Sunday morning with news information provided by the FBI and a response from an Apple official. Feb. 21, 2016, at 2:01 a.m.

DOJ Calls Apple's Refusal To Unlock iPhone A Marketing Stunt

buzzfeed.com

Apple's FBI Privacy Fight Is A Battle For Our Trust

buzzfeed.com

Apple Helped The Government Extract Data Before. Here's Why Things Are Different Now

buzzfeed.com

John Paczkowski is the managing editor for BuzzFeed San Francisco. Formerly deputy managing editor for Re/code and AllThingsD, he's been covering the intersection of technology and culture since 1997.

Contact John Paczkowski at John.Paczkowski@buzzfeed.com.

Chris Geidner is the legal editor for BuzzFeed News and is based in Washington, D.C. In 2014, Geidner won the National Lesbian & Gay Journalists Association award for journalist of the year.

Contact Chris Geidner at chris.geidner@buzzfeed.com.



NEXT ON BUZZFEED NEWS>

More •

Meet Blindy, The Inspirational Blind Penguin Who Is...



This Skillet Mac And Cheese Is The Ultimate Easy Meal



11 Actually Interesting Selfie Facts
Everyone Should Know But Doesn't



21 Cheap And Easy Decorating Tricks For Renters



What Is Your Oscars® IQ?



Maximus The Police Dog Is The Adorable Instagram Account You Need To Follow



Let's Not Get Carried Away With That "Trump Won Latinos" Entrance Poll



21 Of The Best Subscription Boxes For Beauty And Health Addicts



Which Awards Show Blunder Is Basically You Always?

Date Set For Apple-FBI Court Showdown Over Terrorist's iPhone

Terrorist Reportedly Detained In Somalia

After Reading His Emails?

Former Virginia Cab Driver Turned FBI Most-Wanted

Boston Terrorist Suspect Says ISIS Is "Doing A Good

Did The FBI Transform This Teenager Into A Terrorist

Celebrity faux pas are all of us...just in nicer clothes. Make sure to stay on top of all the must-see moments this awards season with DIRECTV.





Facebook Rolls Out Reaction Buttons Today



23 Things Everyone Did On The School Computers



16 Adorable Pet Names Couples Have For Each Other

More Buzz >

MORE BUZZ



Tagged:apple, applefbi, fbi, syed farook

Advertise Jobs Mobile Newsletter

US Edition

US Edition

About Press RSS Privacy User Terms Ad Choices Help Contact

© 2016 BuzzFeed, Inc



Exhibit CC

The Washington Post

National Security

FBI asked San Bernardino to reset the password for shooter's phone backup

By Ellen Nakashima and Mark Berman February 20

In the chaotic aftermath of the shootings in San Bernardino, Calif., in December, FBI investigators seeking to recover data from the iPhone of one of the shooters asked a technician in the California county to reset the phone's iCloud password.

But that action foreclosed the possibility of an automatic backup to the Apple iCloud servers that might have turned up more clues to the origins of the terrorist attack that killed 14 people.

"The county and the FBI were working together cooperatively to obtain data, and at the point when it became clear the only way to accomplish the task at hand was to reset the iCloud password, the FBI asked the county to do so, and the county complied," David Wert, a spokesman for San Bernardino County, said in an email.

The Justice Department disclosed the apparent misstep in a court filing Friday, which is part of a larger, high-stakes battle over whether the government can use the courts to force Apple to create software to help it unlock a customer's iPhone — in this case, one used by Syed Rizwan Farook. Farook, a county health worker, and his wife were killed in a firefight with police hours after the Dec. 2 attack.

"This was happening hours after the worst terror attack since 9/11, and there were still credible reports of a third shooter," said a federal law enforcement official, speaking on the condition of anonymity to discuss an ongoing investigation. "It was a very dynamic time, and the number one priority was figuring out what happened and if there were more attacks coming."

According to senior Apple executives, the FBI's first call to Apple for help came on Saturday, Dec. 5, at 2.46 a.m. With a subpoena, the bureau obtained subscriber data and other details. On Sunday, the FBI, with a warrant, obtained data from Farook's iPhone that had been backed up to iCloud. That backup contained information only through Oct. 19, six weeks before the attack.

The same Sunday, the FBI asked the county for help in retrieving data from the phone, Wert said in an interview. "So the county said we could get to the information on the cloud if we changed the password or had Apple change the password," he said. "The FBI asked us to do that, and we did."

It is not clear why the FBI needed to reset the password if it was able to obtain the backed-up data from Apple.

Nonetheless, by resetting the password, the county, which owned Farook's phone, and the FBI eliminated the possibility of seeing whether additional data beyond Oct. 19 might be recovered from the phone through the auto-backup feature, experts said.

The FBI in a court filing said Farook "may have disabled" the auto-backup. But, tech experts said, there might be other reasons the phone did not back up: It was not near a WiFi network it was familiar with, such as his home or workplace, or it was not turned on long enough to back up. With the password changed, it is impossible to know.

"Even though it has been reported that the iCloud backups were disabled, there still is data that may have been recoverable," said security expert Dan Guido, chief executive of Trail of Bits. Depending on the phone's settings, it might have synched notes, emails, address books — perhaps geolocation data — with the company's network.

In a statement Saturday night, an FBI spokesperson said the bureau's goal "was, and still is," to extract as much evidence as possible from the phone. Tests previously conducted by the FBI showed that "direct data extraction" from Apple's mobile devices often yields more data than an iCloud backup, the spokesperson said.

"Even if the password had not been changed and Apple could have turned on the auto-backup and loaded it to the cloud, there might be information on the phone that would not be accessible" without Apple's help, the spokesperson said.

The <u>showdown between Apple</u> and the government arises out of the FBI's inability to recover data from Farook's phone, especially for the weeks prior to the attack. The Justice Department on Tuesday got a federal judge to order Apple to build software to override an auto-wipe feature on the phone that deletes data after 10 failed tries to enter a password. The FBI could then try to crack the phone's password by "brute force," making many attempts without risking the wiping of the data.

"chilling" pred	Apple chief executive Tim Cook said the firm would challenge the order, warning that it would set a 'chilling" precedent that could lead to more invasive requests for data. On Friday, the Justice Department fired back, charging that Apple's stance was motivated by "marketing" concerns as it promotes itself as a protector of consumer privacy.				
	Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.				
	Mark Berman covers national news for The Washington Post and anchors Post Nation, a destination for breaking news and stories from around the country.				

Exhibit DD

		1			
1	UNITED STATES DISTRICT COURT				
2	EASTERN DISTRICT OF NEW YORK				
3	X				
4	ORDER REQUIRING APPLE INC				
5	TO ASSIST IN THE EXECUTION				
6	OF A SEARCH WARRANT				
7	ISSUED BY THE COURT, ET AL				
8	15 MC 1902				
9	X				
10	United States Courthouse				
11	Brooklyn, New York				
12	October 26, 2015 11:30 o'clock a.m.				
13	TT.00 0 CTOCK d.m.				
14	TRANSCRIPT OF ARGUMENT BEFORE THE HONORABLE JAMES ORENSTEIN				
15	UNITED STATES MAGISTRATE JUDGE				
16	APPEARANCES:				
17	For the Government: ROBERT L. CAPERS United States Attorney				
18	271 Cadman Plaza East Brooklyn, NY 11201				
19	BY: SARITHA KOMATIREDDY				
20	LAUREN H. ELBERT AMEET KABRAWALA				
21	Assistant US Attorneys				
22	For Apple: ZwillGen				
23	1900 M Street NW Washington, DC 20036				
24	BY: MARC J. ZWILLINGER, ESQ.				
25	JEFFREY LANDIS, ESQ.				

GR OCR CM CRR CSR

2 1 Court Reporter: Gene Rudolph 225 Cadman Plaza East 2 Brooklyn, New York (718) 613-2538 3 4 Proceedings recorded by mechanical stenography, transcript produced by computer-aided transcription. 5 6 7 8 9 THE CLERK: Civil cause for oral argument, 15 Miscellaneous 1902, In Re Order Requiring Apple Inc to 10 Assist in the Execution of a Search Warrant. 11 12 THE COURT: Good morning. 13 May we have the appearances, please? For the 14 government? 15 MS. KOMATIREDDY: Good morning, Your Honor. Saritha Komatireddy for the United States. 16 17 joined by Lauren Elbert and Ameet Kabrawala, both Assistant 18 United States Attorneys. 19 THE COURT: Welcome to all of you. 20 MR. ZWILLINGER: Good morning, Your Honor. 21 Marc Zwillinger for Apple. I am joined at counsel 22 table with my colleague Jeffrey Landis. 23 THE COURT: Good morning to both of you. 24 All right, folks. First I want to thank you all for 25 the briefing that you have provided, very informative, very

GR OCR CM CRR CSR

helpful. I know it has been on a somewhat quick schedule, so I appreciate that. It's really helped me get a handle on some of these issues and also made it clear to me how very close some of them are, to my mind.

I will have some questions for both sides as we go along but I do want to hear from you. As we get started though I want to bring to your attention something that one of my colleagues alerted me to because I do intend to ask about it. I will ask my deputy to hand a copy down.

It is a letter from the government and some testimony in a hearing before Judge Johnson in a case in this district. The letter is dated July 9, 2015, and the testimony was taken on September 3rd of this year in United States against Djibo.

I bring it to your attention because the basic assertion on the part of the government that brings us here is the proposition that the iPhone at issue here is one that the DEA and FBI have tried and failed to unlock because of the pass code and the government expands from that in its brief to say that the government, broadly speaking I suppose, is simply unable to unlock the phone at issue here.

So the reason I bring the Djibo materials to your attention is because on page five of the letter the government writes, HSI, Homeland -- Department of Homeland Security -- I always forget what the I stands for. In any event, HSI is in

possession of technology that would allow its forensic technicians to override the pass codes 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 pass code, they would nevertheless have been able to obtain the records stored in the subject iPhone using specialized software. The software works to bypass the bi-code 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.

Then in the testimony in the Djibo case the government's forensic expert expanded on that and explained something about how it works, including under cross-examination by the defendant's counsel in that case, and made clear that the software version in that case was running -- the iPhone in that case was running, the software version of IOS 8.1.2, if I am not mistaken.

I am giving this to you now. I learned of it since your briefing. If you have some thoughts on it I am happy to hear it but I don't want to put you on the spot. I want you to know that this has come to my attention and I'll, of course, afford both sides here an opportunity to submit something further on it if they like.

That's where I am starting from. I am going to have a number of questions, I'm sure. But Ms. Komatireddy, or one

5 1 of your colleagues, or whoever wants to be heard, why don't 2 you start. 3 MS. KOMATIREDDY: Thank you, Your Honor. 4 We would like to make some introductory remarks and of course we are happy to answer any questions the Court may 5 6 have. 7 THE COURT: Yes. 8 MS. KOMATIREDDY: In this case, the most important 9 thing to remember is that a federal court issued a federal 10 search warrant commanding agents to search a phone for 11 evidence of crime, a crystal meth conspiracy. THE COURT: The search warrant has expired over a 12 13 year ago, correct? 14 MS. KOMATIREDDY: There were two search warrants There was one search warrant issued in 2014. 15 issued. 16 THE COURT: That is the one attached to the 17 application. 18 MS. KOMATIREDDY: No, sir. The first search warrant was for the home and the devices. 19 20 THE COURT: No. I am talking about the one attached 21 to the application now before me. 22 MS. KOMATIREDDY: Yes. 23 THE COURT: I should note, by the way, the 24 application said it is attached as Exhibit A. It is not on 25 It should be. I will ask you to correct that. the docket.

CaSasta: 1161tann 109**019**03 PJOD document 1161**9**1 Fifteld 1*02275*156 Pages 670 688 8 Pages 11 46**3**94 6 But it was attached to the email by which I initially got the 1 2 application. 3 Anyway, that warrant has expired over a year ago, 4 hasn't it? MS. KOMATIREDDY: The warrant was issued July 6th. 5 It has to be executed within two weeks of the issuance date. 6 7 With electronic evidence you can initiate the execution of the search warrant by attempting to search the device, turning it 8 9 on and placing it in airplane mode. The agents here began 10 that search but were unable to complete that search because of 11 the password bypass. 12 THE COURT: So you are saying it's already started 13 and you can finish it at any time? 14 MS. KOMATIREDDY: Yes, sir. THE COURT: I am not sure I agree with that. 15 don't think it matters a bit. Even if it expired, I would 16 17 assume that you are making a request for a renewed warrant. 18 But it does raise the question, why is it the 19 government waited from July of 2014 until October of 2015 to 20 ask Apple for this assistance as recounted in your brief only 21 then to tell me that you need me to issue an expedited 22 decision. 23 MS. KOMATIREDDY: Fair enough, Your Honor.

The government, as noted in the brief, there are two agencies involved in this case, the DEA and the FBI.

24

25

first primarily attempted to enter into the phone using its own technology. After being unable to do so, it consulted with the FBI.

I want to note that there were ten cellphones seized from the defendant's home. That search warrant at issue on July 6th was for all ten cellphones. They were in the process of executing a search warrant on the other phones. That took some time. It also took some time for the government to explore the reasonable alternatives available to it in order to execute the search warrant without having asking for third-party assistance.

Once it determined, both agencies determined that they could not get into the phone without Apple's assistance, the government reached out to Apple. I do think it's important to note the government reached out to Apple first before ever applying for any relief in this Court and asked if it could bypass the pass code and do so within time for trial. Apple stated that it could and would with a Court order and stated that it would do within one to two weeks. To accommodate the revised schedule here in the briefing, Apple now stated it can actually do it in one day. That's the turnaround time we now expect.

In that process of those conversations, Apple provided the government with specific language from its legal process guidelines that it required, that it insisted on,

GR OCR CM CRR CSR

requested for what it would consider an order that it could follow in executing the government's request for assistance. When the government applied to this Court for and order, it used that language.

Now, this was a textbook example of Apple's long-standing and responsible corporate practice of bypassing locked cellphones when it has a Court order requiring it to do so.

Since 2008, our initial estimates are that Apple has received at least 70 court orders requiring it to assist in this manner, has never objected to them and has complied. I'm sure counsel for Apple has the exact number available for you. That number is based on an initial survey, an ongoing query of government prosecutors around the country.

THE COURT: I take it, that fact, you are not saying, I don't think you are saying, that it constitutes any sort of waiver. It's really just a question of burden.

MS. KOMATIREDDY: That is correct. It's not a waiver per se.

It's worth noting that Apple in that process since 2008, and we quoted the very first email we have on record, where Apple provided this guidance, throughout that time period it had an established procedure for routinely taking in these requests, complying with them, processing them and informing the public about this practice by continually

publishing and updating its legal process guidelines.

During that same timeframe that it has been processing these requests Apple has grown to become the biggest company in the world. So plainly any burden in terms of employee resources or time or reputation was minimal.

The government's application in this case followed that same template, that same routine procedure. It was not secret. It was not new. It did not invoke any new legal authority. It did not seek any new broad surveillance authority. It did not ask Apple to create any capability that it did not already have. It was just a simple routine request for assistance in carrying out a valid search warrant issued by a federal court, as Apple has done so many times before.

For years Apple has provided this assistance and until two weeks ago Apple indicated to the government that it would provide that assistance again in this case. Apple's position in Court today represents what we consider to be a stunning reversal of that position, and Apple's stated reason for this reversal is a concern for its brand. This is unfortunate. American consumers should expect that American companies protect their privacy and their safety.

THE COURT: Your brief goes to a surprising length to questioning the patriotism of a company that stands on its rights in this way. Whether I agree or disagree with it really doesn't help me resolve the legal issue. But it does

create an atmosphere I think that, it isn't helpful. You don't think they are patriotic to question. You have made that clear in your brief. I'd really just as soon focus on the legal question.

MS. KOMATIREDDY: It's not a question of patriotism, Your Honor. It's a suggestion, Apple states in its brief that it is happy to -- it takes seriously its responsibility of assisting where there is legal access, there is a legal form of access to data, and it takes a stand against improper access. There is no improper access here. There is a valid federal search warrant.

Of course, we welcome this debate and we welcome the opportunity to explore these issues but we are a little bit surprised only because in this case -- Apple has for a long time complied with lawful Court orders requiring and requesting exactly what we are requesting in this case.

THE COURT: I take it -- forgive me for interrupting. I take it, there is no question that, leaving aside any possibility of an appeal to the higher court, if the end result of this case is a court order that Apple must do what the government seeks, Apple is going to comply here, right?

MR. ZWILLINGER: That is correct, Your Honor. Apple would comply with an order of this court.

THE COURT: Okay. That's why I am not sure I

understand. You are not saying that there is some sort of waiver or estoppel based on past practice. I am not sure that what Apple has done before goes to anything other than giving some insight into the burden.

MS. KOMATIREDDY: That's exactly right, Your Honor.

THE COURT: I get that.

MS. KOMATIREDDY: I want to add one more point, Your Honor, which is the comment on what American consumers expect for the company. It's not a comment about patriotism. It's a comment on what Apple has perceived as damage to their brand. This Court shouldn't condone the notion that a company has a negative impact on its brand when it follows US law or that --

THE COURT: It is such a tendentious way of putting things. It's just not going to help me.

Look, there is a wonderful argument to be made, as you make it, that Americans expect that corporate citizens will comply with law. Apple will do so here. There is no question about it.

But there is a competing interest that they have identified and, I take it, you would acknowledge that any private entity called on to be pressed into service by the government is in the best position to identify what its interests are, whether or not they should give way to them. They are in the best position to tell us, here is what we value, here is what is important to us. You may say well,

that's not a good value. We don't think Americans share that value, all right thinking Americans at least.

How does it help me understand the legal issue here?

MS. KOMATIREDDY: It is a comment on the burden,

Your Honor. Our position is, it doesn't actually damage the brand. There is not actually a burden in terms of reputational burden.

THE COURT: Is that based on any kind of data, any evidence or is it just -- it can't be that people won't appreciate it if Apple complies with the law and helps you promote an investigation.

MS. KOMATIREDDY: It's based on a couple of things.

First, in the last seven years Apple has published its practice of complying with these sorts of orders, providing assistance to law enforcement to get into locked phones when there are valid search orders. That practice has been public. It's reasonable to assume that customers have been aware of that. Even a cursory search of Apple support blogs or discussion forums --

THE COURT: So why did the government announce that it's not seeking to seek backdoor legislation?

MS. KOMATIREDDY: That is a separate issue. Here, this is not a backdoor.

THE COURT: It's not a backdoor. It's the same basic idea, which is the government for reasons sufficient to

itself -- this is another reason why I don't think it is useful to have the conversation about whose values are better. But the government announced a decision, surprisingly unknown to me, on the same day that this application was made that they are not going to seek authority from Congress to require a company like Apple to provide access that gets past password or encryption.

If you are saying that look, all right thinking
Americans are going to want a company like Apple to do just
that, I don't understand why the government would balk at
asking Congress to require it.

But it doesn't matter. The question is, Apple says it is a burden. If you can say look, here is some evidence that shows it really doesn't hurt them, we have done some market research or they have and they are not telling you about it, I get it. But if it is just look, we don't think Americans would like this, I understand the argument. You have made it well. But what more does it get me?

MS. KOMATIREDDY: I think the basic point, you are right, Your Honor, that the -- whether or how the government sought backdoor legislation is irrelevant. The basic point --

THE COURT: That's what I said? Okay.

MS. KOMATIREDDY: Here -- the basic point here is,
Apple has been doing this for a long time and it has been
public for a long time. The brand hasn't hurt. That is

1 evidence in itself there is no reputational burden. 2 THE COURT: Okay. You are saying the brand hasn't 3 been hurt because it's grown, the company? 4 MS. KOMATIREDDY: The company has grown. THE COURT: You have done some regression analysis 5 6 that factors out other things that may affect the value of the 7 brand? 8 MS. KOMATIREDDY: I have not, Your Honor. 9 THE COURT: Okay. Why don't you move on to another point then. I think I understand this one. 10 11 MS. KOMATIREDDY: Okay. The Court has made 12 several -- made observation that Congress although it didn't 13 expressly ban what -- the assistance that the government is 14 requesting here, that there is not a gap in the law because recent debate has shown that Congress has refused to authorize 15 16 what the government is requesting here. We believe that the 17 Congressional statements that have been made so far are just 18 that, a few Congressional statements, a few proposed bills, 19 but no actual legally cognizable action. 20 THE COURT: I had a question about that. This I 21 think gets to the heart of one of the most important issues, 22 which is the applicability of the act. 23 You are saying, that what we have here is 24 Congressional silence and silence is meaningless. 25 MS. KOMATIREDDY: Yes, Your Honor.

THE COURT: If I mischaracterizing, please do correct me.

What level of Congressional action or inaction speaks loudly enough for the Court to take into account in deciding whether there is some gap that the All Writs Act fills?

MS. KOMATIREDDY: Actual law.

THE COURT: So short of Congress passing a law prohibiting what you want here, it's fair game? Anything else that Congress may have done in terms of considering legislation one way or the other, because it doesn't result in a statutory prohibition, wouldn't be enough to say, it's off limits for the All Writs Act?

MS. KOMATIREDDY: Yes. Short -- essentially yes.

Because all that Congress has done so far here is start a debate. There are 535 members of Congress. A few have commented. A few have heard testimony, and there are four proposed bills. The four proposed bills that the Court cites in its opinion never even were voted on. They were referred to committee and died there.

THE COURT: How far does this go? This won't be the last time the government seeks to use the All Writs Act, and as we all know by now, pretty thin list of cases that provide guidance. So how far does this go?

If, for example, Congress voted decisively to reject

GR OCR CM CRR CSR

a bill that would explicitly confer the authority that you want the Court to allow here, took a vote on a bill and rejected it, 434-to-1, is that still Congressional silence because you can't parse why people voted against it?

MS. KOMATIREDDY: I think so, Your Honor. The reason is this. Because if there is a Congressional will to actually prohibit this practice, those 435 people could simply pass a law prohibiting it. In fact, Your Honor has actually cited three bills that have been proposed in the current Congress to ban the exact access we are requesting here. Those bills were not passed. They did not get out of committee. They were not the subject of floor debates. They got no traction. That can reasonably be read as Congress saying for now, for whatever reasons, all 435 people have, for now the status quo should remain.

It's also reasonable to assume Congress is aware of the government practice of government obtaining All Writs Act orders and aware of that background when it makes the decision to act or not act. In fact, when you look at the hearings that Your Honor cited, part of the testimony at one of those hearings actually made clear that testimony by the FBI executive assistant director made clear that in the past companies had the ability to decrypt devices when the government obtained a search warrant and a court order. Congress is aware of that practice. The debate that was going

on about the so-called going dark issue was about when you get a Court order, the company not being able to get into a device and whether there should be legislation to address that.

So I think with all of that in mind, given that Congress doesn't have a developed debate on this, in fact a debate I would say is preliminary, there are no bills that went past committee and in fact bills that were proposed to prohibit this practice were not passed, were not debated, were not voted on. All that's left is the status quo.

THE COURT: Last -- not last probably, but one more question on how far does this go.

Another variation on the scenario I posed before. If you have -- a bill goes through Congress that started out with language conferring the authority you seek here, and unanimous agreement to strip it out of the bill before it is passed, so we still don't have legislation one way or the other on it. We have a very clear record to take it away from a bill that otherwise would have it. Still Congressional silence that makes it fair game for a Court to grant the authority under the All Writs Act?

MS. KOMATIREDDY: The hypothetical is, that there is language to prohibit what we are requesting?

THE COURT: No. Say the government can force a company like Apple to break into one of its phones, where the user won't and has forgotten the password. So basically, this

case codified as part of a larger bill and that provision is unanimously stripped out before it passes. So we still have the same statutory regime that we have now but we have everyone in Congress voting to take away something that would give you this authority.

Still Congressional silence?

MS. KOMATIREDDY: It is, Your Honor, because everyone in Congress could easily vote the other way.

Everyone in Congress could easily make an affirmative law that states that it grants this authority.

THE COURT: Okay. If in doing that they say you know what this is a separate bill. We are going to do it next week. It's on the agenda. We are going to vote on it in the intervening week; still can do this under the All Writs Act?

MS. KOMATIREDDY: Yes, sir.

THE COURT: Okay.

MS. KOMATIREDDY: Because Congressional silence is Congressional silence. There are a number of examples of Congress considering bills and doing nothing about them. But that doesn't undermine the current legal authority. A simple example is the House has passed at least 30 times a bill seeking the repeal of the Affordable Care Act. That doesn't undermine the Affordable Care Act's reasonable effect.

THE COURT: Obviously the concern is as Congress goes longer and longer due to influences we are all familiar

with that we needn't rehearse here, it goes longer and longer without revisiting statutes that are daily getting more and more outstripped by the technology. It's taking -- this use, this proposed use of the All Writs Act takes away the legislative authority from Congress and puts it squarely in the courts. It just seems to be so at odds with the separation of powers that we have that it's hard to believe that it squares with the intent of the All Writs Act.

MS. KOMATIREDDY: The All Writs Act was passed as parts of the Judiciary Act of 1789. Some call it antiquated. It's actually foundational. It comports with the separation of powers.

THE COURT: It initially passed in 1789. It has been updated as recently -- Congress passed this version in 1949.

MS. KOMATIREDDY: Right.

My point is, when Congress created the federal courts it also ensured that whatever orders the federal courts issued it could make those orders effective. If federal court issues a search warrant, it could to do what it needed to make that search warrant effective if doing so was reasonable, didn't cause unnecessary burden, there were no alternatives to the government, et cetera.

So with that in mind it's not unreasonable for a Court to do what is necessary to effectuate its orders. I

don't think that affects separation of powers.

As to Congress moving too slowly and therefore delegating what the Court may consider undue authority to the judiciary on this matter, Congress also has to engage in its own agenda setting and prioritization. Given the number of issues that they have to take up, if they feel -- assuming background knowledge that Congress legislates against the background of current law, if they realize and know how current law operates, which is reasonable to assume they do in this case, and they are fine with it operating the way that they are, there is no reason for them to prioritize this particular issue at the top.

In fact, that's what you are seeing here. Because this application is about IOS 7 and before, which in a few years will probably be an obsolete issue. In a few years Apple devices aren't even going to carry IOS 7. So the --

THE COURT: I hope so. I hope they won't. Because the Court here won't let me update to eight. Definitely won't let me get nine.

But go ahead.

MS. KOMATIREDDY: You see my point, Your Honor.

Because this particular issue is actually probably dwindling in importance. It's reasonable for Congress to let the All Writs Act continue to apply and debate what it has been debating, the more salient issue of the future of IOS 8 and

beyond and devices where even when you have a court order you cannot get access.

THE COURT: One other slightly different question about the Congressional silence here. Do we actually have Congressional silence? This is something where I can really use your help. I acknowledge, I could so easily be getting it wrong.

Under CALEA, two related questions. First, Verizon is a, or AT&T, they are clearly covered by CALEA.

MS. KOMATIREDDY: Yes, Your Honor.

THE COURT: If they were to manufacture the same kind of device with the same sort of software carrying password encryption, would Calea's provision against forcing a provider, telecom carrier to engage in this decryption, prevent the Court from ordering Verizon to do what you want Apple to do?

MS. KOMATIREDDY: CALEA wouldn't address that situation because CALEA only requires the telecommunications carriers retain the capability to intercept realtime communications, data and motion. Think Title III wiretap.

THE COURT: No. I know what it requires them to do.

But I thought -- this is where my own note-taking has failed

me. I thought there was a provision in CALEA that

specifically addressed decryption and it exempted from other

obligations of a telecom provider any obligation to provide

Casasta 161577700901902PJOD document 116191 Filited 102275156 Page 22306888 Page 40 48410 22 such encryption services. 1 2 MS. KOMATIREDDY: There is a provision in the House 3 and Senate reports that accompanied CALEA where it 4 states -- Congress states that telecommunications carriers 5 have no responsibility to decrypt encrypted communications that are the subject of court ordered wiretaps unless the 6 7 carrier provided the encryption and can decrypt it. 8 In essence, when considering those realtime 9 communications that are being intercepted on a prospective 10

Title III wiretap, the provider has the obligation to decrypt communications that it is capable of decrypting but not otherwise.

(Continued on next page.)

15 16

11

12

13

14

17 18

19

20

21 22

23

24

25

-	Proceedings	-	
---	-------------	---	--

THE COURT: Okay. And that may moot the second question. I will tell you what I have in mind. On any of this, both sides, if there is something that you think that needs a supplemental submission, you know, I welcome it. We can talk about scheduling for that later. I'm sensitive to the need to expedite.

Is Apple an information service within the meaning of CALEA? The reason I ask, because I have that sort of-- the understanding, maybe mistaken, that I asked just a moment ago, whether decryption, there is an exception for decryption.

But, so, does Apple qualify as information service, within the statute?

MS. KOMATIREDDY: Your Honor, I don't believe it does. I am just looking for the specific statutory definition. CALEA's definition of information service restricts it to telecommunications carrier, classic public utilities, not device manufacturers.

THE COURT: Okay.

That was a very long diversion from what I-- an argument you were making, if you can find your place, I welcome you going back to it.

MS. KOMATIREDDY: Fair enough.

THE COURT: If not, I have other questions I could ask. I wanted you to get to your points.

MS. KOMATIREDDY: I'm a happy to answer any

0CR

RB

questions from the Court. We will rely on our briefs for our legal basis.

THE COURT: Okay. Then I will -- I have to go through my notes.

One of the things, just about the burden, I apologize, I will skip around. You stated the vast majority of cases, where you have gotten assistance from Apple and have been resolved without Apple having to testify. That makes intuitive sense.

Where they have been required to testify, what kind of level of detail is required to authenticate what you get from their services. Does it ever put them in the position of having to reveal something that is a trade secret or something like that?

MS. KOMATIREDDY: Interesting question, Your Honor.

In our survey so far of Government prosecutors, we have not actually identified a specific instance where they have been required to testify. I have had many prosecutors in those 70-cases say, they were not. A few say, yet to be determined because the cases are not yet resolved. Perhaps Apple's counsel has an example.

THE COURT: If you don't mind, do you have a number?

MR. ZWILLINGER: We believe that Apple has been required to testify about twenty times, in cases where they have done these device extractions in the past. It is not a

- Proceedings -

comprehensive count either, that is asking the people who have gone to testify.

THE COURT: Do you know if there has ever been an issue in any of those cases, where the nature of the testimony has itself implicated Apple's interests?

MR. ZWILLINGER: From Apple's perspective there is an issue in all cases, to the extent, to prepare people to testify to not go into information that would implicate Apple's proprietary interests. But, they have managed to find a way to introduce some testimony.

THE COURT: In terms of the burden, it is not a realistic prospect that if you're ordered to do what the Government wants here, at the trial in the case, you are going to have to reveal, how to break a pass code for example.

MR. ZWILLINGER: The burden would not be that that would impose, you know, it would infringe Apple's proprietary interests.

On the other hand, in the cases where Apple doesn't have to testify, there is still significant back and forth, signing of declarations, negotiating stipulations. It is not that every case, where they do a bypass involve the several hours process of a bypass, there is usually extensive work after that, even in cases where they don't have to testify.

THE COURT: Ms. Komatireddy, a separate issue that I'm struggling with here. Just in terms of how the analysis

goes.

There seems to be sort of two halves to the analysis, one is, does the act apply at all. And the second is, if it applies, then we are under New York Tel and the three prong test.

There is a part of the burden analysis that keeps -I keep losing my place, trying to figure out if-- is burden or
applicability. It is this. What you want them to do is not
give over information or do something that they do anyway for
their own business purposes or make available to you,
facilities that are their's, right?

Those three characteristics, capture all of the cases you have cited under the All Writs Act.

What you are asking them to do is do work for you. I am-- so there are two questions. One is, analytically where does that fall? Does it fall into the category, applicability that the All Writs Act either does or doesn't allow that? Or does it fall into category of, is it an unreasonable burden for purposes of New York Tel. Do you see the difference I'm trying to get at?

MS. KOMATIREDDY: I do see the difference. I think analytically it falls under the burden. The All Writs Act does not specify the nature of the assistance. The case law simply says from New York Telephone and onwards, a third party can be required to assist. There is all sorts of situations,

even the cases that New York Telephone cites of third parties, really run the gambit of various cases we have cited about corporations giving corporate records, credit cards, video tapes. But also cases of individuals being asked to answer questions, New York--

THE COURT: Give over information.

MS. KOMATIREDDY: Give over information, there is actually one of the cases that New York Telephone cites, involves an order requiring parents, this is <u>Board of Education versus York</u>, 429 F2D 66 in the 10th Circuit, 1970. Order requiring parents to send their son to a particular school, to further a desegregation. That is not necessarily information that is not use of a facility.

But, so I do think that the All Writs Act doesn't specify or limit the nature of the assistance, it simply provides for assistance. The nature of assistance is appropriate consideration under the burden analysis.

THE COURT: Look, clearly if it is not part of applicability, it is part of burden.

New York Tel also, somewhat confusingly, cites the Battington case, which to me is the clearest example, you know conscripting work. The cop gets on the running board of the cab, says follow that car.

And that is to me is the clearest example in New York Tel of the Court saying, you know, here is a way you can

28 - Proceedings -1 use the All Writs Act. What they don't talk about there, 2 surprising to me is Battington, there was actually a statute 3 that said it is unlawful for a private citizen to disobey that 4 kind of command. Exactly sort of the opposite of the application of the All Writs Act which is saying as long as it 5 is consistent with use-- so, that is what got me wondering 6 7 frankly if the idea of conscripted service, as opposed to the 8 other kinds of assistance that have been afforded under the 9 All Writs Act is sort of a categorical limit on the 10 applicability. 11 So you are saying -- anything -- I'm sorry, anything --10th Circuit. 12 13 MS. KOMATIREDDY: Board of Education versus York. THE COURT: Anything besides York that I should look 14 15 at? 16 MS. KOMATIREDDY: I will go back and we can provide further briefing, we will. 17 18 THE COURT: Okay. 19 MS. KOMATIREDDY: May I also supplement my answer? 20 THE COURT: Please. 21 MS. KOMATIREDDY: Which is, the Court characterized, 22 this as not a situation where Apple is giving over 23 information. The actual process of extracting this data is 24 just that, extracting data. Apple doesn't--25 THE COURT: Talking about information that they

- Proceedings -29 1 currently have. All of these cases are, you know, third 2 party, give me information that you have, or let me use your 3 facilities, right? Or usually combined with one of the other. 4 In any event, you do this anyway. MS. KOMATIREDDY: So this is a combination of giving 5 over information and letting the user facilities --6 7 THE COURT: Not information they have. 8 You want them to go into this phone that you have, 9 and do something that you can't do. You said you can't do. Or here his can't do it. 10 11 But, this is not information they have. You could 12 not execute any search warrant in Apple's servers right now 13 and get the information you wanted, right? 14 MS. KOMATIREDDY: That's correct, Your Honor. THE COURT: Let me ask you this related question, 15 could you subpoena or use some other form of court process, a 16 17 warrant, perhaps an All Writs Act order, to have Apple 18 disclose to you, how to get the information from the phone? 19 MS. KOMATIREDDY: I think the federal Government has 20 authority to issue a Grand Jury subpoena, if not a trial 21 subpoena to call a Apple witness and walk us through exactly 22 how they bypass the software. 23 THE COURT: There is existing procedure that allows 24 you to do what you want to do here.

MS. KOMATIREDDY: But I think that would be more

25

- Proceedings -30 burdensome to Apple, Your Honor, involving --1 2 THE COURT: Yes, but under Pennsylvania versus 3 <u>Marshals</u>, you can't use the All Writs Act to do something for 4 which there is a procedure available under more specific law, right? 5 6 MS. KOMATIREDDY: Under Pennsylvania versus 7 Marshals, you can't use the All Writs Act to do something that 8 a statute curtails you from doing. 9 THE COURT: There is a statute that establishes Rule 10 You are saying that under Rule 41, you can call them into 41. the Grand Jury, and have them walk you through how to do this? 11 12 Why doesn't that end the analysis? 13 MS. KOMATIREDDY: Well, Your Honor, you can call them into the Grand Jury. There are a couple of things to 14 15 consider. First of all, it is not clear having-- called them 16 into the Grand Jury, we don't believe that we have the 17 technical, actual technical capability by which I mean, the 18 device that Apple uses to bypass the pass code. 19 So, there is still a question about whether it is 20 feasible for the Government to do so. 21 Second, calling them into the Grand Jury could cause 22 a higher burden to Apple in terms of their trade secret 23 concerns. 24 THE COURT: That is their call, right? 25 Look, this is such a complicated area, we need to

- Proceedings -31 1 keep the analytic lines clean, right? You are wrapping into 2 burden, there is something that could be worse for them. 3 talking about applicability. Under <u>Pennsylvania versus</u> 4 Marshals, if there is another statutory path available to you, you have to take it, don't you? 5 6 MS. KOMATIREDDY: If there is a statutory path that 7 doesn't permit what is being asked for. That is not-- what is 8 happening here. 9 THE COURT: That is because what you are asking for 10 is being defined so specifically, right? What you are asking 11 for is for Apple to do it for you. 12 MS. KOMATIREDDY: We are asking--13 THE COURT: If what you are asking for is let us get 14 at the information in the phone for which we have a warrant. It sounds like you are saying you do have a way to do that 15 without application of the All Writs Act. 16 17 MS. KOMATIREDDY: So, under that theory, Your Honor, 18 you can subpoena, you can use any prior All Writs Act 19 precedent. 20 Take for example, issuing an All Writs Act order to 21 get the credit card records from the credit card company. 22 Under that theory, you can subpoena the credit card witness to 23 testify about the credit card records as opposed to actually, 24 as opposed to actually produce the records. Or you can

subpoena the credit card custodian to come into the Grand Jury

25

and explain how they accessed those credit card records in the internal system. But that testimony alone we believe will not be sufficient to then go use the system or give the federal Government to use the system to get into the record.

THE COURT: You need the records.

MS. KOMATIREDDY: Yes.

THE COURT: You might need to authenticate those records for, you know, for use in litigation. The testimony about them is not going to be admissible.

But here, what you need is the know how to get to this phone.

MS. KOMATIREDDY: And the technology, Your Honor.

Apple uses this technology in its facilities. It is specific, it can't do this at any Apple store. You have to go to Cupertino headquarters in their facilities, which I suspect can involve a Faraday room, because of remote wire requests.

THE COURT: Let's get rid of the remote wipe request. They said, that they essentially block that request that is pending. Are you saying they are wrong?

MR. ZWILLINGER: Your Honor, if I can clarify that briefly. The brief wasn't intended to suggest that Apple did anything to cause the remote wipe request to not work. It is just a matter of fact that the remote wipe request will not work given the state the device is in. The Court is correct it will not work, but it is not because of action that Apple

33 - Proceedings -1 took. 2 THE COURT: If it is not in a bag or room, and 3 connects to the internet. 4 MR. ZWILLINGER: It will not work. THE COURT: Do you have any reason to doubt that 5 6 representation? 7 MS. KOMATIREDDY: If that is the representation 8 Apple is making, no. 9 THE COURT: So you were saying though why it would 10 not work because they have technology you don't. MS. KOMATIREDDY: That's right. We don't believe 11 12 testimony alone allows us to get into the device. 13 THE COURT: Okay. 14 You know, this goes back to the thing I will ask you to get back to me on. But, Bower, the his agent who 15 16 testifies. Says they have the device that will do this. MS. KOMATIREDDY: Yes, I notice-- we will follow up 17 18 with the assistant who has that case. I can tell you from my 19 own personal knowledge, that the particular IOS involved in 20 that case, 8.1.2, there are certain -- this is all very 21 operating system specific. There are-- I have been informed 22 that there are certain technologies that allow the Government 23 independent of Apple, to get into that particular IOS. 24 But based on our investigation, and what the FBI and 25 DEA has told us about the IOS 7 system on the target phone, we

34 - Proceedings -1 are not able to do that. 2 THE COURT: Is your representation about what the 3 Government can do based on what the FBI and DEA can do, or are 4 you making this representation on behalf of every, I am using the broadest language deliberately. You make this 5 representation on behalf of every deponent of the Government? 6 7 MS. KOMATIREDDY: No, Your Honor, I would not dare. 8 THE COURT: That is an issue. 9 Look, I don't expect you to easily navigate, the 10 possibility that on the Intel side, the Government has this capability. I would be surprised if you would say it in open 11 12 court one way or the other. 13 But, you have to make a representation for purposes of the All Writs Act. You have them. 14 15 MS. KOMATIREDDY: That's correct. THE COURT: The Government cannot do this. 16 17 MS. KOMATIREDDY: When we--18 THE COURT: To make that representation, you need to 19 be right about it. 20 MS. KOMATIREDDY: We are making that representation 21 as the prosecution team. 22 THE COURT: You are not the prosecution team. 23 You want to conscript a third party. Before I do 24 that, don't we have to know that you don't have actually have 25 the capability, and by "you", I mean the United States

- Proceedings -35 Government? 1 2 MS. KOMATIREDDY: I think you have to know the 3 prosecutors in this case and the prosecuting agencies, the FBI 4 and DEA do not have a reasonable available tool. THE COURT: If Southern District U.S. Attorneys' 5 office has the technology and know how, you can still make the 6 7 representation, you have just made. That really allows me to issue an order under the All Writs Act? 8 9 MS. KOMATIREDDY: That is a interesting 10 hypothetical. I think it is unrealistic, the agency is the 11 same. 12 THE COURT: In terms of which office, not 13 unrealistic. 14 But, that is a joke. MS. KOMATIREDDY: 15 I got it. THE COURT: Look, we can slice it finely or not. 16 17 But, as opposed to your Brady obligation, Second Circuit law 18 clearly saying you are not responsible for everything in every 19 Government office. This is different. You are seeking 20 affirmative relief on representation that the Government can't 21 do this. 22 Why don't you have to make that representation for the entire Government? 23 MS. KOMATIREDDY: Well, because-- at the end of the 24 25 day, the question for us is, what is the burden on Apple, and

is this assistance necessary to effectuate the warrant.

THE COURT: The necessity prong.

MS. KOMATIREDDY: It is the necessity prong, Your Honor, but federal prosecutors don't have an obligation to consult the intelligence community in order to investigate crime. And in fact, in doing so --

THE COURT: You can ignore it. But, when you come to the Court and say it is necessary, because we can't do it, why does that excuse you from saying, well, wait a minute, we can do it, as a Government, but we have organized ourselves for reasons that may make a lot of sense in a way that we choose not to.

MS. KOMATIREDDY: Because fundamentally the All Writs Act is a practical gap filing statute. This is not an academic debate about what is possible.

THE COURT: You are trying to have it both ways on the All Writs Act. On the one hand, you a few minutes ago, you were saying, you look at it narrowly. If Congress is silent, even in the face of lots of evidence, that they really thought about this, decided not to do what is at issue here.

You know, it is fair game, the All Writs Act. Now you are saying, look at it practically. I think you have to choose one or the other.

It gets to an interpretive question that I had which is, the reading of it that says if it is not explicitly

- Proceedings -

prohibited by Congress, it is fair game, is one that, I don't have the statute in front of me. Is one that would be achieved by saying, agreeable to the law. But we had these other two words, agreeable to principles and usage of law which seems to go beyond just what is in the statutory text.

And, you know I wonder if you have a definition of those terms that your, your view of the statute doesn't read out of the text.

MS. KOMATIREDDY: So in terms of whether you're looking at the All Writs Act in a practical way or impractical way, our approach is consistent. It is a practical approach.

The reason we don't accept congressional inaction as having legal force, is because that is a practical approach to Congress. Congress has all kinds of reasons it doesn't pass statutes including allowing the status quo to continue when they can't agree on a different way.

THE COURT: Right. But I guess my question is, this is where we get to technical issue principles and usages.

We have for example in CALEA, that broadly regulates an industry with respect to electronic surveillance, and then carves out in some respects, the encryption and puts, you know, clearly defined boundaries on when third parties can be conscripted into the task.

There is a sense of what is the spirit, what is the principles and usages.

RB OCR

And to my mind that, that is a coherent understanding of the statute. That where you can infer what Congress was intending, from what they have done and what they have not done, you can fill in the gaps to the extent it is consistent with that overall understanding of legislation.

I'm trying to understand how you get to, as long as Congress hasn't explicitly prohibited it, a Court can do it, and make that coherent under the text of the statute.

I phrased it badly.

Make that consistent with a statute that includes not just agreeable to the law but agreeable to principles and usages of law.

MS. KOMATIREDDY: I understand the Court's concern. I think when looking at CALEA that way, I think there is something to be said, if you have a comprehensive legislative scheme. The key there is actually a legislative scheme, one passed into law like CALEA that addresses the issue. If there is in fact comprehensive and addresses ten possible iterations of a particular requested authority, and leaves one out, perhaps there is reasonable inference as a matter of statutory interpretation for an actual statute to say that there is an implied prohibition. We don't have that here. CALEA doesn't even come close to addressing the issue we have here. We don't have a comprehensive statutory scheme about Federal Court's requiring third parties to assist in the execution of

RB OCR

a valid search warrant.

For as long as that has been happening it has been governed by the All Writs Act. In this particular context with request to bypass of a pass code where a company is already capable of conducting that bypass. There is no specific expressed or implied Congressional action on that issue, which is why the law is left where it is.

THE COURT: I do have a couple of more questions. I don't want you to lose things that you want to say.

MS. KOMATIREDDY: No, that is all right Your Honor.

THE COURT: Your last answer reminded me of this.

In terms of, we have a scheme where courts effectuate warrants by calling on third parties. I asked you before about give me an example, if you have one, requiring a service from a third party.

Your argument on this, this goes to the first element of the New York Telephone which we have not discussed yet, how closely related.

You have inserted into this, I don't mean that pejoratively at all. You sort of cast the argument in terms of something New York Tel doesn't talk about. At least not explicitly. Apple is in a position to thwart your investigation.

I want to make sure I understand. First of all, are they in a position to do anything going forward to thwart the

- Proceedings -

investigation or is it simply that before you got the warrant they had done something, created this operating system, that gave somebody else the possibility to thwart an investigation, by turning on encryption.

MS. KOMATIREDDY: We are not making an allegation that Apple would affirmatively do something.

THE COURT: There is nothing that they can do to stand in the way of your investigation other than not take action.

MS. KOMATIREDDY: I can't represent what they are capable of doing in terms of, that is not within my kin. I can say-- the issue, the reason we believe there is cross connection and the way New York Tel frames it, is where a company's services or facilities are being used as part of an ongoing criminal enterprise.

And, in fact, this is more fully discussed in one of the other case, <u>United States versus Hall</u>, which is the credit card records case. It talks at length about the close connection because in that case, it actually says, you know, the case involves federal law enforcement trying to get the credit card records, not of the defendant, but another person, companion.

THE COURT: Come on, in Hall the bank was extending credit to a fugitive, while that person was a fugitive. It was making it possible on a go forward basis, for the fugitive

41 - Proceedings -1 to escape the law. What is Apple doing here that is 2 comparable to that? They are taking some action going forward 3 prospectively that is helping the defendant in your case. 4 MS. KOMATIREDDY: So it was not actually extending credit to the fugitive. It was extending credit to a 5 companion that would have location information. 6 7 THE COURT: While you were trying to catch this 8 person, the bank is taking actions prospectively. What is 9 Apple doing here that is comparable? MS. KOMATIREDDY: The common thread is that it is 10 11 the company's services that are being used by the criminal. 12 THE COURT: What services of Apple, what service is 13 Apple now providing to the defendant in this case? 14 MS. KOMATIREDDY: There are three services. the actual pass code lock feature. The operating system which 15 Apple currently owes and currently licences to the owner of 16 17 that cellphone. 18 THE COURT: Can they do anything without taking back 19 something they have sold to the defendant or to somebody who 20 gave it to him, short of taking back something they have 21 already sold, can they do anything to defeat the encryption 22 here? 23 MS. KOMATIREDDY: I'm sorry, short of taking? They 24 can assist us by bypassing the lock. 25 THE COURT: Yes, for them to do that they have to

take it back, you have to give it to them.

MS. KOMATIREDDY: You are saying, take back the phone. They already own the software.

THE COURT: What can they do to the software? I have to say, of all the very good arguments in your brief, the thing about the end user license agreement struck me as a total red herring. I don't get at all, why what the license agreement does in terms of regulating what any of the parties here can do or can't do, that is of any relevance to the dispute here.

MS. KOMATIREDDY: The relevant point is that Apple owns and currently operates the software that is preventing the federal warrant from being executed. Because the pass code lock is enabled and still active. Because the pass code feature that deletes the contents of the phone after ten failed attempts, is possibly enabled and could thwart execution of the search warrant. I understand that Apple has represented that the remote wipe is no longer available. So, we can take that out of-- assuming that is true, we can take that out of the analysis.

The argument stands that it is Apple's software that is currently operating, that stands between a Federal Court's warrant being executed, and evidence of crime being --

THE COURT: Let me ask you, I think we have all been searching for analogies one way or another here. I have seen

- Proceedings -

some suggestions about the safe and you know conscripting the locksmith. It seems fanciful.

But here is one that I think is not fanciful. The last company that makes lethal injection drugs, decides to stop doing it. In fact Justice Alito referred to this in recent cases, gorilla warfare by these companies. Right.

So the last company that has been providing drugs for execution, says to the Government, we are no longer going to help you out when it is time to execute somebody in Terre Haute.

Can -- are they thwarting a lawful death sentence by doing that, and can they therefore be compelled under the All Writs Act to re-import something that is held abroad or release something from existing stock or actually manufacture the drug anew?

MS. KOMATIREDDY: So, with each of these, it is a case by case analysis. I think we have to return to the factors under New York Telephone and the factors in the All Writs Act. I think you have to look at what the relevant applicable law is and I have to concede in this area I'm not familiar with the expansive 8th Amendment Law on this.

THE COURT: In terms it is fact specific under the burden, is that relationship close enough for purposes of the first element of New York Tel, to say look, this company, you know they have got the monopoly on this point on doing it, on

making these drugs. Now they are out of business. They are thwarting us from carrying out a lawful death sentence.

Does that get you passed the first step?

MS. KOMATIREDDY: Your Honor, I have to be honest with you here, it is hard to say. Here is the reason I hesitate with this analysis. The analogy is different because there, we are not talking about an order that is a warrant that can-- that can be simply executed but for one step in between. We are talking about a potential death sentence issued by a jury.

THE COURT: Sorry. Look, that is not right. It is an order of the Court. The sentence is, a Court order just as the warrant is a Court order.

MS. KOMATIREDDY: And the question is, whether the company that makes the injection.

THE COURT: They are the last company around and there are fewer of them. We get to the point where there is one. They say, you know what, they are not going to do it, deliberately to try to frustrate public policy, right. We don't want there to be executions, so we are going to withdraw the drug from availability. The All Writs Act, can tell them to do otherwise.

MS. KOMATIREDDY: That would depend on the law of whether you can require a company. That could depend on several things. The relevant Food and Drug law, whether you

can require a company to develop a drug in that manner.

THE COURT: There is silence on this. We are in the exact same position as we are here. You have silence.

You are doing a really wonderful job of representing the Government here, but you understand the question I'm trying to ask.

MS. KOMATIREDDY: I do understand the question. It is a tough question.

The thing that is particularly tough about that question is, it is hard to say, so there are two questions, you have asked. One, does the All Writs Act permit that order. That requires considering all three of the factors. I have.

THE COURT: But that is not the question I asked.

The question I asked is, does the intent to thwart the execution of that death sentence, bring the company closely enough to thwarting of a lawful court order that you satisfied the first element of New York Tel. Not does it satisfy all three elements, just the first.

MS. KOMATIREDDY: So, I don't think it is intended to thwart, but establishes the connection. Based on the case law I reviewed from New York Tel and <u>United States versus</u>

Hall. It is when the company's facilities are being used in some way. I mean this context, in some way, for an illegal purpose. So in that context it would be the company so called

46 - Proceedings -1 facilities, drug making features are being used or not being 2 used. 3 Right. THE COURT: 4 MS. KOMATIREDDY: So, the difficult part of that question is, understanding who is sufficiently closely 5 6 connected. It may be that company, it may be someone else is 7 more closely connected. 8 So I --9 THE COURT: Like who? 10 MS. KOMATIREDDY: It may be that you can-- the Federal Government can develop those things on its own. 11 12 THE COURT: You mean like here, the Government might 13 be able to find the technology and know how on its own, 14 perhaps by asking his. 15 MS. KOMATIREDDY: So. THE COURT: 16 Right? MS. KOMATIREDDY: I think I have addressed the his 17 18 point. 19 THE COURT: I know. Theoretically the Government 20 can do this. 21 MS. KOMATIREDDY: No, Your Honor. 22 THE COURT: Theoretically, in the hypothetical, the 23 Government can do it on its own. The same here. 24 MS. KOMATIREDDY: Based on our investigation, we 25 can't bypass the pass code on this particular phone.

THE COURT: Right. I am positing a scenario, where there is nobody else who is making this drug. So I'm trying to make it as close as possible. I just-- instead of fighting the hypo, I really appreciate addressing the question I'm trying to ask, which is, does it satisfy the first test, that first prong of the New York Tel test in the -- that drug scenario, context.

(Pause.)

MS. KOMATIREDDY: I apologize for taking a moment.

THE COURT: These are hard questions. No problem.

If you want to consider it and get back to me, I completely understand and that is fine.

MS. KOMATIREDDY: Your Honor, the hypothetical is so inflammatory, I would like to consider it and get back to you.

THE COURT: It is purposefully so. Because to some extent, what you are talking about, and this gets to very much the burden in New York Tel. You are saying, it is not much of a burden. And part of how you get there is, well, the American people would not think that, you know, a company would not want to help law enforcement.

But, at some point, not just a matter of marketing and dollars and cents. At some point, a private actor, I'm not saying necessarily Apple has. Somebody can say we don't want to do this. As a matter of conscience, this is something we don't think should be done.

RB OCR

I'm trying to draw parallels intentionally to the company that says, we don't think our drugs should be used to kill people.

Can the All Writs Act compel service over a conscientious objection which is very different from saying, can it compel information or the use of a facility. There is something just categorically different about compelling service.

So, yes, it is intentionally a tough and inflammatory hypothetical because I want to get a sense of how far you are -- understanding of the All Writs Act goes.

MS. KOMATIREDDY: I'm happy to consider that further and get back to you on that Your Honor.

But I would note that in this case, there is no conscientious objection. Apple has been doing this for years without any objection.

THE COURT: Right.

MS. KOMATIREDDY: And they are more concerned about public perception, which is a fair concern, but that is not the law. And, the law shouldn't change that perception.

THE COURT: I don't know if it is or not. I really don't know.

I am almost not completely exhausted the questions I wanted to ask you, I very much appreciate how responsive you have been, especially, you have indulged sort of my jumping

all over the place.

The last one, this goes back belatedly to Congressional inaction.

There is a case from the Ninth Circuit, 1970, that is cited but not really taken on analytically in New York Tel, called application for United States for relief, Ninth Circuit, 1970.

And, in that case, the Ninth Circuit did what I was suggesting before, sort of like looking at the sort of overall state of the legislation, what has been done and what hasn't, and denied the refund of the All Writs Act there.

What was going on there, was a request for telecom assistance for a wire tap after the original statute was passed in 1968, but before Congress acted to-- partly in response to this case, to require telecom assistance.

New York Tel cites it, but I don't think they are really saying they were wrong. They weren't saying they were right either. But it does have a reading of the All Writs Act that seems to be disagreeing with you, about the meaning of Congressional silence or the lack of affirmative legislation.

Again, if you don't have a case clearly in mind that is fine, I will let you respond later.

Did the Ninth Circuit get it wrong there, or can you square it somehow with your understanding of the meaning of Congressional inaction here.

- Proceedings -

MS. KOMATIREDDY: I need to review the case to get back to you. The distinction that pops out from the outset is if it is a case about requiring assistance for Title III wire tap and there is a Title III wire tap statute which in itself is an extensive statute already in place. You have the presence of a complicated relatively exhaustive statutory scheme. So there is something to be said there for reading it, that the entirety of that statutory scheme and absence of specific authority which would otherwise be obvious, missing from that statutory scheme.

I am happy to review the case and follow up on that.

THE COURT: I may well have skipped some things, but I want to hear from Apple, give it a chance as well.

But, if you have not had a chance to get to some arguments, I want to hear them.

MS. KOMATIREDDY: Your Honor, we are happy to hear from Apple.

THE COURT: You have been very patient there Apple.

MR. ZWILLINGER: Thank you, Your Honor.

There were two points I wanted to emphasize and the Court touched on both of them. But I just would take a little time to underscore them.

We do believe that providing expert services on a device in the Government's custody, is different than providing access to records or facilities that are in our

possession and control.

In all of the cases that you mentioned, the Government cites, involve records or facilities that are in the third party's control. For example, there were logs from the phone company, there are credit card transactions from a credit card company, there were surveillance tapes in an apartment complex. They were not only in the possession and control of a third party, but they were in the normal course of their business.

Here we put a device in the stream of commerce. The Government is asking us to essentially do what they want and would like to have their own agents do, which is perform forensics services and unlock it. That type of conscription does not have a precedent in the All Writs Act cases that have been cited. So I wanted to focus on that.

The second is, the most important difference between this and what was set out in New York Telephone, is that there is no indication that Congress intended the Government to have this power here.

In New York Telephone, there was a greater included power. There was a greater power which was the power to wire tap the contents of communications. And the Government said that surely has to include the lesser included power of performing a pen register. And not performing the pen register would have frustrated the intent of Congress.

RB OCR

- Proceedings -52 1 In this situation it is the exact opposite. 2 enforcement is seeking an order that the Congress has never 3 authorized, and it is not a subset of the authority that 4 Congress has already granted. 5 We are talking about CALEA. We agree, that this is 6 outside the bounds of CALEA, but we draw completely different 7 conclusions from that. 8 CALEA only covers data in transmissions, but only 9 providers, only certain types of providers, providing certain 10 types of services, were given the obligation to build in a way 11 to assist law enforcement. 12 And, Ms. Komatireddy points out that Apple is 13 outside that scope. 14 (Transcript continues on next page.) 15 16 17 18 19 20 21 22 23 24

25

THE COURT: Are you inside the scope of the information service?

MR. ZWILLINGER: I need to get back to the Court on that. I don't think we've taken a position on that, but we're outside the scope of what's a required actor under CALEA.

THE COURT: Go ahead.

MR. ZWILLINGER: And <u>CALEA</u> is where Congress has been debating making amendments or amending the statue to encompass a wider variety of services and a wider variety of providers and that's the debate that Congress needs to have.

What's going on here is this is not a gap in the law that the All Writs Act would fill in. This is pushing the law to a new frontier and if the government wants these types of authorities to require providers to provide forensic services to the government, I think the place to go is Congress because we can't use the All Writs Act which, as we had some discussion, was passed in 1789 and amended in 1946, to circumvent this question. This is the question of the time which is what is the balance between privacy and government access today and Congress needs to speak on that and if we give the government the power they're asking under the All Writs Act, we circumvent that entire debate.

THE COURT: Can I ask, on the issue of burden, even if you're not sort of legally foreclosed in any way from making the arguments you are making, I am troubled by the fact

that there is a history here and it's not just, you know, saying here is what you need to do, government, if you want something from us. You are writing a request for them and it is hard for me to think of an analogous situation where somebody who does not want to do something says, but I'll tell you how to get it done.

MR. ZWILLINGER: Let me address that.

THE COURT: What explains why you are providing this kind of help? Is it not that, hey, you know, we want to foster law enforcement, we do, we just don't want to be seen out there as, you know, compromising the privacy of our users' devices?

MR. ZWILLINGER: Right. So let me address that in two ways.

First, the legal backdrop of this, by the way, is under New York Tel, the question was is the activity something that the provider does in their normal course of business and is it offensive in any way to the provider.

Apple doesn't do this and never did this voluntarily. Apple was always compelled by a court order to perform these services when it did it and all of that was done in an ex parte proceeding, the same type of proceeding that would result in the authorization of a search warrant.

THE COURT: I'm sorry. It's not just these are ex parte proceedings. You get one of these orders. If you

don't like it, you know you can go to a court and say, you know, relieve us from this obligation or, if you've had several of these things and you don't want to keep doing it, you can seek declaratory judgment, right, because there's clearly the ongoing controversy that will get you past the jurisdictional bar.

If you didn't want to do this, if it was really burdensome to you, do you disagree that you had steps available to you that you have just not taken?

MR. ZWILLINGER: Apple could have challenged the order that they received, there's no question it could have, but also the weight of the authority was that Apple was regularly receiving these orders from magistrates, receiving these orders from courts indicating that Apple was being compelled to do this and no court and no state court or federal court had invited Apple to submit its views.

THE COURT: But, clearly, you don't need to be invited to court when you think your interests are at stake and you have been getting these orders but from the very few that I have seen with the exception of the one in the Southern District which I don't think was to Apple, whatever XXX Inc. was, it appears not to be Apple, but there has been one that's been publicly available out of Oakland.

From all I can see in these cases, there are boilerplate applications and boilerplate orders and nothing

about them, again, from the limited slice of it I've seen, that would have suggested to you, I think, well, it's futile for us to go to court and try to win the case because they've decided the issue.

MR. ZWILLINGER: Well, I would think the fact that we were repeatedly getting these orders and being contacted by law enforcement did play into the fact that it seemed that this had been somewhat settled views and settled authority from multiple judges.

THE COURT: But, look, you know how it works, especially at the magistrate level. There are plenty of just very pro forma applications and orders that get signed and the fact that that happens doesn't necessarily indicate that the issue has been given the kind of thought that would be required if you were to challenge it and seek to vindicate your perceived rights.

So, I am just trying to understand why I shouldn't read something into the fact that you have never tried to challenge these orders.

MR. ZWILLINGER: Let me make one comment about the language though because I think it's important.

One of the reasons for the language that we offered to law enforcement is because we were getting so many orders and the orders were not consistent as to what Apple was and wasn't required to do, and because there were questions

related to, you know, does Apple have to decrypt the device, does Apple have to do X or Y, certain language was come up with so that if Apple saw that in an order, it would be clear, one, that it was being compelled to perform these services, and it wasn't, you know, any voluntary action on its part, two, exactly what services it was being required to do and

So, the point of the standardized language was, in fact, because we were getting these with such frequency, that we wanted to accomplish that and make it clear that we were being compelled.

THE COURT: Okay.

what it wasn't required to do.

MR. ZWILLINGER: So I don't think giving the language is a concession to the fact that the All Writs Act provides authority to issues those types of orders.

THE COURT: Look, your language doesn't invoke the All Writs Act, I get that, but in terms of the burden, first, you haven't challenged it and you still haven't explained why not. Second, you provided language for reasons I understand about consistency, but you also did not say anything about burdens beyond the immediate expense.

If you are saying we want to craft language that is going to say here's exactly what we have to do, you require, if I'm not mistaken -- I don't have the language in front of me. Do you require compensation?

MR. ZWILLINGER: No, we've never required compensation.

THE COURT: But you can, and you don't do anything about that.

I mean, the point is well taken that Apple is a pretty darn big company, maybe they don't care so much about the costs of these 70 things in the big picture. It just seems to me that there's a dog that didn't bark here.

MR. ZWILLINGER: I think the way to address this, Your Honor, is the following.

Right now, Apple is aware that customer data is under siege from a variety of different directions. Never has the privacy and security of customer data been as important as it is now. And, in fact, Apple built an operating system which is why we're only talking here about IOS 7 systems, operating systems IOS 8 and IOS 9, that puts Apple in a position where it cannot do this, that is, going forward with 390 percent of the devices involved, Apple cannot perform these services. So, Apple has taken itself out of the middle of being in a position where it can be used as an attack vector or in any way to compromise the security and privacy of customer devices.

So, when the court asks Apple today does the All Writs Act provide authority to force it to do this, Apple says no, it does not, because what we are being forced to do is

expert forensic services, we're being forced to become an agent of law enforcement and we cannot be forced to do that with our old devices or with our new devices.

THE COURT: One of the arguments you make about burden is that complying with the order implicates the trust relationship that you have with your customers. I'm not sure I understand why.

I mean, as you have taken pains to make clear in the language you propose, you only break into one of these phones if you're compelled by law. Well, we all have an obligation to follow the law. So how does that imperil the trust consumers have?

MR. ZWILLINGER: Well, it's a somewhat ironic question in light of the prior question which is why hasn't Apple been challenging these in the past. That is, if Apple in a position where it is no longer going to be able to turn these devices and bypass them and give data to law enforcement and now Apple is being invited by this court to comment on its views, I think Apple's views are we are not in the business of accessing our customers' data, we have never been in the business of accessing our customers' data and we shouldn't be in that business either on our own or being conscripted by law enforcement.

THE COURT: Okay. Explain to me sort of the path from you're ordered to do something unwillingly to because you

did so, consumers lose confidence in you.

MR. ZWILLINGER: I think it's the same question you asked me a minute ago, why didn't Apple challenge the prior orders.

THE COURT: No, it's not. It's really a different question. That's why I'm asking it again.

In other words, tell me the thought process in some hypothetical consumer's head.

MR. ZWILLINGER: Well, I think a hypothetical consumer could think if Apple is not in the business of accessing my data and if Apple has built a system to prevent itself from accessing data, why is it continuing to comply with orders that don't have a clear lawful basis in doing so.

THE COURT: Well, clear lawful basis, but when a court says you must do it, and I have considered your arguments about a lawful basis, and still saying, sorry, you have an obligation or you're paying a fine or somebody is going to jail, how does that imperil trust?

MR. ZWILLINGER: So I think the answer is if it becomes crystal clear, if you say and whatever other court this goes to after you say that the All Writs Act provides clear authority to do this and that we have found that there's sufficient basis in law to conscript you into government service, then it wouldn't undermine customer trust, but at this point, it does because right now, it's not clear.

THE COURT: But, see, that's why I'm having trouble and it does go back to the earlier question.

The thing that does seem to imperil consumer trust is not that you comply with a court order, but that you don't take all the steps available to you to fight that order before complying.

Here, you're doing that at invitation and I don't know what plans, if any, and you don't have to tell me what lies ahead if I grant the government's motion, but you have had apparently 70 prior instances where you have not taken the steps available to you. That I can see imperils the trust, but complying with an order after you fight it, how is that going to do it? And if you want, address why doesn't it imperil trust to the point that it's hard for me to put much weight on your burden argument if in the past you haven't taken these steps.

MR. ZWILLINGER: Well, I think of two things.

One is having been in this area of law a while, we have seen the law evolve. Right? There was a time when cell site data was available with a mere subpoena by the government. There was a time when contents of communications was available with a subpoena or court order by the government and now it's accepted as somewhat orthodoxy that a warrant is required for contents of communications.

So, the law evolves and by understanding that the

All Writs Act doesn't provide the clear cut authority that 1 2 Apple once may have thought it did, I think Apple has to 3 continue to say that if Apple is forced to do what it does not 4 want to do -- right? The court posited the question before, is Apple saying it does not want to do this. Apple is saying 5 it does not want to do this. It does not want to be in the 6 7 business of being a mechanism by which customer data is 8 disclosed. Although it will comply with lawful orders when 9 required to do so, it doesn't think that that's the position 10 that Apple should be in and Apple has communicated to its 11 consumers that it doesn't want to be in that position. 12 THE COURT: I was discussing with Ms. Komatireddy 13 alternate means that might be available. 14 MR. ZWILLINGER: Yes. THE COURT: What's your take on, from both a 15 technical level and the legal one, the alternative of subpoena 16 or other process ordering Apple to tell the government how to 17 18 break into the phone? 19 MR. ZWILLINGER: So, before I address that, can I 20 clarify something on the record --21 THE COURT: Yes. 22 MR. ZWILLINGER: -- with regard to the question you 23 asked about the Djibo case? 24 THE COURT: Yes. 25 MR. ZWILLINGER: It was my understanding that

Ms. Komatireddy said that this concerns an IOS 8 system.

1

3

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

2 Apple is not aware of any mechanism to break into an IOS 8 or

IOS 9. Not aware of it at all. I think this was speculation

4 | in the testimony, but the testimony did say that the declarant

here or the person testifying, the forensic expert, said that

he personally broke an IOS, an iPhone 4S running 7.0.

THE COURT: But he was also saying that he understands that it has been used successfully for 8.1.2 which is the phone --

MR. ZWILLINGER: We're not aware of that. We're not aware of that indication. We have heard that there were third parties advertising the ability, forensic service providers the ability to access a 7.0 phone. We have no independent verification of that, but we had heard that as well. So there may be other means for this case for this phone although we don't think those exist in the future.

As to your question, however, we do agree with the government that we do not think there's an easy mechanism by which Apple can disclose to the government the method of access.

THE COURT: Technically or legally?

MR. ZWILLINGER: Well, we don't think, legally, we can be forced but, technically, we don't think it would work. The way the system is configured, it requires certain authentication from our servers and on that point, I think

Ms. Komatireddy was correct that we couldn't provide the instruction manual that would just work.

THE COURT: Just to close the loop, why, legally?
What would be the bar to the subpoena or even an All Writs Act order because information is clearly something that an All Writs Act order covers obviously?

MR. ZWILLINGER: I think it would be forcing the company to disclose some of the most confidential trade secrets it has and I think Apple would find that the legal justification in this case wouldn't be there for that type of order, we would argue.

THE COURT: Burden or just not --

MR. ZWILLINGER: Even more. I mean, we're talking about at this point, you know, the most confidential trade secret issue, but we don't think we have to get there. We agree with the government that the system requires Apple authentication.

THE COURT: Okay. There was another burden question

I wanted to ask you and it slipped my mind unfortunately.

MR. ZWILLINGER: If I could, Your Honor.

THE COURT: Yes. Go ahead, please.

MR. ZWILLINGER: I do think Ms. Komatireddy's argument or review of what Congress has been discussing is far too narrow. She said the debate was just about providing law enforcement access to certain types of communications. I

don't think that's what the debate has been about. The debate has been an entire societal debate about the role of providers and being required to assist law enforcement and I think the debate covers this topic and a variety of other topics.

So, this doctrine that Congressional inaction can't be used as a basis for making this decision I think doesn't apply in All Writs Act. The whole point of All Writs Act is to figure out what Congress has passed and hasn't passed and are you filling in a scheme that has some interstitial problems or are you giving authority that Congress never intended. So I think you have to look at what Congress has done and hasn't done. CALEA is a comprehensive scheme by which certain types of providers are required to provide assistance for law enforcement. That's the title of the statute.

So, I don't think her view is correct. I think, one, you have to consider what Congress has chosen not to do and, two, you have to lock at <u>CALEA</u> and say what was the bargain struck with <u>CALEA</u>, who was required to perform services and who was not, and then decide whether this is an issue that the court can fill in.

THE COURT: This does remind me of the question I had before and it was somewhat related.

Look, is it really burdensome for you in a bigger picture sense to do what the government wants here? And there

are two things I have in mind.

One is, in sort of a narrower sense, your brief almost makes the argument. It's an advertisement for buying our new phones, right, because we won't be able to do this. If you just get our newer phone, we can't do this for the government. So, yes, sell more phones.

The second one, and not quite as facetiously, there is a broader societal debate and it seems that it's reached a point somewhat to your liking quite recently which is as things currently stand, the administration isn't seeking back-door legislation.

Are you worried at all that a decision here and in other courts like it saying you can't rely on the All Writs Act which the government may have been assuming it could would reopen the question for the government and for Congress to have back-door legislation.

In other words, are you better off having the transitory orders under the All Writs Act?

MR. ZWILLINGER: I think on the second point first, Apple is better off for having a robust public debate that if new authority is going to be granted and we do this, leading down the road to all sorts of new authorities, it should be done by Congress. So whether advantageous -- the result is advantageous or not, the process is right to go to Congress and have a public debate and not to do it this way.

THE COURT: Okay.

MR. ZWILLINGER: Going back to your first point about the advertisement for the new phones, one of the problems with the type of authority that the government is seeking is that it's hard to draw the line where it stops. Would it stop at unlocking? Why wouldn't the government say all the same things about modifying software? Why wouldn't they claim we have a Title III order and the only way to get it to be implemented is if we ask you to you make changes to the product?

THE COURT: There was a case like that, wasn't there? I'm blanking on it. It was essentially trying to set down an update to the phone that would allow the government to do something that it had gotten authority for. Does that ring any bells?

MR. ZWILLINGER: We're not aware.

THE COURT: I'm sorry. I hope I'm not making it up. Go ahead.

MR. ZWILLINGER: The point is that the line drawing question, that is, the authority they're seeking, if Apple stays sufficiently involved with a product that's admittedly locked and in a draw, the argument under New York Tel prong one that we're sufficiently involved in this product, we're doing nothing with this device right now. It's sitting in a drawer locked. We're providing no services to it. If the

characterize what's going on here is that we are asking for technical assistance. We're also asking for information as

24

25

counsel just represented, the actual bypass and process information required from Apple's servers that it has.

If you look at <u>New York Telephone</u> and one of the other cases that we've cited from the District of Puerto Rico, <u>In Re Application</u>, which orders the phone company to assist in essential monitoring, in those cases, the court issues All Writs Act orders both for information and for technical assistance in order to effectuate that particular obtaining of information. So, labor is conceived as part of the types of assistance that a court can require.

MR. ZWILLINGER: Your Honor, I'm very glad she brought up that District of Puerto Rico case because I think she's reading it exactly wrong. The court denied authority under the All Writs Act in that case. The court ruled that the All Writs Act did not provide a basis for authority and said Rule 41 provided the authority.

THE COURT: I'm reminded of Judge Nickerson who argued before the Supreme Court. One Justice thought a case said one thing and another one thought it said something. The lawyers argued very different readings of the same case and a Justice said, well, how are we supposed to resolve this? And Judge Nickerson said, I'm afraid Your Honor will just have to read the case. I have to do that.

MR. ZWILLINGER: I would proffer that but the language is fairly clear. The government has -- issuance of

the requested order directly under the All Writs Act would not be necessary or appropriate in aid of this court's jurisdiction where no jurisdiction exists thus, there must be a separate jurisdictional basis for me to grant this application.

MS. KOMATIREDDY: You're right, and the separate jurisdictional basis is Rule 41.

I mean, the thing is with these All Writs Act orders, historically what's happened is the government has asked for two things. One, it's asked for the court to provide, to allow it to obtain a certain amount of information and provide, through the All Writs Act, access and authority to get that information and then, second, for the court to instruct a third party to assist in obtaining that information.

Here, we don't have to do that. This case is actually more narrow because the government has separate legal authority, a search warrant, to obtain the data. All we're asking for is technical assistance.

THE COURT: I get it. One last thing.

The <u>Pennsylvania versus Marshals</u> case, the court ended up saying there that the court could not require the Marshal Service to transport a prisoner who was required to be in federal court. Right?

MS. KOMATIREDDY: Right, but, Your Honor, in that

case, there was actually a habeas statute that was directly on point and the habeas statute had a provision that said that state court personnel were required to do the transfer. So in that instance, again, you have a statute that is not on point. Very different from here.

THE COURT: If not by statute, I know it's counterfactual, would it pass the burden test and all the other prongs of New York Tel?

MS. KOMATIREDDY: I think so. It depends a little bit on the burden. I think the question about close connection is easier there because if it's a transfer as it was in that case of a state prisoner to a federal facility, at least the United States Marshals have some relation to the federal, to that part of the system.

THE COURT: But they're not standing in the way of the transport. They're just not doing it.

MS. KOMATIREDDY: Yes.

THE COURT: In other words, in that way, it seems to be very analogous to this case.

MS. KOMATIREDDY: That's true, Your Honor, and I think this is why it's important to look at all of the factual situations of that particular circumstance because in all likelihood, if I were to suppose what would happen in that situation, the court gives an order to transfer a particular prisoner, the government probably would just send an agent as

opposed to request the assistance of marshals.

THE COURT: Right. You said there was a second case.

MS. KOMATIREDDY: Yes, Your Honor. We followed up with the Assistant who handled the case in <u>Djibo</u>, 15-CR-088, and I'll at least provide some additional information on how we believe we got into this pass code, but I want to represent to the court that I'll personally follow it up after our hearing is over.

My understanding is I'm advised the technology in that case worked by trying every possible pass code. In that case, they did not have a reason to believe that the feature that initiates a wipe after ten failed attempts was activated. Here --

THE COURT: The testimony, and I know you haven't had a chance to read it, but the testimony talks about that and defeating that, I won't pretend to have followed exactly the technical explanation, but to defeat that, rather than it wasn't turned on.

MS. KOMATIREDDY: All right. You know, in terms of better practice, let me consult with the AUSA and I'll get back to you.

THE COURT: Okay.

All right. Everybody, this has been very, very helpful and really wonderful advocacy by both sides. I am

```
73
    happy to set a schedule for you to get back to me on the
1
 2
    various items that have come up, just a letter from each side.
 3
              How long do you want? I would like simultaneous
 4
    letters rather than giving one side priority over the other.
5
              MS. KOMATIREDDY: We would request two days so
 6
    Wednesday.
7
              THE COURT:
                          Wednesday. Would that work for you
8
    guys?
9
              MR. ZWILLINGER: I think we can do Wednesday.
              THE COURT: Okay. Great.
10
11
              MR. ZWILLINGER: Thank you, Your Honor.
12
              THE COURT: All right. Then I will get a decision
13
    out as quickly as I can.
14
              Thank you all. Have a very good day.
15
              MS. KOMATIREDDY: Thank you, Judge.
16
               (Matter concluded.)
17
18
19
20
21
22
23
24
25
```

		1
4	718 [1] - 2:2	add [2] - 11:7, 68:15
1	7 10[1] 2.2	additional [1] - 72:6
	8	address [7] - 17:3, 21:17, 54:7, 54:13,
10th [2] - 27:10, 28:12	0	58:9, 61:13, 62:19
11201 [1] - 1:18		addressed [2] - 21:24, 46:17
11:30 [1] - 1:12	8 [4] - 20:25, 58:16, 63:1, 63:2	addresses [2] - 38:17, 38:18
15 [2] - 1:8, 2:10	8.1.2 [3] - 4:17, 33:20, 63:8	addressing [2] - 38:23, 47:4
15-CR-088 [1] - 72:5	8th [1] - 43:21	administration [1] - 66:10
1789 [3] - 19:10, 19:13, 53:17		admissible [1] - 32:9
1900 [1] - 1:23	9	admittedly [1] - 67:21
1902 [2] - 1:8, 2:10		advantageous [2] - 66:23, 66:24
1946 [1] - 53:17	9 [3] - 3:12, 58:16, 63:3	advertisement [2] - 66:3, 67:3
1949 [1] - 19:15	0 [0] 0.12, 00.10, 00.0	advertising [1] - 63:12
1968 [1] - 49:14	Α	advised [1] - 72:10
1970 [3] - 27:10, 49:4, 49:7	/ \	advocacy [1] - 72:25
	_	affect [1] - 14:6
2	a.m [1] - 1:12	affects [1] - 20:1
	ability [3] - 16:23, 63:12, 63:13	affirmatively [1] - 40:6
20036 [1] - 1:23	able [6] - 4:5, 17:2, 34:1, 46:13, 59:16,	afford [1] - 4:22
2008 [2] - 8:9, 8:21	66:4	Affordable [2] - 18:22, 18:23
2008 [2] - 8.9, 8.21	abroad [1] - 43:13	afforded [1] - 28:8
2015 [3] - 1:12, 3:12, 6:19	absence [1] - 50:8	afraid [1] - 69:22
225 [1] - 2:1	academic [1] - 36:15	agencies [3] - 6:25, 7:12, 35:3
26 [1] - 1:12	accept [1] - 37:12	agency [1] - 35:10
271 [1] - 1:18	accepted [1] - 61:23	agenda [2] - 18:13, 20:5
2 [.]	access [13] - 10:8, 10:9, 10:10, 13:6,	agent [3] - 33:15, 59:2, 71:25
3	16:10, 21:2, 50:25, 53:20, 63:13, 63:20,	agents [4] - 4:4, 5:10, 6:9, 51:12
<u> </u>	64:25, 70:12	ago [6] - 5:13, 6:3, 9:15, 23:9, 36:17,
	accessed [2] - 4:10, 32:1	60:3
30 [1] - 18:21	accessing [4] - 59:20, 59:21, 60:11, 60:12	agree [6] - 6:15, 9:24, 37:16, 52:5,
390 [1] - 58:18	accommodate [1] - 7:20	63:17, 64:16
3rd [1] - 3:13	accompanied [1] - 22:3	agreeable [4] - 37:3, 37:4, 38:11
	accomplish [1] - 57:10	agreement [3] - 17:15, 42:6, 42:8
4	account [1] - 15:4	ahead [5] - 20:20, 53:6, 61:9, 64:21,
	achieved [1] - 37:3	67:18
41 [4] - 30:10, 69:16, 70:7	acknowledge [2] - 11:20, 21:6	aid [1] - 70:2
429 [1] - 27:10	act [4] - 14:22, 16:19, 26:3	aided [1] - 2:4
434-to-1 [1] - 16:3	Act [62] - 15:5, 15:13, 15:22, 16:17,	airplane [1] - 6:9
435 [2] - 16:7, 16:14	17:20, 18:14, 18:22, 19:4, 19:8, 19:9,	AL [1] - 1:7 alerted [1] - 3:8
4S [1] - 63:6	19:10, 20:24, 26:13, 26:17, 26:22,	Alito [1] - 43:5
	27:14, 28:1, 28:5, 28:9, 29:17, 30:3,	allegation [1] - 40:5
5	30:7, 31:16, 31:18, 31:20, 34:14, 35:8,	allow [6] - 4:1, 16:2, 26:17, 33:22,
	36:14, 36:17, 36:21, 37:10, 39:3, 43:13,	67:13, 70:11
535 M 15:16	43:19, 44:21, 45:11, 48:4, 48:11, 49:11,	allowing [1] - 37:15
535 [1] - 15:16	49:18, 51:14, 53:12, 53:16, 53:22,	allows [3] - 29:23, 33:12, 35:7
6	57:14, 57:17, 58:24, 60:21, 62:1, 64:4,	almost [2] - 48:23, 66:3
U	64:6, 65:7, 66:14, 66:18, 68:20, 69:7,	alone [2] - 32:2, 33:12
	69:14, 69:15, 70:1, 70:8, 70:12	alternate [1] - 62:13
613-2538 [1] - 2:2	Act's [1] - 18:23	alternative [1] - 62:16
66 [1] - 27:10	acted [1] - 49:14	alternatives [2] - 7:9, 19:22
6th [2] - 6:5, 7:6	action [7] - 14:19, 15:3, 32:25, 39:6,	Ameet [1] - 2:17
_	40:9, 41:2, 57:5	AMEET [1] - 1:20
7	actions [1] - 41:8	amended [1] - 53:17
	activated [1] - 72:13	amending [1] - 53:8
7 [4] - 20:14, 20:16, 33:25, 58:15	active [1] - 42:14 activity [1] - 54:16	Amendment [1] - 43:21
7.0 [2] - 63:6, 63:13	activity [1] - 54.16 actor [2] - 47:22, 53:5	amendments [1] - 53:8
7.0 [2] - 00.0, 00.10 70 [3] - 8:10, 58:7, 61:10	actual [8] - 47.22, 53.5 actual [8] - 14:19, 15:7, 28:23, 30:17,	American [4] - 9:20, 11:8, 47:19
70-cases [1] - 24:19	38:21, 41:15, 68:20, 69:1	Americans [5] - 11:16, 12:1, 12:2,
	33.21, 11.13, 30.20, 30.1	

brief [9] - 3:19, 6:20, 6:24, 9:22, 10:3,

briefing [4] - 2:25, 4:19, 7:20, 28:17

10:6, 32:21, 42:5, 66:2

briefly [1] - 32:21

2

13:9, 13:17 amount [1] - 70:11 analogies [1] - 42:25 analogous [2] - 54:4, 71:19 analogy [1] - 44:6 analysis [9] - 14:5, 25:25, 26:3, 26:6, 27:17, 30:12, 42:20, 43:17, 44:6 analytic [1] - 31:1 analytically [3] - 26:15, 26:22, 49:5 anew [1] - 43:15 announce [1] - 12:20 announced [1] - 13:3 answer [6] - 5:5, 23:25, 27:4, 28:19, 39:11, 60:19 antiquated [1] - 19:10 anyway [3] - 6:3, 26:9, 29:4 apartment [1] - 51:7 apologize [2] - 24:6, 47:9 appeal [1] - 10:19 appearances [1] - 2:13 APPEARANCES [1] - 1:16 apple [1] - 28:24 APPLE [1] - 1:4 Apple [111] - 1:22, 2:10, 2:21, 6:20, 7:14, 7:15, 7:18, 7:20, 7:23, 8:9, 8:12, 8:20, 8:22, 9:3, 9:10, 9:13, 9:14, 9:15, 10:6, 10:14, 10:20, 10:21, 10:23, 11:3, 11:10, 11:17, 12:10, 12:13, 12:18, 13:6, 13:9, 13:12, 13:24, 17:24, 20:16, 21:16, 23:7, 23:11, 24:7, 24:8, 24:23, 25:18, 28:22, 29:17, 29:21, 30:1, 30:18, 30:22, 31:11, 32:13, 32:14, 32:21, 32:25, 33:8, 33:23, 35:25, 39:22, 40:6, 41:1, 41:9, 41:12, 41:13, 41:16, 42:11, 42:17, 47:23, 48:15, 50:13, 50:17, 50:18, 52:12, 54:19, 54:20, 55:10, 55:12, 55:14, 55:16, 55:21, 55:22, 56:24, 57:1, 57:2, 57:3, 58:5, 58:11, 58:14, 58:16, 58:18, 58:19, 58:23, 58:24, 59:15, 59:18, 60:3, 60:10, 60:11, 62:2, 62:3, 62:5, 62:10, 62:17, 63:2, 63:19, 64:9, 64:16, 66:20, 67:20 Apple's [13] - 7:13, 8:5, 9:16, 9:18, 24:21, 25:5, 25:6, 25:9, 25:16, 29:12, 42:21, 59:19, 69:2 applicability [6] - 14:22, 26:8, 26:16, 27:19, 28:10, 31:3 applicable [1] - 43:20 application [11] - 5:17, 5:21, 5:24, 6:2, 9:6, 13:4, 20:14, 28:5, 31:16, 49:6, 70:5 Application [1] - 69:5 applications [2] - 55:25, 56:12 applied [1] - 8:3 applies [1] - 26:4 apply [3] - 20:24, 26:3, 65:7 applying [1] - 7:16 appreciate [4] - 3:2, 12:10, 47:4, 48:24 approach [3] - 37:11, 37:13 appropriate [2] - 27:17, 70:2 area [3] - 30:25, 43:20, 61:18

argue [1] - 64:11 argued [2] - 69:18, 69:20 argument [11] - 2:9, 11:15, 13:17, 23:20, 39:16, 39:20, 42:21, 61:15, 64:23, 66:3, 67:22 ARGUMENT [1] - 1:14 arguments [6] - 42:5, 50:15, 53:25, 59:4, 60:16, 68:9 aside [1] - 10:19 assertion [1] - 3:16 ASSIST [1] - 1:5 assist [8] - 8:10, 26:25, 38:25, 41:24, 52:11, 65:3, 69:5, 70:14 Assist [1] - 2:11 assistance [26] - 6:20, 7:11, 7:13, 8:2, 9:12, 9:14, 9:16, 12:15, 14:13, 24:7, 26:23, 27:15, 27:16, 28:8, 36:1, 49:13, 49:15, 50:3, 65:14, 68:20, 68:25, 69:8, 69:10, 70:19, 72:1 assistant [2] - 16:22, 33:18 Assistant [3] - 1:21, 2:17, 72:5 assisting [1] - 10:8 assume [4] - 6:17, 12:17, 16:16, 20:9 assuming [3] - 20:6, 42:19, 66:14 AT&T [1] - 21:9 atmosphere [1] - 10:1 attached [4] - 5:16, 5:20, 5:24, 6:1 attack [1] - 58:20 attempted [1] - 7:1 attempting [1] - 6:8 attempts [2] - 42:16, 72:13 attention [4] - 3:7, 3:15, 3:23, 4:21 Attorney [1] - 1:17 Attorneys [2] - 1:21, 2:18 Attorneys' [1] - 35:5 AUSA [1] - 72:21 authenticate [2] - 24:11, 32:7 authentication [2] - 63:25, 64:17 authorities [2] - 53:14, 66:22 authority [33] - 9:9, 9:10, 13:5, 16:1, 17:14, 17:20, 18:5, 18:10, 18:20, 19:5, 20:3, 29:20, 38:19, 50:9, 52:3, 55:12, 56:8, 57:15, 58:24, 60:22, 62:1, 65:10, 66:21, 67:4, 67:14, 67:20, 68:6, 68:20, 69:13, 69:15, 69:16, 70:12, 70:18 authorization [1] - 54:23 authorize [1] - 14:15 authorized [1] - 52:3 availability [1] - 44:21 available [14] - 7:9, 8:12, 26:10, 30:4, 31:4, 35:4, 42:18, 55:9, 55:23, 61:5, 61:11, 61:20, 61:22, 62:13 aware [10] - 12:17, 16:16, 16:18, 16:25, 58:11, 63:2, 63:3, 63:10, 63:11, 67:16

В

back-door [2] - 66:11, 66:16

briefs [1] - 24:1 bring [4] - 3:7, 3:15, 3:22, 45:16 brings [1] - 3:16 broad [1] - 9:9 broader [1] - 66:8 broadest [1] - 34:5 broadly [2] - 3:20, 37:19 broke [1] - 63:6 Brooklyn [3] - 1:11, 1:18, 2:2 brought [1] - 69:12 build [1] - 52:10 built [2] - 58:14, 60:11 burden [32] - 8:17, 9:4, 11:4, 12:4, 12:6, 12:7, 13:13, 14:1, 19:22, 24:5, 25:11, 25:15, 26:6, 26:7, 26:18, 26:22, 27:17, 27:19, 30:22, 31:2, 35:25, 43:23, 47:17, 47:18, 53:23, 57:17, 59:5, 61:15, 64:12, 64:18, 71:7, 71:10 burdens [1] - 57:21 burdensome [3] - 30:1, 55:8, 65:24 business [9] - 26:10, 44:1, 51:9, 54:17, 59:19, 59:21, 59:22, 60:10, 62:7 buy [1] - 68:5 buying [1] - 66:3 BY [3] - 1:7, 1:19, 1:24 bypass [12] - 4:7, 6:11, 7:17, 25:21, 25:22, 29:22, 30:18, 39:4, 39:5, 46:25, 59:17, 69:1 bypassing [2] - 8:6, 41:24

C

cab [1] - 27:23 Cadman [2] - 1:18, 2:1 CALEA [19] - 21:8, 21:9, 21:17, 21:18, 21:23, 22:3, 23:8, 37:19, 38:14, 38:17, 38:22, 52:5, 52:6, 52:8, 53:5, 53:7, 65:12, 65:18, 65:19 Calea's [2] - 21:13, 23:15 cannot [5] - 21:2, 34:16, 58:17, 58:18, capability [5] - 9:10, 21:19, 30:17, 34:11, 34:25 capable [3] - 22:11, 39:5, 40:11 CAPERS [1] - 1:17 capture [1] - 26:12 car [1] - 27:23 card [10] - 31:21, 31:22, 31:23, 31:25, 32:1, 40:18, 40:21, 51:5, 51:6 cards [1] - 27:3 care [1] - 58:6 Care [2] - 18:22, 18:23 carrier [3] - 21:14, 22:7, 23:16 carriers [2] - 21:19, 22:4 carry [1] - 20:16 carrying [3] - 9:12, 21:12, 44:2 carves [1] - 37:21 case [57] - 3:11, 4:11, 4:14, 4:15, 4:16, 5:8, 6:25, 9:6, 9:16, 10:14, 10:16,

10:20, 18:1, 20:10, 25:13, 25:21, 26:23, 27:21, 33:18, 33:20, 35:3, 40:17, 40:18, 40:19, 40:20, 41:3, 41:13, 43:17, 45:21, 48:14, 49:4, 49:8, 49:15, 49:21, 50:1, 50:3, 50:11, 56:3, 62:23, 63:15, 64:10, 67:11, 69:12, 69:14, 69:18, 69:20, 69:23, 70:16, 70:21, 71:1, 71:12, 71:19, 72:3. 72:5. 72:11. 72:12 cases [20] - 15:23, 24:7, 24:20, 24:24, 25:4, 25:7, 25:18, 25:23, 26:13, 27:1, 27:2, 27:4, 27:8, 29:1, 43:6, 51:2, 51:14, 55:24, 69:4, 69:6 cast [1] - 39:20 catch [1] - 41:7 categorical [1] - 28:9 categorically [1] - 48:7 category [2] - 26:16, 26:18 cell [1] - 61:19 cellphone [1] - 41:17 cellphones [3] - 7:4, 7:6, 8:7 cellular [1] - 4:8 cents [1] - 47:22 certain [9] - 33:20, 33:22, 52:9, 57:2, 63:24, 64:25, 65:13, 70:11 cetera [1] - 19:23 challenge [3] - 56:15, 56:19, 60:3 challenged [2] - 55:10, 57:18 challenging [1] - 59:15 chance [3] - 50:13, 50:14, 72:16 change [1] - 48:20 changes [1] - 67:9 characteristics [1] - 26:12 characterize [1] - 68:24 characterized [1] - 28:21 choose [2] - 36:12, 36:23 chosen [1] - 65:17 Circuit [7] - 27:10, 28:12, 35:17, 49:4, 49:7, 49:8, 49:23 circumstance [1] - 71:22 circumvent [2] - 53:18, 53:22 cited [7] - 16:9, 16:20, 26:13, 27:2, 49:5, 51:15, 69:4 cites [6] - 15:19, 27:1, 27:8, 27:20, 49:16, 51:3 citizen [1] - 28:3 citizens [1] - 11:16 civil [1] - 2:9 claim [1] - 67:8 clarify [2] - 32:20, 62:20 classic [1] - 23:16 clean [1] - 31:1 clear [18] - 3:3, 4:15, 10:3, 16:21, 16:22, 17:17, 30:15, 57:3, 57:10, 59:8, 60:13, 60:14, 60:20, 60:22, 60:25, 62:1, 68:7, 69:25 clearest [2] - 27:21, 27:24 clearly [8] - 21:9, 27:18, 35:18, 37:22, 49:21, 55:5, 55:17, 64:5 CLERK [1] - 2:9

close [7] - 3:3, 38:23, 40:18, 43:23, 47:3, 64:3, 71:10 closely [4] - 39:18, 45:16, 46:5, 46:7 code [14] - 3:19, 4:5, 4:8, 4:9, 7:17, 25:14, 30:18, 39:4, 41:15, 42:14, 46:25, 72:7, 72:11 codes [1] - 4:2 codified [1] - 18:1 cognizable [1] - 14:19 coherent [2] - 38:1, 38:8 colleague [1] - 2:22 colleagues [2] - 3:8, 5:1 combination [1] - 29:5 combined [1] - 29:3 command [1] - 28:4 commanding [1] - 5:10 comment [6] - 11:8, 11:9, 11:10, 12:4, 56:20, 59:18 commented [1] - 15:17 commerce [1] - 51:10 committee [3] - 15:20, 16:12, 17:7 common [1] - 41:10 communicated [1] - 62:10 communications [8] - 21:20, 22:5, 22:9, 22:11, 51:22, 61:21, 61:24, 64:25 community [1] - 36:5 companies [3] - 9:21, 16:23, 43:6 companion [2] - 40:22, 41:6 company [29] - 9:4, 9:23, 11:9, 11:11, 13:6, 13:9, 14:3, 14:4, 17:2, 17:24, 31:21, 39:4, 43:4, 43:7, 43:24, 44:15, 44:16, 44:24, 45:1, 45:16, 45:25, 46:6, 47:19, 48:2, 51:5, 51:6, 58:6, 64:8, 69:5 company's [3] - 40:14, 41:11, 45:23 comparable [2] - 41:2, 41:9 compel [2] - 48:4, 48:6 compelled [6] - 43:12, 54:20, 55:15, 57:4, 57:11, 59:10 compelling [1] - 48:7 compensation [2] - 57:25, 58:2 competing [1] - 11:19 complete [1] - 6:10 completely [3] - 47:12, 48:23, 52:6 complex [1] - 51:7 complicated [2] - 30:25, 50:6 complied [2] - 8:11, 10:15 complies [1] - 12:10 comply [6] - 10:21, 10:24, 11:17, 60:12, 61:4, 62:8 complying [5] - 8:24, 12:14, 59:5, 61:6. 61:12 comports [1] - 19:11 comprehensive [5] - 25:1, 38:15, 38:18, 38:24, 65:12 compromise [1] - 58:21 compromising [1] - 54:11 computer [1] - 2:4 computer-aided [1] - 2:4 concede [1] - 43:20

4 61:24 conceived [1] - 69:9 Court [31] - 2:1, 5:5, 7:16, 7:18, 8:3, concern [4] - 9:19, 18:24, 38:13, 48:19 context [4] - 39:3, 45:24, 45:25, 47:7 8:7, 9:17, 10:15, 11:11, 14:11, 15:4, concerned [1] - 48:18 continually [1] - 8:25 15:18, 16:2, 17:2, 17:19, 19:25, 20:3, 20:18, 21:15, 24:1, 27:25, 28:21, 32:24, concerns [2] - 30:23, 63:1 continue [3] - 20:24, 37:15, 62:3 36:8, 38:7, 44:12, 44:13, 50:21, 53:3, Continued [1] - 22:13 concession [1] - 57:14 69.18 concluded [1] - 73:16 continues [1] - 52:14 continuing [1] - 60:12 court's [1] - 70:2 conclusions [1] - 52:7 condone [1] - 11:11 control [3] - 51:1, 51:4, 51:8 Court's [4] - 38:13, 38:25, 42:22, 68:19 Courthouse [1] - 1:10 conducting [1] - 39:5 controversy [1] - 55:5 courts [6] - 19:6, 19:18, 39:12, 55:14, confer [1] - 16:1 conversation [1] - 13:2 66:13 conversations [1] - 7:23 conferring [1] - 17:14 covered [1] - 21:9 cop [1] - 27:22 confidence [1] - 60:1 covers [3] - 52:8, 64:6, 65:4 confidential [2] - 64:8, 64:14 copied [1] - 4:10 craft [1] - 57:22 configured [1] - 63:24 copy [1] - 3:9 create [2] - 9:10, 10:1 corporate [3] - 8:6, 11:16, 27:3 confusingly [1] - 27:20 created [2] - 19:17, 40:2 Congress [51] - 13:5, 13:11, 14:12, corporations [1] - 27:3 14:15, 15:8, 15:10, 15:15, 15:16, 15:25, credit [14] - 27:3, 31:21, 31:22, 31:23, correct [10] - 5:13, 5:25, 8:18, 10:23, 31:25, 32:1, 40:17, 40:21, 40:24, 41:5, 16:10, 16:13, 16:16, 16:25, 17:5, 17:13, 15:2, 29:14, 32:24, 34:15, 64:1, 65:16 51:5, 51:6 18:4, 18:8, 18:9, 18:19, 18:24, 19:5, costs (1) - 58:7 crime [3] - 5:11, 36:6, 42:23 19:14, 19:17, 20:2, 20:4, 20:7, 20:23, counsel [5] - 2:21, 4:14, 8:12, 24:21, criminal [2] - 40:15, 41:11 22:4, 36:18, 37:1, 37:14, 38:3, 38:7, 69:1 49:14, 51:18, 51:25, 52:2, 52:4, 53:7, cross [2] - 4:14, 40:12 count [1] - 25:1 53:10, 53:15, 53:20, 64:23, 65:8, 65:10, cross-examination [1] - 4:14 counterfactual [1] - 71:7 65:11, 65:17, 66:15, 66:23, 66:24 crystal [2] - 5:11, 60:20 country [1] - 8:14 congressional [1] - 37:12 Cupertino [1] - 32:15 couple [3] - 12:12, 30:14, 39:8 Congressional [17] - 14:17, 14:18, current [4] - 16:9, 18:20, 20:8, 20:9 course [5] - 4:22, 5:5, 10:12, 51:8, 14:24, 15:3, 16:3, 16:6, 17:18, 18:6, 54:17 cursory [1] - 12:18 18:17, 18:18, 21:4, 21:5, 39:6, 49:3, curtails [1] - 30:8 COURT [152] - 1:1, 1:7, 2:12, 2:19, 49:20, 49:25, 65:5 custodian [1] - 31:25 2:23, 5:7, 5:12, 5:16, 5:20, 5:23, 6:12, connected [2] - 46:6, 46:7 6:15, 8:15, 9:22, 10:17, 10:25, 11:6, custody [1] - 50:24 connection [4] - 40:13, 40:19, 45:21, customer [5] - 58:11, 58:13, 58:22, 11:13, 12:8, 12:20, 12:24, 13:22, 14:2, 71:11 60:24, 62:7 14:5, 14:9, 14:20, 15:1, 15:8, 15:21, connects [1] - 33:3 17:10, 17:23, 18:11, 18:16, 18:24, customers [2] - 12:17, 59:6 conscience [1] - 47:24 19:13, 20:17, 21:3, 21:11, 21:21, 23:1, customers' [2] - 59:20, 59:21 conscientious [2] - 48:5, 48:15 23:18, 23:23, 24:3, 24:22, 25:3, 25:11, cut [1] - 62:1 conscript [2] - 34:23, 60:23 25:24, 27:6, 27:18, 28:14, 28:18, 28:20, conscripted [3] - 28:7, 37:23, 59:22 28:25, 29:7, 29:15, 29:23, 30:2, 30:9, D 30:24, 31:9, 31:13, 32:5, 32:7, 32:17, conscripting [2] - 27:22, 43:1 33:2, 33:5, 33:9, 33:13, 34:2, 34:8, conscription [1] - 51:13 daily [1] - 19:2 34:16, 34:18, 34:22, 35:5, 35:12, 35:16, consider [8] - 8:1, 9:17, 20:3, 30:15, damage [2] - 11:10, 12:5 47:11, 47:14, 48:12, 65:17 36:2, 36:7, 36:16, 37:17, 39:8, 39:11, dare [1] - 34:7 40:7, 40:23, 41:7, 41:12, 41:18, 41:25, consideration [1] - 27:17 dark [1] - 17:1 42:4, 42:24, 43:22, 44:11, 44:16, 45:2, considered [1] - 60:15 darn [1] - 58:6 45:14, 46:3, 46:9, 46:12, 46:16, 46:19, considering [4] - 15:10, 18:19, 22:8, data [17] - 4:3, 10:9, 12:8, 21:20, 46:22, 47:1, 47:10, 47:15, 48:17, 48:21, 45:12 28:23, 28:24, 52:8, 58:11, 58:13, 59:17, 50:12, 50:18, 53:1, 53:6, 53:23, 54:8, consistency [1] - 57:20 59:20, 59:21, 60:11, 60:12, 61:20, 62:7, 54:24, 55:17, 56:10, 57:12, 57:16, 58:3, consistent [5] - 28:6, 37:11, 38:5, 70.18 59:4, 59:24, 60:5, 60:14, 61:1, 62:12, 38:10, 56:24 date [1] - 6:6 62:15, 62:21, 62:24, 63:7, 63:21, 64:3, conspiracy [1] - 5:11 dated [1] - 3:12 64:12, 64:18, 64:21, 65:22, 67:1, 67:11, constitutes [1] - 8:16 days [1] - 73:5 67:17, 68:8, 68:11, 68:15, 68:22, 69:17, consult [2] - 36:5, 72:21 70:20, 71:6, 71:15, 71:18, 72:2, 72:15, DC [1] - 1:23 consulted [1] - 7:2 72:23, 73:7, 73:10, 73:12 DEA [6] - 3:18, 6:25, 33:25, 34:3, 35:4 consumer [2] - 60:10, 61:3 court [40] - 5:9, 8:10, 9:13, 10:19, death [4] - 43:11, 44:2, 44:9, 45:16 consumer's [1] - 60:8 10:20, 10:24, 16:24, 19:19, 21:1, 22:6, debate [18] - 10:12, 14:15, 15:16, consumers [5] - 9:20, 11:8, 59:12, 29:16, 34:12, 45:17, 54:20, 55:1, 55:15, 16:25, 17:5, 17:6, 20:24, 36:15, 53:10, 60:1, 62:11

CMH OCR RMR CRR FCRR

55:16, 55:18, 56:3, 58:23, 59:18, 60:15,

60:20, 61:4, 61:22, 62:4, 65:21, 69:6,

70:21, 70:22, 70:24, 71:3, 71:24, 72:8

69:10, 69:13, 69:14, 70:10, 70:13,

contacted [1] - 56:6

contained [1] - 4:3

contents [4] - 42:15, 51:22, 61:21,

53:22, 64:24, 65:1, 65:2, 65:4, 66:8,

66:20, 66:25

debated [1] - 17:8

debates [1] - 16:12

DISTRICT [2] - 1:1, 1:1 ensured [1] - 19:18 debating [2] - 20:25, 53:8 decide [1] - 65:20 district [1] - 3:12 entangled [1] - 68:1 decided [2] - 36:20, 56:4 District [4] - 35:5, 55:21, 69:4, 69:12 enter [2] - 4:9, 7:1 decides [1] - 43:4 diversion [1] - 23:19 enterprise [1] - 40:15 deciding [1] - 15:5 Djibo [5] - 3:14, 3:22, 4:11, 62:23, 72:5 entire [3] - 35:23, 53:22, 65:2 decision [6] - 6:22, 13:3, 16:18, 65:6, docket [1] - 5:25 entirety [1] - 50:8 66:12, 73:12 doctrine [1] - 65:5 entity [1] - 11:21 decisively [1] - 15:25 dog [1] - 58:8 entry [1] - 4:8 declarant [1] - 63:4 dollars [1] - 47:22 escape [1] - 41:1 declarations [1] - 25:20 done [17] - 9:13, 11:3, 13:14, 14:5, especially [2] - 48:25, 56:11 declaratory [1] - 55:4 15:10, 15:15, 24:25, 38:3, 38:4, 40:2, ESQ [2] - 1:24, 1:25 47:25, 49:10, 54:6, 54:21, 65:12, 66:23 decrypt [5] - 16:23, 22:5, 22:7, 22:10, essence [1] - 22:8 57:1 door [2] - 66:11, 66:16 essential [1] - 69:6 decrypting [1] - 22:11 doubt [1] - 33:5 essentially [4] - 15:14, 32:18, 51:11, decryption [4] - 21:14, 21:24, 23:10 down [3] - 3:9, 66:22, 67:13 defeat [2] - 41:21, 72:18 draw [4] - 48:1, 52:6, 67:5, 67:22 established [1] - 8:23 defeating [1] - 72:17 drawer [1] - 67:25 establishes [2] - 30:9, 45:21 defendant [4] - 40:21, 41:3, 41:13, drawing [1] - 67:19 estimates [1] - 8:9 drug [6] - 43:15, 44:21, 45:1, 46:1, estoppel [1] - 11:2 defendant's [3] - 4:5, 4:14, 7:5 47:2. 47:6 ET [1] - 1:7 defined [2] - 31:10, 37:22 Drug [1] - 44:25 et [1] - 19:23 definitely [1] - 20:18 drugs [4] - 43:4, 43:7, 44:1, 48:2 event [2] - 3:25, 29:4 definition [3] - 23:15, 37:6 due [1] - 18:25 evidence [7] - 5:11, 6:7, 12:9, 13:13, delegating [1] - 20:3 during [1] - 9:2 14:1, 36:19, 42:23 deletes [1] - 42:15 dwindling [1] - 20:22 evolve [1] - 61:19 deliberately [2] - 34:5, 44:19 evolves [1] - 61:25 denied [2] - 49:11, 69:13 E ex [2] - 54:22, 54:25 Department [1] - 3:24 exact [4] - 8:12, 16:10, 45:3, 52:1 deponent [1] - 34:6 exactly [8] - 10:16, 11:5, 28:4, 29:21, easier [1] - 71:11 deputy [1] - 3:9 57:6, 57:23, 69:13, 72:17 easily [4] - 18:8, 18:9, 21:6, 34:9 desegregation [1] - 27:12 examination [1] - 4:14 East [2] - 1:18, 2:1 detail [1] - 24:11 example [11] - 8:5, 15:25, 18:21, EASTERN [1] - 1:1 determined [3] - 7:12, 24:20 24:21, 25:14, 27:21, 27:24, 31:20, easy [1] - 63:18 37:19, 39:14, 51:4 develop [2] - 45:1, 46:11 Education [2] - 27:10, 28:13 examples [1] - 18:18 developed [1] - 17:5 effect [1] - 18:23 device [14] - 4:9, 6:8, 17:2, 21:12, exception [2] - 23:10, 55:20 effective [2] - 19:19, 19:21 23:17, 24:25, 30:18, 32:24, 33:12, excuse [1] - 36:9 effectuate [4] - 19:25, 36:1, 39:12, 33:16, 50:24, 51:10, 57:1, 67:24 execute [3] - 7:10, 29:12, 43:9 devices [10] - 5:19, 16:23, 20:16, 21:1, executed [4] - 6:6, 42:13, 42:23, 44:8 eight [1] - 20:18 54:12, 58:18, 58:22, 59:3, 59:17 executing [2] - 7:7, 8:2 either [4] - 25:1, 26:17, 49:18, 59:22 died [1] - 15:20 Execution [1] - 2:11 Elbert [1] - 2:17 difference [3] - 26:19, 26:21, 51:16 execution [5] - 6:7, 38:25, 42:17, 43:8, ELBERT [1] - 1:20 different [12] - 21:3, 35:19, 37:16, 45:16 electronic [2] - 6:7, 37:20 44:6, 48:5, 48:7, 50:24, 52:6, 58:12, EXECUTION [1] - 1:5 element [3] - 39:17, 43:24, 45:18 60:5, 69:20, 71:5 executions [1] - 44:20 elements [1] - 45:19 difficult [1] - 46:4 executive [1] - 16:22 email [2] - 6:1, 8:21 directions [1] - 58:12 exempted [1] - 21:24 emphasize [1] - 50:20 directly [2] - 70:1, 71:1 exhausted [1] - 48:23 employee [1] - 9:5 director [1] - 16:22 exhaustive [1] - 50:6 enabled [2] - 42:14, 42:16 disagree [2] - 9:24, 55:8 Exhibit [1] - 5:24 encompass [1] - 53:9 disagreeing [1] - 49:19 exist [1] - 63:16 encrypted [1] - 22:5 disclose [3] - 29:18, 63:19, 64:8 existing [2] - 29:23, 43:14 encryption [7] - 13:7, 21:13, 22:1, disclosed [1] - 62:8 exists [1] - 70:3 22:7, 37:21, 40:4, 41:21 discussed [2] - 39:17, 40:16 expanded [1] - 4:12 end [4] - 10:20, 30:12, 35:24, 42:6 discussing [2] - 62:12, 64:23 expands [1] - 3:19 ended [1] - 70:22 discussion [2] - 12:19, 53:17 expansive [1] - 43:21 enforcement [14] - 12:15, 40:20, disobey [1] - 28:3 expect [5] - 7:22, 9:20, 11:8, 11:16, 47:20, 52:2, 52:11, 54:10, 56:7, 56:23, dispute [1] - 42:10 34.9 59:2, 59:17, 59:23, 64:25, 65:3, 65:14 distinction [1] - 50:2 expedite [1] - 23:6 engage [2] - 20:4, 21:14

expedited [1] - 6:21 fighting [1] - 47:3 gap [4] - 14:14, 15:5, 36:14, 53:11 expense [1] - 57:21 figure [2] - 26:7, 65:8 gaps [1] - 38:4 expert [4] - 4:12, 50:23, 59:1, 63:5 filing [1] - 36:14 Gene [1] - 2:1 expired [3] - 5:12, 6:3, 6:16 fill [3] - 38:4, 53:12, 65:21 explain [1] - 32:1 filling [1] - 65:9 56:14 Explain [1] - 59:24 fills [1] - 15:6 glad [1] - 69:11 explained [2] - 4:12, 57:18 fine [4] - 20:10, 47:12, 49:22, 60:17 gorilla [1] - 43:6 explains [1] - 54:8 finely [1] - 35:16 explanation [1] - 72:18 finish [1] - 6:13 explicitly [4] - 16:1, 36:25, 38:7, 39:22 first [21] - 2:24, 5:18, 7:1, 7:15, 8:21, 12:13, 21:8, 30:15, 39:16, 39:24, 43:24, explore [2] - 7:9, 10:13 44:3, 45:18, 45:19, 47:5, 47:6, 54:15, expressed [1] - 39:6

57:17, 66:19, 67:2, 68:19 expressly [1] - 14:13 extend [1] - 68:7 five [1] - 3:23 extending [3] - 40:23, 41:4, 41:5 floor [1] - 16:12

extensive [2] - 25:22, 50:5 focus [2] - 10:3, 51:15 extent [3] - 25:7, 38:4, 47:16 folks [1] - 2:24 extracting [2] - 28:23, 28:24 extractions [1] - 24:25

F

F2D [1] - 27:10

face [1] - 36:19

57:9, 57:14, 58:14

factual [1] - 71:21

fairly [1] - 69:25

falls [1] - 26:22

36:21, 37:1, 48:19, 68:23

fall [3] - 26:16, 26:18

familiar [2] - 18:25, 43:21

fanciful [2] - 43:2, 43:3

Faraday [1] - 32:16

feasible [1] - 30:20

features [1] - 46:1

34:3, 35:3

51:3

facetiously [1] - 66:7

facilities [10] - 26:11, 29:3, 29:6,

facility [3] - 27:13, 48:6, 71:12

factors [4] - 14:6, 43:18, 45:12

32:13, 32:15, 40:14, 45:23, 46:1, 50:25,

fact [20] - 8:15, 16:8, 16:19, 17:5, 17:7,

20:13, 32:23, 36:6, 38:18, 40:16, 43:5,

43:22, 53:25, 56:5, 56:7, 56:13, 56:18,

failed [4] - 3:18, 21:22, 42:16, 72:13

fair [8] - 6:23, 15:9, 17:19, 23:22,

far [9] - 14:17, 15:15, 15:21, 15:24,

FBI[7] - 3:18, 6:25, 7:3, 16:21, 33:24,

feature [4] - 4:2, 41:15, 42:15, 72:12

federal [16] - 5:9, 9:13, 10:11, 19:17,

19:18, 19:19, 29:19, 32:3, 36:4, 40:20,

few [9] - 14:18, 15:16, 15:17, 20:14,

42:13, 55:16, 70:24, 71:12, 71:14

Federal [3] - 38:24, 42:22, 46:11

20:15, 24:19, 36:17, 55:19

fight [2] - 61:5, 61:12

fewer [1] - 44:17

17:11, 24:16, 48:11, 64:23, 68:7

follow [6] - 8:2, 27:23, 33:17, 50:11, 59:11. 72:8

followed [3] - 9:6, 72:4, 72:17 following [1] - 58:10 follows [1] - 11:12 Food [1] - 44:25

force [3] - 17:23, 37:13, 58:24 forced [5] - 58:25, 59:1, 59:2, 62:3, 63:23

forcing [2] - 21:13, 64:7 foreclosed [1] - 53:24

forensic [6] - 4:1, 4:12, 53:14, 59:1, 63:5, 63:12

forensics [1] - 51:13 forget [1] - 3:25 forgive [1] - 10:17 forgotten [1] - 17:25

form [2] - 10:8, 29:16 forma [1] - 56:12

forth [1] - 25:19 forums [1] - 12:19

forward [4] - 39:25, 40:25, 41:2, 58:17

foster [1] - 54:10 foundational [1] - 19:11 four [2] - 15:18

frames [1] - 40:13 frankly [1] - 28:7 frequency [1] - 57:9 front [2] - 37:2, 57:24 frontier [1] - 53:13

frustrate [1] - 44:19 frustrated [1] - 51:25

fugitive [4] - 40:24, 40:25, 41:5 fully [1] - 40:16

fundamentally [1] - 36:13 futile [1] - 56:2

future [2] - 20:25, 63:16

G

gambit [1] - 27:2 game [4] - 15:9, 17:19, 36:21, 37:1

given [5] - 17:4, 20:5, 32:24, 52:10, governed [1] - 39:3 Government [26] - 1:17, 24:16, 25:13, 29:19, 30:20, 32:4, 33:22, 34:3, 34:6, 34:10, 34:16, 35:1, 35:19, 35:20, 35:23, 36:10, 43:8, 45:5, 46:11, 46:12, 46:19, 46:23, 51:3, 51:11, 51:18, 51:22 government [55] - 2:14, 3:10, 3:16, 3:19, 3:20, 3:23, 6:19, 6:24, 7:8, 7:14, 7:15, 7:24, 8:3, 8:14, 9:15, 10:21, 11:22, 12:20, 12:25, 13:3, 13:10, 13:20, 14:13, 14:16, 15:22, 16:17, 16:24, 17:23, 19:23, 53:13, 53:15, 53:19, 53:21, 54:2, 60:23, 61:21, 61:22, 62:17, 63:18, 63:19, 64:16, 65:25, 66:6, 66:14, 66:15, 67:4, 67:6, 67:13, 68:1, 68:6, 69:25, 70:9, 70:17, 71:25 Government's [1] - 50:24 government's [4] - 4:12, 8:2, 9:6, 61:9 Grand [6] - 29:20, 30:11, 30:14, 30:16, 30:21, 31:25

6

grant [3] - 17:19, 61:9, 70:4 granted [3] - 52:4, 66:21, 68:6 grants [1] - 18:10 great [1] - 73:10

greater [2] - 51:20, 51:21 grown [3] - 9:3, 14:3, 14:4 guess [1] - 37:17

guidance [2] - 8:22, 15:24 guidelines [2] - 7:25, 9:1 guys [1] - 73:8

Η

habeas [2] - 71:1, 71:2 Hall [3] - 40:17, 40:23, 45:23 halves [1] - 26:2 hand [3] - 3:9, 25:18, 36:17 handle [1] - 3:2 handled [1] - 72:5 happy [8] - 4:19, 5:5, 10:7, 23:25, 48:12, 50:11, 50:16, 73:1 hard [7] - 19:7, 44:5, 45:10, 47:10, 54:4, 61:14, 67:5 Haute [1] - 43:10 head [1] - 60:8 headquarters [1] - 32:15 hear [5] - 3:6, 4:20, 50:13, 50:15, 50:16 heard [4] - 5:1, 15:17, 63:11, 63:14

hearing [2] - 3:11, 72:9

heart [1] - 14:21

hearings [2] - 16:19, 16:21

CMH 0CR CRR **FCRR** RMR

held [1] - 43:13 65:5 interpretive [1] - 36:24 INC [1] - 1:4 help [7] - 9:25, 11:14, 12:3, 21:6, 43:9, 47:20, 54:9 Inc [2] - 2:10, 55:21 helped [1] - 3:2 include [1] - 51:23 helpful [3] - 3:1, 10:1, 72:25 included [2] - 51:20, 51:23 helping [1] - 41:3 includes [1] - 38:10 helps [1] - 12:10 including [2] - 4:13, 37:15 herring [1] - 42:7 independent [2] - 33:23, 63:13 hesitate [1] - 44:6 indicate [1] - 56:13 higher [2] - 10:19, 30:22 indicated [1] - 9:15 historically [1] - 70:9 indicating [1] - 55:14 history [1] - 54:1 indication [2] - 51:18, 63:11 home [2] - 5:19, 7:5 individuals [1] - 27:4 Homeland [2] - 3:24 indulged [1] - 48:25 honest [1] - 44:4 industry [1] - 37:20 Honor [45] - 2:15, 2:20, 5:3, 6:23, 10:6, infer [1] - 38:2 67:21, 67:23 10:23, 11:5, 11:8, 12:5, 13:20, 14:8, inference [1] - 38:20 14:25, 16:5, 16:8, 16:20, 18:7, 20:21, inflammatory [2] - 47:14, 48:10 21:10, 23:13, 24:15, 29:14, 30:1, 30:13, influences [1] - 18:25 31:17, 32:12, 32:20, 34:7, 36:4, 39:10, information [30] - 23:7, 23:11, 23:15, 44:4, 46:21, 47:13, 48:13, 50:16, 50:19, 63:2, 63:3, 63:6 25:8, 26:9, 27:6, 27:7, 27:13, 28:23, 58:10, 64:20, 68:13, 68:17, 69:11, 28:25, 29:2, 29:6, 29:7, 29:11, 29:13, 69:22, 70:25, 71:20, 72:4, 73:11 29:18, 31:14, 41:6, 48:6, 53:2, 64:5, HONORABLE [1] - 1:14 68:21, 68:25, 69:2, 69:7, 69:9, 70:11, hope [3] - 20:17, 67:17 70:13, 70:15, 72:6 hours [1] - 25:22 informative [1] - 2:25 House [2] - 18:21, 22:2 informed [1] - 33:21 HSI [3] - 3:24, 3:25, 4:4 informing [1] - 8:25 hurt [3] - 13:14, 13:25, 14:3 infringe [1] - 25:16 hypo [1] - 47:4 initial [2] - 8:9, 8:13 hypothetical [7] - 17:21, 35:10, 46:22, initiate [1] - 6:7 ISSUED [1] - 1:7 47:13, 48:10, 60:8, 60:9 initiates [1] - 72:13 44:10 injection [2] - 43:4, 44:15

Т

idea [2] - 12:25, 28:7 identified [2] - 11:20, 24:17 identify [1] - 11:22 ignore [1] - 36:7 III_[5] - 21:20, 22:10, 50:3, 50:4, 67:8 illegal [1] - 45:24 immediate [1] - 57:21 impact [1] - 11:12 imperil [4] - 59:11, 60:18, 61:3, 61:14 imperils [1] - 61:11 implemented [1] - 67:9 implicate [1] - 25:8 implicated [1] - 25:5 implicates [1] - 59:5 implied [2] - 38:22, 39:6 import [1] - 43:13 importance [1] - 20:23 important [8] - 5:8, 7:15, 11:25, 14:21, 51:16, 56:21, 58:13, 71:21 impose [1] - 25:16 impractical [1] - 37:10 improper [2] - 10:9, 10:10 IN [1] - 1:5 inaction [5] - 15:3, 37:12, 49:3, 49:25,

inserted [1] - 39:19 inside [1] - 53:1 insight [1] - 11:4 insisted [1] - 7:25 instance [2] - 24:17, 71:4 instances [1] - 61:10 instead [1] - 47:3 instruct [1] - 70:14 instruction [1] - 64:2 Intel [1] - 34:10 intelligence [1] - 36:5 intend [1] - 3:8 intended [4] - 32:21, 45:20, 51:18, 65:11 intending [1] - 38:3 intent [3] - 19:8, 45:15, 51:25 intentionally [2] - 48:1, 48:9 intercept [1] - 21:19 intercepted [1] - 22:9 interest [1] - 11:19 interesting [2] - 24:15, 35:9 interests [5] - 11:23, 25:5, 25:9, 25:17, 55:18 internal [1] - 32:2 internet [1] - 33:3 interpretation [1] - 38:21

interrupting [1] - 10:18 interstitial [1] - 65:9 intervening [1] - 18:14 introduce [1] - 25:10 introductory [1] - 5:4 intuitive [1] - 24:9 investigate [1] - 36:5 investigation [7] - 12:11, 33:24, 39:23, 40:1, 40:3, 40:8, 46:24 invitation [1] - 61:7 invited [3] - 55:16, 55:18, 59:18 invoke [2] - 9:8, 57:16 involve [3] - 25:21, 32:16, 51:3 involved [5] - 6:25, 33:19, 58:18, involves [2] - 27:9, 40:20 involving [1] - 30:1 IOS [14] - 4:17, 20:14, 20:16, 20:25, 33:19, 33:23, 33:25, 58:15, 58:16, 63:1, iPhone [5] - 3:17, 4:3, 4:6, 4:16, 63:6 ironic [1] - 59:13 irrelevant [1] - 13:21 issuance [2] - 6:6, 69:25 issue [29] - 3:17, 3:21, 6:21, 7:5, 9:25, 12:3, 12:22, 17:1, 20:12, 20:15, 20:22, 20:25, 25:4, 25:7, 25:24, 29:20, 34:8, 35:8, 36:20, 37:18, 38:17, 38:23, 39:7, 40:12, 53:23, 56:4, 56:14, 64:15, 65:21 issued [7] - 5:9, 5:15, 6:5, 9:12, 19:19, issues [7] - 3:3, 10:13, 14:21, 19:20, 20:6, 57:15, 69:6 issuing [1] - 31:20 items [1] - 73:2 iterations [1] - 38:18 itself [6] - 13:1, 14:1, 25:5, 50:4, 58:19, 60:12

J

jail [1] - 60:18 JAMES [1] - 1:14 Jeffrey [1] - 2:22 JEFFREY [1] - 1:25 job [1] - 45:4 Johnson [1] - 3:11 joined [2] - 2:17, 2:21 joke [1] - 35:14 JUDGE [1] - 1:15 Judge [4] - 3:11, 69:17, 69:22, 73:15 judges [1] - 56:9 judgment [1] - 55:4 Judiciary [1] - 19:10 judiciary [1] - 20:4 July [4] - 3:12, 6:5, 6:19, 7:6 jumping [1] - 48:25

jury [1] - 44:10 Justice [3] - 43:5, 69:18, 69:21 justification [1] - 64:10

30:21, 31:25

K

Kabrawala [1] - 2:17 KABRAWALA [1] - 1:20 keep [4] - 26:7, 31:1, 55:3, 68:8 keeps [1] - 26:6 kev [1] - 38:16 kill [1] - 48:3 kin [1] - 40:11 kind [6] - 12:8, 21:12, 24:10, 28:4, 54:9, 56:14 kinds [2] - 28:8, 37:14 knowledge [2] - 20:7, 33:19 KOMATIREDDY [110] - 1:19, 2:15, 5:3, 5:8, 5:14, 5:18, 5:22, 6:5, 6:14, 6:23, 8:18, 10:5, 11:5, 11:7, 12:4, 12:12, 12:22, 13:19, 13:23, 14:4, 14:8, 14:11, 14:25, 15:7, 15:14, 16:5, 17:21, 18:7, 18:15, 18:17, 19:9, 19:16, 20:21, 21:10, 21:17, 22:2, 23:13, 23:22, 23:25, 24:15, 26:21, 27:7, 28:13, 28:16, 28:19, 28:21, 29:5, 29:14, 29:19, 29:25, 30:6, 30:13, 31:6, 31:12, 31:17, 32:6, 32:12, 33:7, 33:11, 33:17, 34:7, 34:15, 34:17, 34:20, 35:2, 35:9, 35:15, 35:24, 36:3, 36:13, 37:9, 38:13, 39:10, 40:5, 40:10, 41:4, 41:10, 41:14, 41:23, 42:2, 42:11, 43:16, 44:4, 44:14, 44:23, 45:7, 45:20, 46:4, 46:10, 46:15, 46:17, 46:21, 46:24, 47:9, 47:13, 48:12, 48:18, 50:1, 50:16, 68:17, 68:23, 70:6, 70:25, 71:9, 71:17, 71:20, 72:4, 72:20, 73:5, 73:15 Komatireddy [7] - 2:16, 4:25, 25:24, 52:12, 62:12, 63:1, 64:1 Komatireddy's [1] - 64:22

L

labor [1] - 69:9
lack [1] - 49:20
LANDIS [1] - 1:25
Landis [1] - 2:22
language [16] - 7:24, 8:4, 17:14, 17:22, 34:5, 56:21, 56:22, 57:2, 57:8, 57:14, 57:16, 57:19, 57:22, 57:24, 59:9, 69:25
larger [1] - 18:1
last [10] - 12:13, 15:22, 17:10, 39:11, 43:4, 43:7, 44:16, 49:2, 70:20
LAUREN [1] - 1:20
Lauren [1] - 2:17

14:14, 15:7, 15:8, 16:8, 18:9, 20:8, 20:9, 26:23, 30:4, 35:17, 37:3, 37:4, 38:11, 38:12, 38:17, 39:7, 40:20, 41:1, 43:20, 44:23, 44:25, 45:22, 47:20, 48:20, 52:1, 52:11, 53:11, 53:12, 54:10, 56:7, 56:23, 59:2, 59:10, 59:11, 59:17, 59:22, 60:23, 61:18, 61:19, 61:25, 64:24, 65:3, 65:14 lawful [8] - 10:15, 43:11, 44:2, 45:17, 60:13, 60:14, 60:16, 62:8 lawyers [1] - 69:20 leading [1] - 66:21 learned [1] - 4:18 least [6] - 8:10, 12:2, 18:21, 39:21, 71:13, 72:6 leaves [1] - 38:19 leaving [1] - 10:18 left [2] - 17:9, 39:7 legal [15] - 7:24, 9:1, 9:8, 9:25, 10:4, 10:8, 12:3, 18:20, 24:2, 37:13, 54:15, 62:16, 64:9, 70:17 legally [5] - 14:19, 53:24, 63:21, 63:22, 64:3 legislates [1] - 20:7 legislation [10] - 12:21, 13:21, 15:11, 17:3, 17:16, 38:5, 49:10, 49:20, 66:11, legislative [3] - 19:5, 38:15, 38:16 length [2] - 9:22, 40:18 lesser [1] - 51:23 lethal [1] - 43:4 letter [4] - 3:10, 3:12, 3:23, 73:2letters [1] - 73:4 letting [1] - 29:6 level [4] - 15:3, 24:11, 56:11, 62:16 licences [1] - 41:16 license [2] - 42:6, 42:7 lies [1] - 61:9 light [1] - 59:14 likelihood [1] - 71:23 limit [2] - 27:15, 28:9 limited [1] - 56:1 limits [1] - 15:13 line [3] - 67:5, 67:19, 68:3 lines [1] - 31:1 list [1] - 15:23 litigation [1] - 32:8 location [1] - 41:6 lock [4] - 41:15, 41:24, 42:14, 65:18 locked [4] - 8:7, 12:15, 67:22, 67:25

looking [4] - 23:14, 37:10, 38:14, 49:9 loop [1] - 64:3 lose [2] - 39:9, 60:1 losing [1] - 26:7 loudly [1] - 15:4 8

M

magistrate [1] - 56:11 MAGISTRATE [1] - 1:15 magistrates [1] - 55:13 main [1] - 68:19 majority [1] - 24:6 managed [1] - 25:9 manner [2] - 8:11, 45:1 manual [1] - 64:2 manufacture [2] - 21:11, 43:14 manufacturers [1] - 23:17 MARC [1] - 1:24 Marc [1] - 2:21 market [1] - 13:15 marketing [1] - 47:21 Marshal [1] - 70:23 marshals [1] - 72:1 Marshals [5] - 30:3, 30:7, 31:4, 70:21, 71:13 materials [1] - 3:22 matter [7] - 13:12, 20:4, 32:23, 38:20, 47:21, 47:24, 73:16 matters [1] - 6:16 MC [1] - 1:8 mean [9] - 30:17, 34:25, 39:19, 45:24, 46:12, 58:5, 59:8, 64:13, 70:8 meaning [3] - 23:7, 49:19, 49:24 meaningless [1] - 14:24 means [2] - 62:13, 63:15 mechanical [1] - 2:4 mechanism [3] - 62:7, 63:2, 63:18 members [1] - 15:16 mentioned [1] - 51:2 mere [1] - 61:20 meth [1] - 5:11 method [1] - 63:19 middle [1] - 58:19 might [3] - 32:7, 46:12, 62:13 mind [9] - 3:4, 17:4, 19:24, 23:2, 24:22, 38:1, 49:21, 64:19, 66:1 minimal [1] - 9:5 minute [2] - 36:9, 60:3 minutes [1] - 36:17 Miscellaneous [1] - 2:10 mischaracterizing [1] - 15:1 missing [1] - 50:9 mistaken [3] - 4:17, 23:9, 57:24 mode [1] - 6:9 modifying [1] - 67:7 moment [3] - 23:9, 47:9, 68:10 monitoring [1] - 69:6

CMH OCR RMR CRR FCRR

look [21] - 11:15, 13:8, 13:13, 13:16,

36:18, 36:22, 43:19, 43:24, 44:11,

16:19, 27:18, 28:14, 30:25, 34:9, 35:16,

56:10, 57:16, 65:11, 65:24, 69:3, 71:21

locksmith [1] - 43:2

long-standing [1] - 8:6

logs [1] - 51:4

monopoly [1] - 43:25 moot [1] - 23:1 morning [4] - 2:12, 2:15, 2:20, 2:23 most [5] - 5:8, 14:21, 51:16, 64:8, 64.14 motion [2] - 21:20, 61:9 move [1] - 14:9 moving [1] - 20:2 MR [43] - 2:20, 10:23, 24:23, 25:6, 25:15, 32:20, 33:4, 50:19, 53:3, 53:7, 54:7, 54:13, 55:10, 56:5, 56:20, 57:13, 58:1, 58:9, 59:13, 60:2, 60:9, 60:19, 61:17, 62:14, 62:19, 62:22, 62:25, 63:10, 63:22, 64:7, 64:13, 64:20, 64:22, 66:19, 67:2, 67:16, 67:19, 68:10, 68:13, 69:11, 69:24, 73:9, 73:11 MS [109] - 2:15, 5:3, 5:8, 5:14, 5:18, 5:22, 6:5, 6:14, 6:23, 8:18, 10:5, 11:5, 11:7, 12:4, 12:12, 12:22, 13:19, 13:23, 14:4, 14:8, 14:11, 14:25, 15:7, 15:14, 16:5, 17:21, 18:7, 18:15, 18:17, 19:9, 19:16, 20:21, 21:10, 21:17, 22:2, 23:13, 23:22, 23:25, 24:15, 26:21, 27:7, 28:13, 28:16, 28:19, 28:21, 29:5, 29:14, 29:19, 29:25, 30:6, 30:13, 31:6, 31:12, 31:17, 32:6, 32:12, 33:7, 33:11, 33:17, 34:7, 34:15, 34:17, 34:20, 35:2, 35:9, 35:15, 35:24, 36:3, 36:13, 37:9, 38:13, 39:10, 40:5, 40:10, 41:4, 41:10, 41:14, 41:23, 42:2, 42:11, 43:16, 44:4, 44:14, 44:23, 45:7, 45:20, 46:4, 46:10, 46:15, 46:17, 46:21, 46:24, 47:9, 47:13, 48:12, 48:18, 50:1, 50:16, 68:17, 68:23, 70:6, 70:25, 71:9, 71:17, 71:20, 72:4, 72:20, 73:5, 73:15 multiple [1] - 56:9

Ν

must [3] - 10:20, 60:15, 70:3

narrow [2] - 64:24, 70:17 narrower [1] - 66:2 narrowly [1] - 36:18 nature [4] - 25:4, 26:23, 27:15, 27:16 navigate [1] - 34:9 necessarily [3] - 27:12, 47:23, 56:13 necessary [4] - 19:25, 36:1, 36:8, 70:2 necessity [2] - 36:2, 36:3 need [11] - 6:21, 23:6, 30:25, 32:5, 32:7, 32:10, 34:18, 50:1, 53:3, 54:2, 55:17 needed [1] - 19:20 needn't [1] - 19:1 needs [3] - 23:4, 53:10, 53:20 negative [1] - 11:12 negotiating [1] - 25:20 never [9] - 8:11, 15:19, 52:2, 54:19, 56:18, 58:1, 58:12, 59:20, 65:10 nevertheless [1] - 4:5

new [10] - 9:8, 9:9, 53:13, 59:3, 66:4, 66:21, 66:22, 67:3, 68:5 NEW [1] - 1:1 New [27] - 1:11, 2:2, 26:4, 26:19, 26:24, 27:1, 27:5, 27:8, 27:20, 27:24, 39:17, 39:21, 40:13, 43:18, 43:24, 45:18, 45:22, 47:6, 47:17, 49:5, 49:16, 51:17, 51:20, 54:16, 67:22, 69:3, 71:8 newer [1] - 66:5 next [3] - 18:12, 22:13, 52:14 Nickerson [2] - 69:17, 69:22 nine [1] - 20:19 Ninth [4] - 49:4, 49:6, 49:8, 49:23 nobody [1] - 47:2 normal [2] - 51:8, 54:17 note [5] - 5:23, 7:4, 7:15, 21:22, 48:14 note-taking [1] - 21:22 noted [1] - 6:24 notes [1] - 24:4 nothing [4] - 18:19, 40:7, 55:25, 67:24 notice [1] - 33:17 noting [1] - 8:20 notion [1] - 11:11 number [6] - 4:25, 8:12, 8:13, 18:18, 20:5, 24:22 NW [1] - 1:23

0

NY [1] - 1:18

o'clock [1] - 1:12 Oakland [1] - 55:23 objected [1] - 8:11 objection [3] - 48:5, 48:15, 48:16 obligation [8] - 21:25, 22:10, 35:17, 36:4, 52:10, 55:2, 59:10, 60:17 obligations [1] - 21:25 observation [1] - 14:12 obsolete [1] - 20:15 obtain [4] - 4:3, 4:6, 70:11, 70:18 obtained [1] - 16:24 obtaining [3] - 16:17, 69:8, 70:14 obvious [2] - 50:9, 68:3 obviously [2] - 18:24, 64:6 October [2] - 1:12, 6:19 odds [1] - 19:6 OF [3] - 1:1, 1:6, 1:14 offensive [1] - 54:18 offered [1] - 56:22 office [3] - 35:6, 35:12, 35:19 old [1] - 59:3 once [3] - 4:9, 7:12, 62:2 one [61] - 3:7, 3:17, 4:25, 5:15, 5:16, 5:20, 7:19, 7:21, 11:7, 14:10, 14:21, 15:11, 16:20, 17:10, 17:16, 17:24, 21:3, 24:5, 26:3, 26:15, 27:8, 29:3, 34:12, 36:17, 36:23, 37:1, 37:2, 38:16, 38:19, 39:14, 40:16, 41:14, 42:25, 43:3, 44:8, 44:18, 45:11, 49:2, 54:25, 55:20, 55:22,

56:20, 56:22, 57:4, 59:4, 59:9, 61:18, 62:16, 65:17, 66:2, 66:7, 67:3, 67:23, 68:10, 69:3, 69:18, 69:19, 70:10, 70:20, ongoing [3] - 8:13, 40:15, 55:5 onwards [1] - 26:24 open [1] - 34:11 operates [2] - 20:9, 42:12 operating [7] - 20:10, 33:21, 40:2, 41:15, 42:22, 58:14, 58:16 opinion [1] - 15:19 opportunity [2] - 4:22, 10:13 opposed [5] - 28:7, 31:23, 31:24, 35:17. 72:1 opposite [2] - 28:4, 52:1 oral [1] - 2:9 order [38] - 7:9, 7:18, 8:1, 8:3, 8:7, 10:20, 10:24, 16:24, 17:2, 21:1, 27:9, 27:11, 29:17, 31:20, 35:8, 36:5, 44:7, 44:12, 44:13, 45:12, 45:17, 52:2, 54:20, 55:11, 57:3, 59:5, 61:4, 61:5, 61:12, 61:22, 64:5, 64:6, 64:11, 67:8, 69:8, 70:1, 71:24 ORDER [1] - 1:4 Order [1] - 2:10 ordered [4] - 22:6, 25:12, 59:25, 68:2 ordering [2] - 21:15, 62:17 orders [26] - 8:10, 10:15, 12:14, 12:16, 16:18, 19:18, 19:19, 19:25, 54:25, 55:13, 55:14, 55:19, 55:25, 56:6, 56:12, 56:19, 56:23, 56:24, 57:15, 60:4, 60:13, 62:8, 66:18, 69:5, 69:7, 70:9 ORENSTEIN [1] - 1:14 organized [1] - 36:10 original [1] - 49:13 orthodoxy [1] - 61:23 otherwise [4] - 17:18, 22:12, 44:22, 50:9 ourselves [1] - 36:10 outset [1] - 50:2 outside [3] - 52:6, 52:13, 53:5 outstripped [1] - 19:3 overall [2] - 38:5, 49:9 override [1] - 4:2 owes [1] - 41:16 own [11] - 7:2, 20:5, 21:22, 26:10, 33:19, 42:3, 46:11, 46:13, 46:23, 51:12, 59:22 owner [1] - 41:16

Р

owns [1] - 42:12

page [3] - 3:23, 22:13, 52:14 pains [1] - 59:8 parallels [1] - 48:1 parents [2] - 27:9, 27:11 parse [1] - 16:4 part [12] - 3:16, 16:20, 18:1, 26:6,

27:18, 27:19, 40:14, 46:4, 47:18, 57:5, 66:5, 67:13, 68:5, 69:5 private [3] - 11:21, 28:3, 47:22 69:9, 71:14 phones [7] - 7:7, 12:15, 17:24, 59:9, pro [1] - 56:12 parte [2] - 54:22, 54:25 66:4, 66:6, 67:3 problem [1] - 47:10 particular [11] - 20:12, 20:22, 27:11, phrased [1] - 38:9 problems [2] - 65:10, 67:4 33:19, 33:23, 38:19, 39:3, 46:25, 69:8, picture [2] - 58:7, 65:25 procedure [4] - 8:23, 9:7, 29:23, 30:4 71:22, 71:24 place [5] - 23:20, 26:7, 49:1, 50:5, proceeding [2] - 54:22 particularly [1] - 45:9 53:15 Proceedings [1] - 2:4 parties [6] - 27:1, 37:22, 38:25, 39:13, placing [1] - 6:9 proceedings [1] - 54:25 42:8, 63:12 plainly [1] - 9:4 process [12] - 7:6, 7:23, 7:25, 8:20, partly [1] - 49:14 plans [1] - 61:8 9:1, 25:22, 28:23, 29:16, 60:7, 62:17, parts [1] - 19:10 play [1] - 56:7 66:24, 69:1 party [7] - 7:11, 26:24, 29:2, 34:23, Plaza [2] - 1:18, 2:1 processing [2] - 8:24, 9:3 39:15, 51:8, 70:14 plenty [1] - 56:11 produce [1] - 31:24 party's [1] - 51:4 point [26] - 11:7, 13:19, 13:21, 13:23, produced [1] - 2:4 pass [16] - 3:19, 4:2, 4:5, 7:17, 16:8, 14:10, 19:17, 20:21, 42:11, 43:25, product [3] - 67:10, 67:21, 67:23 25:14, 30:18, 37:14, 39:4, 41:15, 42:13, 44:17, 46:18, 47:21, 47:22, 57:8, 58:5, proffer [1] - 69:24 42:14, 46:25, 71:7, 72:7, 72:11 60:25, 61:14, 63:25, 64:14, 65:7, 66:9, prohibit [3] - 16:7, 17:8, 17:22 passed [13] - 16:11, 17:8, 17:16, 66:19, 67:2, 67:19, 71:2, 71:4 prohibited [2] - 37:1, 38:7 18:21, 19:9, 19:13, 19:14, 38:17, 44:3, points [5] - 23:24, 50:20, 52:12, 68:14, prohibiting [2] - 15:9, 16:8 49:14, 53:17, 65:8 68:18 prohibition [2] - 15:12, 38:22 passes [1] - 18:2 policy [1] - 44:19 promote [1] - 12:11 passing [1] - 15:8 pops [1] - 50:2 prong [5] - 26:5, 36:2, 36:3, 47:6, password [4] - 6:11, 13:6, 17:25, posed [1] - 17:12 67:22 21:13 posited [1] - 62:4 prongs [1] - 71:8 past [8] - 11:2, 13:6, 16:22, 17:7, positing [1] - 47:1 propose [1] - 59:9 24:25, 55:5, 59:15, 61:15 position [15] - 9:17, 9:18, 11:22, proposed [6] - 14:18, 15:18, 16:9, path [3] - 31:4, 31:6, 59:24 11:24, 12:5, 24:12, 39:22, 39:25, 45:3, 17:7, 19:4 patient [1] - 50:18 53:4, 58:17, 58:20, 59:16, 62:9, 62:11 proposition [1] - 3:17 patriotic [1] - 10:2 possession [3] - 4:1, 51:1, 51:7 proprietary [2] - 25:9, 25:16 patriotism [3] - 9:23, 10:5, 11:9 possibility [3] - 10:19, 34:10, 40:3 prosecuting [1] - 35:3 pause [1] - 68:12 possible [5] - 36:15, 38:18, 40:25, prosecution [2] - 34:21, 34:22 Pause [1] - 47:8 47:3, 72:11 prosecutors [5] - 8:14, 24:16, 24:18, paying [1] - 60:17 possibly [1] - 42:16 35:3, 36:4 pejoratively [1] - 39:20 potential [1] - 44:9 prospect [1] - 25:12 pen [2] - 51:24 power [6] - 51:19, 51:21, 51:23, 53:21 prospective [1] - 22:9 pending [1] - 32:19 powers [3] - 19:7, 19:12, 20:1 prospectively [2] - 41:3, 41:8 Pennsylvania [4] - 30:2, 30:6, 31:3, practical [4] - 36:14, 37:10, 37:11, protect [1] - 9:21 37:13 provide [14] - 9:16, 13:6, 15:23, 21:25, people [8] - 12:9, 16:4, 16:7, 16:14, practically [1] - 36:22 28:16, 53:14, 58:24, 62:1, 64:1, 65:13, practice [10] - 8:6, 8:25, 11:2, 12:14, 69:15, 70:11, 70:12, 72:6 25:1, 25:7, 47:19, 48:3 per [1] - 8:19 12:16, 16:7, 16:17, 16:25, 17:8, 72:21 provided [7] - 2:25, 7:24, 8:22, 9:14, perceived [2] - 11:10, 56:16 precedent [2] - 31:19, 51:14 22:7, 57:19, 69:16 percent [1] - 58:18 preliminary [1] - 17:6 provider [5] - 21:14, 21:25, 22:10, perception [2] - 48:19, 48:20 prepare [1] - 25:7 54:17, 54:18 perform [5] - 51:12, 54:21, 57:4, presence [1] - 50:6 providers [7] - 52:9, 53:10, 53:14, 58:18, 65:19 pressed [1] - 11:21 63:12, 65:2, 65:13 performing [2] - 51:24 pretend [1] - 72:17 provides [3] - 27:16, 57:15, 60:21 perhaps [4] - 24:20, 29:17, 38:20, pretty [2] - 15:23, 58:6 providing [9] - 12:14, 41:13, 43:7, 46:14 prevent [2] - 21:15, 60:11 50:23, 50:25, 52:9, 54:8, 64:24, 67:25 period [1] - 8:23 preventing [1] - 42:12 provision [5] - 18:1, 21:13, 21:23, permit [2] - 31:7, 45:11 primarily [1] - 7:1 22:2. 71:2 person [4] - 40:21, 40:24, 41:8, 63:5 principles [4] - 37:4, 37:18, 37:25, public [8] - 8:25, 12:16, 13:25, 23:16, personal [1] - 33:19 38:11 44:19, 48:19, 66:20, 66:25 personally [2] - 63:6, 72:8 prioritization [1] - 20:5 publicly [1] - 55:23 personnel [1] - 71:3 prioritize [1] - 20:11 published [1] - 12:13 perspective [1] - 25:6 priority [1] - 73:4 publishing [1] - 9:1 phone [21] - 3:21, 5:10, 7:1, 7:13, 29:8, prisoner [3] - 70:23, 71:12, 71:25 Puerto [2] - 69:4, 69:12 29:18, 31:14, 32:11, 33:25, 42:3, 42:15, privacy [5] - 9:21, 53:19, 54:11, 58:13, purpose [1] - 45:25 46:25, 51:5, 62:18, 63:9, 63:13, 63:15, 58:21 purposefully [1] - 47:15

purposes [4] - 26:10, 26:19, 34:13, 43:23 pushing [1] - 53:12 put [4] - 4:20, 24:12, 51:10, 61:14 puts [3] - 19:5, 37:21, 58:16 putting [1] - 11:13

Q

qualify [1] - 23:11 query [1] - 8:13 questioning [1] - 9:23 questions [13] - 3:5, 4:25, 5:5, 21:8, 23:23, 24:1, 26:15, 27:5, 39:8, 45:10, 47:10, 48:23, 56:25 quick [1] - 3:1 quickly [1] - 73:13 quite [2] - 66:7, 66:9 quo [3] - 16:15, 17:9, 37:15 quoted [1] - 8:21

R

raise [1] - 6:18 rather [2] - 72:18, 73:4 Re [2] - 2:10, 69:5 re [1] - 43:13 re-import [1] - 43:13 reached [3] - 7:14, 7:15, 66:8 read [5] - 16:13, 37:7, 56:18, 69:23, reading [4] - 36:25, 49:18, 50:7, 69:13 readings [1] - 69:20 realistic [1] - 25:12 realize [1] - 20:8 really [18] - 3:2, 8:17, 9:25, 10:3, 13:14, 21:5, 27:2, 35:7, 36:19, 45:4, 47:4, 48:21, 49:5, 49:17, 55:7, 60:5, 65:24, 72:25 realtime [2] - 21:19, 22:8 reason [11] - 3:22, 9:18, 13:1, 16:6, 20:11, 23:8, 33:5, 37:12, 40:12, 44:5, 72:12 reasonable [9] - 7:9, 12:17, 16:16, 18:23, 19:21, 20:9, 20:23, 35:4, 38:20 reasonably [1] - 16:13 reasons [6] - 12:25, 16:14, 36:11, 37:14, 56:22, 57:19 received [2] - 8:10, 55:11 receiving [2] - 55:13 recent [2] - 14:15, 43:6 recently [2] - 19:14, 66:9 record [5] - 8:21, 17:17, 32:4, 62:20, recorded [1] - 2:4 records [13] - 4:6, 4:10, 27:3, 31:21, 31:23, 31:24, 32:1, 32:5, 32:8, 40:18, 40:21, 50:25, 51:3

recounted [1] - 6:20 red [1] - 42:7 referred [2] - 15:20, 43:5 refund [1] - 49:11 refused [1] - 14:15 regard [1] - 62:22 regime [1] - 18:3 register [2] - 51:24, 51:25 regression [1] - 14:5 regularly [1] - 55:13 regulates [1] - 37:19 regulating [1] - 42:8 rehearse [1] - 19:1 reject [1] - 15:25 rejected [1] - 16:3 related [5] - 21:8, 29:15, 39:18, 57:1, relation [1] - 71:13 relationship [2] - 43:23, 59:6 relatively [1] - 50:6 release [1] - 43:14 relevance [1] - 42:9 relevant [3] - 42:11, 43:19, 44:25 relief [3] - 7:16, 35:20, 49:6 relieve [1] - 55:2 rely [2] - 24:1, 66:13 remain [1] - 16:15 remarks [1] - 5:4 remember [1] - 5:9 remind [1] - 65:22 reminded [2] - 39:11, 69:17 remote [5] - 32:16, 32:17, 32:22, 32:23, 42:18 renewed [1] - 6:17 reopen [1] - 66:15 repeal [1] - 18:22 repeatedly [1] - 56:6 Reporter [1] - 2:1 reports [1] - 22:3 represent [2] - 40:10, 72:7 representation [11] - 33:6, 33:7, 34:2, 34:4, 34:6, 34:13, 34:18, 34:20, 35:7, 35:20, 35:22 represented [2] - 42:18, 69:1 representing [1] - 45:4 represents [1] - 9:17 reputation [1] - 9:5 reputational [2] - 12:7, 14:1 request [12] - 6:17, 8:2, 9:11, 32:18, 32:22, 32:23, 39:4, 49:12, 54:3, 72:1, 73:5 requested [3] - 8:1, 38:19, 70:1 requesting [6] - 10:16, 14:14, 14:16, 16:10, 17:22 requests [3] - 8:24, 9:3, 32:16 require [11] - 13:5, 13:11, 44:24, 45:1,

24:18, 24:24, 26:25, 53:5, 56:15, 56:25, 57:6, 57:7, 58:1, 61:24, 62:9, 65:3, 65:13, 65:19, 69:2, 70:23, 71:3 requirement [1] - 4:8 requires [5] - 21:18, 21:21, 45:12, 63:24, 64:16 Requiring [1] - 2:10 REQUIRING [1] - 1:4 requiring [8] - 8:7, 8:10, 10:15, 27:9, 27:11, 38:25, 39:14, 50:3 research [1] - 13:15 resolve [2] - 9:25, 69:21 resolved [2] - 24:8, 24:20 resources [1] - 9:5 respect [1] - 37:20 respects [1] - 37:21 respond [1] - 49:22 response [2] - 49:15, 68:16 responsibility [2] - 10:7, 22:5 responsible [2] - 8:6, 35:18 responsive [1] - 48:24 restricts [1] - 23:16 result [4] - 10:20, 15:11, 54:23, 66:23 retain [1] - 21:19 return [1] - 43:17 reveal [2] - 24:13, 25:14 reversal [2] - 9:18, 9:19 review [3] - 50:1, 50:11, 64:23 reviewed [1] - 45:22 revised [1] - 7:20 revisiting [1] - 19:2 Rico [2] - 69:4, 69:12 rid [1] - 32:17 rights [2] - 9:24, 56:16 ring [1] - 67:14 road [1] - 66:22 ROBERT [1] - 1:17 robust [1] - 66:20 role [1] - 65:2 room [2] - 32:16, 33:2 routine [2] - 9:7, 9:11 routinely [1] - 8:23 Rudolph [1] - 2:1 Rule [4] - 30:9, 30:10, 69:16, 70:7 ruled [1] - 69:14 run [1] - 27:2 running [4] - 4:16, 27:22, 63:6

S

safe [1] - 43:1 safety [1] - 9:21 salient [1] - 20:25 SARITHA [1] - 1:19 Saritha [1] - 2:16 satisfied [1] - 45:17 satisfy [2] - 45:18, 47:5 saw [1] - 57:3 scenario [3] - 17:12, 47:1, 47:7

49:15, 53:14, 57:23, 57:25, 68:20,

required [20] - 7:25, 24:10, 24:11,

69:10, 70:22

squarely [1] - 19:5 schedule [3] - 3:1, 7:20, 73:1 short [4] - 15:8, 15:14, 41:20, 41:23 scheduling [1] - 23:5 shown [1] - 14:15 squares [1] - 19:8 scheme [9] - 38:16, 38:24, 39:12, 50:7, shows [1] - 13:14 stake [1] - 55:18 50:8, 50:10, 65:9, 65:12 stand [3] - 10:9, 40:8, 66:10 side [3] - 34:10, 73:2, 73:4 school [1] - 27:12 sides [4] - 3:5, 4:22, 23:3, 72:25 standardized [1] - 57:8 scope [3] - 52:13, 53:1, 53:5 siege [1] - 58:12 standing [2] - 8:6, 71:15 se[1] - 8:19 signed [1] - 56:12 stands [4] - 3:25, 9:23, 42:21, 42:22 search [25] - 5:10, 5:12, 5:14, 5:15, significant [1] - 25:19 start [2] - 5:2, 15:16 5:18, 6:8, 6:10, 7:5, 7:7, 7:10, 9:12, signing [1] - 25:20 started [3] - 3:6, 6:12, 17:13 silence [12] - 14:24, 16:3, 17:19, 18:6. 10:11, 12:16, 12:18, 16:24, 19:20, starting [1] - 4:24 19:21, 29:12, 39:1, 42:17, 54:23, 70:18 18:17, 18:18, 21:4, 21:5, 45:2, 45:3, state [5] - 32:24, 49:10, 55:15, 71:3, Search [1] - 2:11 49.20 71:12 SEARCH [1] - 1:6 silent [1] - 36:19 statements [2] - 14:17, 14:18 searching [1] - 42:25 simple [2] - 9:11, 18:20 states [4] - 10:6, 18:10, 22:4 second [9] - 23:1, 26:3, 30:21, 51:16, simply [6] - 3:20, 16:7, 26:24, 27:15, STATES [2] - 1:1, 1:15 57:19, 66:7, 66:19, 70:13, 72:2 40:1, 44:8 States [10] - 1:10, 1:17, 2:16, 2:18, Second [1] - 35:17 simultaneous [1] - 73:3 3:13, 34:25, 40:17, 45:22, 49:6, 71:13 secret [4] - 9:8, 24:13, 30:22, 64:15 site [1] - 61:20 statue [1] - 53:8 secrets [1] - 64:9 sitting [1] - 67:24 status [3] - 16:15, 17:9, 37:15 Security [1] - 3:24 situation [5] - 21:18, 28:22, 52:1, 54:4, statute [19] - 23:12, 28:2, 30:8, 30:9, security [3] - 4:2, 58:13, 58:21 36:14, 37:2, 37:7, 38:2, 38:8, 38:10, see [6] - 20:21, 26:19, 26:21, 55:24, 38:21, 49:13, 50:4, 50:5, 65:15, 71:1, situations [2] - 26:25, 71:22 61:1, 61:11 71:2, 71:4, 71:6 skip [1] - 24:6 seeing [1] - 20:13 statutes [2] - 19:2, 37:15 skipped [1] - 50:12 seek [6] - 9:9, 12:21, 13:5, 17:14, 55:4, statutory [11] - 15:12, 18:3, 23:14, slice [2] - 35:16, 56:1 slightly [1] - 21:3 31:4, 31:6, 37:5, 38:20, 38:24, 50:6, seeking [8] - 12:21, 18:22, 35:19, 52:2, slipped [1] - 64:19 50:8, 50:10 66:10, 67:5, 67:20, 68:6 stays [1] - 67:21 slowly [1] - 20:2 seeks [2] - 10:21, 15:22 stenography [1] - 2:4 so-called [1] - 17:1 seem [2] - 61:3, 68:3 step [2] - 44:3, 44:8 societal [2] - 65:2, 66:8 seized [1] - 7:4 steps [5] - 55:8, 61:5, 61:11, 61:16, software [11] - 4:7, 4:15, 4:16, 21:12, sell [1] - 66:6 68:2 29:22, 42:3, 42:4, 42:12, 42:21, 67:7 Senate [1] - 22:3 still [12] - 16:3, 17:16, 17:18, 18:2, sold [2] - 41:19, 41:21 18:6, 18:14, 25:19, 30:19, 35:6, 42:14, send [2] - 27:11, 71:25 solved [1] - 68:4 57:18, 60:16 sense [6] - 24:9, 36:11, 37:24, 48:10, someone [1] - 46:6 65:25, 66:2 stipulations [1] - 25:20 somewhat [7] - 3:1, 27:20, 56:8, sensitive [1] - 23:5 stock [1] - 43:14 59:13, 61:23, 65:23, 66:9 sentence [5] - 43:11, 44:2, 44:9, stop [2] - 43:5, 67:6 son [1] - 27:11 44:12, 45:16 stops [2] - 67:5, 68:3 soon [1] - 10:3 separate [6] - 12:22, 18:12, 25:24, store [1] - 32:14 sorry [6] - 28:11, 41:23, 44:11, 54:24, 70:4, 70:6, 70:17 stored [1] - 4:6 60:16, 67:17 separation [3] - 19:7, 19:11, 20:1 stream [1] - 51:10 sort [14] - 8:17, 11:1, 21:12, 23:8, 26:2, September [1] - 3:13 Street [1] - 1:23 28:4, 28:9, 39:20, 48:25, 49:9, 53:24, seriously [1] - 10:7 59:24, 66:2 strip [1] - 17:15 servers [3] - 29:12, 63:25, 69:2 sorts [3] - 12:14, 26:25, 66:22 stripped [1] - 18:2 service [12] - 11:21, 23:7, 23:11, sought [1] - 13:21 struck [2] - 42:6, 65:19 23:15, 28:7, 39:14, 41:12, 48:4, 48:8, sounds [1] - 31:15 struggling [1] - 25:25 53:2, 60:24, 63:12 Southern [2] - 35:5, 55:20 stunning [1] - 9:18 Service [1] - 70:23 speaking [1] - 3:20 subject [4] - 4:3, 4:6, 16:12, 22:6 services [19] - 22:1, 24:12, 40:14, submission [1] - 23:4 speaks [1] - 15:4 41:11, 41:12, 41:14, 50:23, 51:13, specialized [1] - 4:7 submit [2] - 4:22, 55:16 52:10, 53:9, 53:14, 54:21, 57:4, 57:6, subpoena [10] - 29:16, 29:20, 29:21, specific [9] - 7:24, 23:14, 24:17, 30:4, 58:19, 59:1, 65:20, 67:25, 68:21 31:18, 31:22, 31:25, 61:20, 61:22, 32:14, 33:21, 39:6, 43:22, 50:9 set [3] - 51:17, 67:12, 73:1 specifically [2] - 21:24, 31:10 62:16, 64:4 setting [1] - 20:5 specify [2] - 26:23, 27:15 subset [1] - 52:3 settled [2] - 56:8 successfully [1] - 63:8 speculation [1] - 63:3 seven [1] - 12:13 sufficient [3] - 12:25, 32:3, 60:23 spirit [1] - 37:24 several [4] - 14:12, 25:21, 44:25, 55:3 spot [1] - 4:20 sufficiently [4] - 46:5, 67:21, 67:23, share [1] - 12:1 square [1] - 49:24

suggest [1] - 32:21 suggested [1] - 56:2 suggesting [1] - 49:9 suggestion [1] - 10:6 suggestions [1] - 43:1 supplement [2] - 28:19, 68:18 supplemental [1] - 23:4 support [1] - 12:18 suppose [2] - 3:20, 71:23 supposed [1] - 69:21 Supreme [1] - 69:18 surely [1] - 51:23 surprised [2] - 10:14, 34:11 surprising [2] - 9:22, 28:2 surprisingly [1] - 13:3 surveillance [3] - 9:9, 37:20, 51:6 survey [2] - 8:13, 24:16 suspect [1] - 32:15 system [13] - 32:2, 32:3, 32:4, 33:21, 33:25, 40:2, 41:15, 58:14, 60:11, 63:1, 63:24, 64:16, 71:14 systems [2] - 58:15, 58:16

Т

table [1] - 2:22 talks [2] - 40:18, 72:16 tap [4] - 49:13, 50:4, 51:22 tapes [2] - 27:4, 51:6 target [1] - 33:25 task [1] - 37:23 team [2] - 34:21, 34:22 technical [8] - 30:17, 37:18, 62:16, 68:25, 69:7, 70:19, 72:18 technically [2] - 63:21, 63:23 technicians [1] - 4:2 technologies [1] - 33:22 technology [9] - 4:1, 7:2, 19:3, 32:12, 32:13, 33:10, 35:6, 46:13, 72:10 Tel [16] - 26:4, 26:19, 27:20, 27:25, 39:21, 40:13, 43:24, 45:18, 45:22, 47:6, 47:17, 49:5, 49:16, 54:16, 67:22, 71:8 telecom [4] - 21:14, 21:25, 49:12, 49:15 telecommunications [3] - 21:18, 22:4, 23:16 Telephone [8] - 26:24, 27:1, 27:8, 39:17, 43:18, 51:17, 51:20, 69:3 telephone [1] - 4:8 template [1] - 9:7 ten [5] - 7:4, 7:6, 38:18, 42:15, 72:13 tendentious [1] - 11:13 terms [16] - 9:4, 12:6, 15:10, 25:11, 25:25, 30:22, 35:12, 37:7, 37:9, 39:12, 39:20, 40:11, 42:8, 43:22, 57:17, 72:20 Terre [1] - 43:9 test [4] - 26:5, 47:5, 47:6, 71:7 testifies [1] - 33:16 testify [9] - 24:8, 24:10, 24:18, 24:24,

25:2, 25:8, 25:19, 25:23, 31:23 testifying [1] - 63:5 testimony [15] - 3:11, 3:12, 4:11, 15:17, 16:20, 16:21, 25:4, 25:10, 32:2, 32:8, 33:12, 63:4, 72:15, 72:16 text [3] - 37:5, 37:8, 38:8 textbook [1] - 8:5 THE [154] - 1:5, 1:7, 1:14, 2:9, 2:12, 2:19, 2:23, 5:7, 5:12, 5:16, 5:20, 5:23, 6:12, 6:15, 8:15, 9:22, 10:17, 10:25, 11:6, 11:13, 12:8, 12:20, 12:24, 13:22, 14:2, 14:5, 14:9, 14:20, 15:1, 15:8, 15:21, 17:10, 17:23, 18:11, 18:16, 18:24, 19:13, 20:17, 21:3, 21:11, 21:21, 23:1, 23:18, 23:23, 24:3, 24:22, 25:3, 25:11, 25:24, 27:6, 27:18, 28:14, 28:18, 28:20, 28:25, 29:7, 29:15, 29:23, 30:2, 30:9, 30:24, 31:9, 31:13, 32:5, 32:7, 32:17, 33:2, 33:5, 33:9, 33:13, 34:2, 34:8, 34:16, 34:18, 34:22, 35:5, 35:12, 35:16, 36:2, 36:7, 36:16, 37:17, 39:8, 39:11, 40:7, 40:23, 41:7, 41:12, 41:18, 41:25, 42:4, 42:24, 43:22, 44:11, 44:16, 45:2, 45:14, 46:3, 46:9, 46:12, 46:16, 46:19, 46:22, 47:1, 47:10, 47:15, 48:17, 48:21, 50:12, 50:18, 53:1, 53:6, 53:23, 54:8, 54:24, 55:17, 56:10, 57:12, 57:16, 58:3, 59:4, 59:24, 60:5, 60:14, 61:1, 62:12, 62:15, 62:21, 62:24, 63:7, 63:21, 64:3, 64:12, 64:18, 64:21, 65:22, 67:1, 67:11, 67:17, 68:8, 68:11, 68:15, 68:22, 69:17, 70:20, 71:6, 71:15, 71:18, 72:2, 72:15, 72:23, 73:7, 73:10, 73:12 their's [1] - 26:11 theoretically [2] - 46:19, 46:22 theory [2] - 31:17, 31:22 therefore [2] - 20:2, 43:12 therein [1] - 4:3 they've [1] - 56:3 thin [1] - 15:23 thinking [2] - 12:2, 13:8 thinks [1] - 68:1 third [13] - 7:11, 26:24, 27:1, 29:1, 34:23, 37:22, 38:25, 39:13, 39:14, 51:4, 51:8, 63:11, 70:14 third-party [1] - 7:11 thoughts [1] - 4:19 thread [1] - 41:10 three [6] - 16:9, 26:5, 26:12, 41:14, 45:12, 45:19 throughout [1] - 8:22 thwart [6] - 39:22, 39:25, 40:3, 42:16, 45:15, 45:21 thwarting [3] - 43:11, 44:2, 45:17 timeframe [1] - 9:2 Title [5] - 21:20, 22:10, 50:3, 50:4, 67:8 title [1] - 65:14 TO [1] - 1:5 today [3] - 9:17, 53:20, 58:23

top [1] - 20:12 topic [1] - 65:4 topics [1] - 65:4 total [1] - 42:7 touched [1] - 50:21 tough [3] - 45:8, 45:9, 48:9 traction [1] - 16:13 trade [4] - 24:13, 30:22, 64:8, 64:14 transactions [1] - 51:5 TRANSCRIPT [1] - 1:14 transcript [2] - 2:4, 52:14 transcription [1] - 2:4 transfer [3] - 71:3, 71:11, 71:24 transitory [1] - 66:18 transmissions [1] - 52:8 transport [2] - 70:23, 71:16 trial [3] - 7:17, 25:13, 29:20 tried [2] - 3:18, 56:18 trouble [1] - 61:1 troubled [1] - 53:25 true [2] - 42:19, 71:20 trust [7] - 59:5, 59:11, 60:18, 60:24, 61:3, 61:11, 61:14 try [2] - 44:19, 56:3 trying [13] - 26:7, 26:20, 36:16, 38:6, 40:20, 41:7, 45:6, 47:2, 47:5, 48:1, 56:17, 67:12, 72:11 turn [1] - 59:16 turnaround [1] - 7:22 turned [1] - 72:19 turning [2] - 6:8, 40:4 twenty [1] - 24:24 two [19] - 5:14, 6:6, 6:24, 7:19, 9:15, 21:8, 26:2, 26:15, 37:4, 45:10, 50:20, 54:14, 57:6, 61:17, 65:18, 66:1, 68:18, 70:10, 73:5 type [4] - 51:13, 54:22, 64:10, 67:4 types [7] - 52:9, 52:10, 53:13, 57:15, 64:25, 65:13, 69:9

tool [1] - 35:4

U

U.S [1] - 35:5 unable [3] - 3:21, 6:10, 7:2 unanimous [1] - 17:15 unanimously [1] - 18:2 under [29] - 4:13, 17:20, 18:14, 21:8, 26:4, 26:13, 26:22, 27:17, 28:8, 30:2, 30:4, 30:6, 30:10, 31:3, 31:17, 31:22, 35:8, 38:8, 43:12, 43:18, 43:22, 53:5, 53:21, 54:16, 58:12, 66:18, 67:22, 69:14, 70:1 undermine [3] - 18:20, 18:23, 60:24 underscore [1] - 50:22 undue [1] - 20:3 unfortunate [1] - 9:20 unfortunately [1] - 64:19 UNITED [2] - 1:1, 1:15

took [4] - 7:7, 7:8, 16:2, 33:1

warfare [1] - 43:6

14

United [10] - 1:10, 1:17, 2:16, 2:18, 3:13, 34:25, 40:17, 45:22, 49:6, 71:13 unknown [1] - 13:3 unlawful [1] - 28:3 unless [1] - 22:6 unlock [4] - 3:18, 3:21, 4:8, 51:13 unlocked [1] - 4:10 unlocking [1] - 67:6 unnecessary [1] - 19:22 unrealistic [2] - 35:10, 35:13 unreasonable [2] - 19:24, 26:18 unwillingly [1] - 59:25 up [10] - 20:6, 33:17, 50:11, 57:2, 67:17, 69:12, 70:22, 72:4, 72:8, 73:2 update [2] - 20:18, 67:13 updated [1] - 19:14 updating [1] - 9:1 US [2] - 1:21, 11:12 usage [1] - 37:4 usages [3] - 37:18, 37:25, 38:12 useful [1] - 13:2 user [3] - 17:25, 29:6, 42:6 users' [1] - 54:11 uses [2] - 30:18, 32:13 utilities [1] - 23:17

V

valid [4] - 9:12, 10:10, 12:16, 39:1 value [4] - 11:25, 12:1, 12:2, 14:6 values [1] - 13:2 variation [1] - 17:12 variety [4] - 53:9, 58:12, 65:4 various [2] - 27:2, 73:2 vast [1] - 24:6 vector [1] - 58:21 verification [1] - 63:14 Verizon [2] - 21:8, 21:15 version [3] - 4:15, 4:17, 19:14 versus [8] - 27:10, 28:13, 30:2, 30:6, 31:3, 40:17, 45:22, 70:21 video [1] - 27:3 view [2] - 37:7, 65:16 views [4] - 55:16, 56:8, 59:19 vindicate [1] - 56:15 voluntarily [1] - 54:20 voluntary [1] - 57:5 vote [3] - 16:2, 18:8, 18:13 voted [4] - 15:19, 15:25, 16:4, 17:9 voting [1] - 18:4

W

wait [1] - 36:9 waited [1] - 6:19 waiver [3] - 8:17, 8:19, 11:2 walk [2] - 29:21, 30:11 wants [4] - 5:1, 25:13, 53:13, 65:25

Warrant [1] - 2:11 warrant [30] - 5:10, 5:12, 5:15, 5:18, 6:3, 6:5, 6:8, 6:17, 7:5, 7:7, 7:10, 9:12, 10:11, 16:24, 19:20, 19:21, 29:12, 29:17, 31:14, 36:1, 39:1, 40:1, 42:13, 42:17, 42:23, 44:7, 44:13, 54:23, 61:23, 70:18 WARRANT [1] - 1:6 warrants [2] - 5:14, 39:12 Washington [1] - 1:23 ways [2] - 36:16, 54:14 Wednesday [3] - 73:6, 73:7, 73:9 week [2] - 18:13, 18:14 weeks [3] - 6:6, 7:19, 9:15 weight [2] - 55:12, 61:15 welcome [5] - 2:19, 10:12, 23:4, 23:21 whole [1] - 65:7 wider [2] - 53:9 win [1] - 56:3 wipe [5] - 32:17, 32:22, 32:23, 42:18, 72:13 wire [5] - 32:16, 49:13, 50:3, 50:4, 51:21 wiretap [2] - 21:20, 22:10 wiretaps [1] - 22:6 withdraw [1] - 44:20 witness [2] - 29:21, 31:22 wonder [1] - 37:6 wonderful [3] - 11:15, 45:4, 72:25 wondering [1] - 28:6 words [5] - 4:4, 37:4, 60:7, 66:17, 71:18 works [3] - 4:7, 4:13, 56:10 world [1] - 9:4 worried [1] - 66:12 worse [1] - 31:2 worth [1] - 8:20 wrapping [1] - 31:1 writes [1] - 3:24

X

Writs [60] - 15:5, 15:13, 15:22, 16:17,

17:20, 18:14, 19:4, 19:8, 19:9, 20:24,

26:13, 26:17, 26:22, 27:14, 28:1, 28:5,

31:20, 34:14, 35:8, 36:14, 36:17, 36:21,

37:10, 39:3, 43:13, 43:19, 44:21, 45:11,

48:4, 48:11, 49:11, 49:18, 51:14, 53:12,

53:16, 53:22, 57:14, 57:17, 58:24,

60:21, 62:1, 64:4, 64:6, 65:7, 66:13,

66:18, 68:20, 69:7, 69:14, 69:15, 70:1,

28:9, 29:17, 30:3, 30:7, 31:16, 31:18,

XXX [1] - 55:21

70:8, 70:12

writing [1] - 54:3

Υ

year [3] - 3:13, 5:13, 6:3 years [5] - 9:14, 12:13, 20:15, 48:15 YORK [1] - 1:1 York [30] - 1:11, 2:2, 26:4, 26:19, 26:24, 27:1, 27:5, 27:8, 27:10, 27:20, 27:25, 28:13, 28:14, 39:17, 39:21, 40:13, 43:18, 43:24, 45:18, 45:22, 47:6, 47:17, 49:5, 49:16, 51:17, 51:20, 54:16, 67:22, 69:3, 71:8

Ζ

ZwillGen [1] - 1:22 ZWILLINGER [44] - 1:24, 2:20, 10:23, 24:23, 25:6, 25:15, 32:20, 33:4, 50:19, 53:3, 53:7, 54:7, 54:13, 55:10, 56:5, 56:20, 57:13, 58:1, 58:9, 59:13, 60:2, 60:9, 60:19, 61:17, 62:14, 62:19, 62:22, 62:25, 63:10, 63:22, 64:7, 64:13, 64:20, 64:22, 66:19, 67:2, 67:16, 67:19, 68:10, 68:13, 69:11, 69:24, 73:9, 73:11 Zwillinger [1] - 2:21

1	THEODORE J. BOUTROUS JR., SBN 13	32099	
2	tboutrous@gibsondunn.com NICOLA T. HANNA, SBN 130694		
	nhanna@gibsondunn.com		
3	ERIC D. VANDEVELDE, SBN 240699 evandevelde@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP		
4	GIBSON, DUNN & CRUTCHER LLP 333 South Grand Avenue		
5	Los Angeles, CA 90071-3197		
6	Los Angeles, CA 90071-3197 Telephone: 213.229.7000 Facsimile: 213.229.7520		
7	THEODORE B. OLSON, SBN 38137		
8	tolson@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP		
9	1050 Connecticut Avenue, N.W.		
	Washington, DC 20036-5306 Telephone: 202.955.8500		
10	Facsimile: 202.467.0539		
11	MARC J. ZWILLINGER* marc@zwillgen.com		
12	marc@zwillgen.com JEFFFREY G. LANDIS* jeff@zwillgen.com		
13	ZWILLGENTPLLC		
14	1900 M Street N.W., Suite 250 Washington, D.C. 20036		
15	Telephone: 202.706.5202 Facsimile: 202.706.5298		
	*Pro Hac Vice Admission Pending		
16	Attorneys for Apple Inc.		
17	UNITED STATES DISTRICT COURT		
18	CENTRAL DISTRI	ICT OF CALIFORNIA	
19	EASTERN DIVISION		
20	IN THE MATTER OF THE SEARCH	ED No. CM 16-10 (SP)	
21	OF AN APPLE IPHONE SEIZED		
22	DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK	DECLARATION OF LISA OLLE IN SUPPORT OF APPLE INC'S	
23	LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	MOTION TO VACATE ORDER COMPELLING APPLE INC. TO	
24		ASSIST AGENTS IN SEARCH, AND OPPOSITION TO GOVERNMENT'S	
		MOTION TO COMPEL ASSISTANCE	
25		Hearing:	
26		Date: March 22, 2016 Time: 1:00 p.m.	
27		Place: Courtroom 3 or 4 Judge: Hon. Sheri Pym	
28		ton. Shell I jill	

I, Lisa Olle, declare:

- 1. I am over the age of eighteen years and am competent and authorized to make this declaration. I have personal knowledge of the facts set forth below. If called as a witness, I would and could testify to the statements and facts contained herein, all of which are true and accurate to the best of my knowledge and belief.
- 2. I have worked as an attorney at Apple for more than eight years. Prior to Apple, I worked as an attorney at Perkins Coie LLP. My current title is Manager, Global Privacy & Law Enforcement Compliance Team. My responsibilities include overseeing Apple's response to legal requests for customer data that Apple receives from international, federal, state, and local law enforcement agencies.
- 3. I attended University of California, Berkeley, where I obtained a Bachelor of Arts degree in Legal Studies and attended University of California, Boalt Hall School of Law, where I obtained a Juris Doctor.
- 4. I oversaw Apple's response to the legal requests that Apple received related to the December 2, 2015 shooting in San Bernardino, California.
- 5. On Saturday, December 5, 2015, Apple's emergency 24/7 call center received a call at approximately 2:46 a.m. PST requesting information relating to the case. Throughout that day, Apple employees were in regular communication with the FBI regarding its investigation. The same day, Apple received legal process seeking customer or subscriber information regarding three names and nine specific accounts. In response to that request, Apple made two productions of information that same day.
- 6. Throughout the investigation, I and other Apple representatives, including a senior engineer, continually made ourselves available to the government, on a 24/7 basis, participating in teleconferences, providing technical assistance, answering questions from the FBI, and suggesting potential alternatives for the government to attempt to obtain data from the Subject Device.
- 7. On Sunday, December 6, 2015, Apple received a search warrant for information relating to three accounts, including, but not limited to, account

information, emails, and messages, associated with the accounts. In response to that search warrant, Apple provided the government with information in Apple's possession that same day.

- 8. On Wednesday, December 16, 2015, Apple received legal process seeking customer or subscriber information regarding one name and seven specific accounts. In response, Apple provided the government with information in Apple's possession that same day.
- 9. On Friday, January 22, 2016, Apple received a search warrant for the iCloud account related to the Subject Device for the same types of information as in the previous warrant. In response, Apple provided the government with information in Apple's possession on Tuesday, January 26, 2016.
- 10. I have reviewed the Government's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, the Memorandum of Points and Authorities in support of that application, and the Declaration of Christopher Pluhar. I have also reviewed the Court's February 16, 2016 Order Compelling Apple Inc. to Assist Agents in Search and the Government's February 19, 2016 Motion to Compel.
- 11. The Court's February 16, 2016 Order granted Apple the opportunity to present information to the Court regarding the government's request, including the burden of providing the services the government seeks.
- 12. In addition to the technical burden of designing, creating, validating, deploying, and eradicating (or maintaining) an operating system such as the government seeks here, there would be significant additional burdens placed on Apple's law enforcement compliance team.
- 13. Just by way of a few examples, for each device, the law enforcement compliance team would need to arrange to receive, safeguard and deliver the device to the Apple engineers responsible for creating and deploying the operating system. The law enforcement compliance team would also need to preserve and log the chain of custody for the device the entire time it was in Apple's possession. Once the operating

system was created and deployed on the device, someone in the law enforcement compliance group would then need to liaise with the relevant law enforcement agency to create the ability for that agency to submit passcodes to the "hacked" device. Based on past experience, this will likely involve technical escalations where Apple personnel will need to provide law enforcement with technical guidance and assistance regarding how to submit passcodes to the device. Once law enforcement (presumably) gains access to the relevant device, the Apple law enforcement compliance team would then need to transmit any data on the device, and/or the device itself to law enforcement.

- 14. I believe that Apple would likely create one or two secure facilities with security measures akin to a those used in a Sensitive Compartmented Information Facility ("SCIF"), where all work on a device would need to be performed and the device would need to be stored. Access to such facilities would need to be tightly controlled and monitored around the clock.
- 15. Each year Apple complies with thousands of lawful requests for data and information from international, federal, state, and local law enforcement agencies.
- 16. Given my background and experience, I believe that if Apple were required to comply with the order in this case, it would receive similar orders from other law enforcement agencies, and Apple would need to hire people whose sole function would be to assist with processing and effectuating such orders. These people would have no other necessary business or operations function at Apple. They would likely include paralegals, and engineers or forensic specialists who were dedicated full time to preparing for and testifying at trials and hearings. This would be in addition to whatever additional personnel would be necessary to design, create,

Case 5:16-cm-00010-SP Document 16-32 Filed 02/25/16 Page 5 of 5 Page ID #:480

validate, deploy, and eradicate (or maintain and protect) the operating system itself.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 25th day of February 2016 in Sunnyvale, California.

Manager, Global Privacy & Law Enforcement Compliance Team

Apple Inc.

Gibson, Dunn &

1	THEODORE J. BOUTROUS JR., SBN 132099	
2	tboutrous@gibsondunn.com NICOLA T. HANNA, SBN 130694	
	nhanna@gibsondunn.com ERIC D. VANDEVELDE, SBN 240699	
3	evandevelde@gibsondunn.com	
4	evandevelde@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP	
5	333 South Grand Avenue Los Angeles, CA 90071-3197	
6	Los Angeles, CA 90071-3197 Telephone: 213.229.7000 Facsimile: 213.229.7520	
7	THEODORE B. OLSON, SBN 38137	
	tolson@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP	
8	1050 Connecticut Avenue, N.W.	
9	1050 Connecticut Avenue, N.W. Washington, DC 20036-5306 Telephone: 202.955.8500 Facsimile: 202.467.0539	
0	Facsimile: 202.467.0539	
11	MARC J. ZWILLINGER*	
12	marc@zwillgen.com JEFFFREY G. LANDIS*	
13	jeff@zwillgen.com ZWILLGEN PLLC	
	1900 M Street N.W., Suite 250	
14	1900 M Street N.W., Suite 250 Washington, D.C. 20036 Telephone: 202.706.5202 Facsimile: 202.706.5298	
15	Facsimile: 202.706.5298 *Pro Hac Vice Admission Pending	
16	170 The Vice Mainission Fending	
17	Attorneys for Apple Inc.	
18	UNITED STATES DISTRICT COURT	
19	CENTRAL DISTRICT OF CALIFORNIA	
20	EASTERN DIVISION	
21	IN THE MATTER OF THE SEARCH ED No. CM 16-10 (SP)	
22	OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A DECLARATION OF ERIK	
23	SEARCH WARRANT ON A BLACK NEUENSCHWANDER IN SUPPORT	Γ
	LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203 OF APPLE INC'S MOTION TO VACATE ORDER COMPELLING	
24	APPLE INC. TO ASSIST AGENTS IS SEARCH, AND OPPOSITION TO	N
25	GOVERNMENT'S MOTION TO	
26	COMPEL ASSISTANCE	
27	Hearing: Date: March 22, 2016	
28	Time: 1:00 p.m. Place: Courtroom 3 or 4	
	Tidee. Courtoon 5 of 4	

I, Erik Neuenschwander, declare:

- 1. I am over the age of eighteen years and am competent and authorized to make this declaration. I have personal knowledge of the facts set forth below except as to any facts set forth upon information and belief. As to those facts, I believe them to be true. If called as a witness, I would and could testify to the statements and facts contained herein, all of which are true and accurate to the best of my knowledge and belief.
- 2. I have reviewed the Government's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, the Memorandum of Points and Authorities in support of that application, and the Declaration of Christopher Pluhar. I have also reviewed the Court's February 16, 2016 Order Compelling Apple Inc. to Assist Agents in Search and the Government's February 19, 2016 Motion to Compel.
- 3. To the extent Apple Inc. ("Apple") is required to perform the services that the government demands in these documents, I will likely be tasked with planning the project, which would be implemented by multiple engineers and additional Apple personnel across different groups.

Background

4. I have worked for Apple for over eight years, with more than half of that period focused on privacy matters. I am presently Manager of User Privacy. In that role, I am primarily responsible for the privacy design of Apple's products and services. This includes performing ongoing reviews of the privacy impact of various features in, and data collected by, Apple products and services (in coordination with a team of Apple engineers under my supervision), coordinating with Apple's global privacy policy organization and, with the legal department, coordinating outreach and communications with regulators and standards bodies. Prior to becoming User Privacy Manager, my title was Product Security and Privacy Manager, a role I held for four years.

- 5. Prior to joining Apple in 2007, I spent over four years at Microsoft Corporation as a Program Manager.
- 6. I attended Stanford University where I obtained both a Bachelor of Science degree in Symbolic Systems and a Master of Arts degree in Philosophy.

 During the time I was getting my Master of Arts degree, I was also a teaching fellow at Stanford, teaching classes in Computer Science including C++ and Object-Oriented Programming.
- 7. All told, I have spent the majority of the last 13 years focusing on software engineering, with a significant focus on privacy and security dating back more than twenty years.

Overview of Security of Apple's Devices

- 8. In September 2014, Apple announced that iPhones and other devices operating Apple's then-newest operating system, iOS 8, would include hardware- and software-based encryption of the password-protected contents of the devices by default. These protections are designed to prevent anyone without the passcode from accessing stored data on the device.
- 9. When a user sets up an iPhone, the user designates a device passcode, consisting of four, six, or more alphanumeric characters. This passcode is part of the encryption for files with certain classes of protection. The stronger the user passcode is, the stronger the encryption becomes. On iPhones running iOS 8 or newer operating systems, the major types of user data, including messages, photos, contacts, email, notes, and calendar data all are encrypted with keys protected by a key derived from the user-chosen passcode. The end result is a person must know that passcode to read this data.
- 10. To prevent "brute-force" attempts to determine the passcode by submitting multiple guesses in rapid succession, iOS includes a variety of safeguards.
- 11. One of these safeguards is referred to as a "large iteration count." This safeguard functions to slow attempts to unlock an iPhone by increasing the

computational burden of each attempt. The iteration count is calibrated so that one attempt to unlock an iPhone takes approximately 80 milliseconds.

- 12. As another safeguard, Apple imposes time delays, including one which escalates after the entry of invalid passcodes to deter anyone attempting to improperly access a phone by guessing the passcode. After enough consecutive incorrect attempts to enter the passcode, the time delay is set to an infinite value, such that the device will refuse to accept any further passcode entries. There is also a user-configurable setting ("Erase Data") which automatically deletes keys needed to read encrypted data after ten consecutive incorrect attempts. Even when this setting is disabled, however, the infinite delay limits the number of passcode attempts.
- 13. A further safeguard for iOS devices is the creation of a Unique ID ("UID") for every device during fabrication, which is not accessible to the operating system or stored by Apple. When the decryption key for a device is being generated, the user-chosen passcode is entangled with that device's UID. This means that data is protected with a key cryptographically tied to a given device, and consequently iOS is designed to require passcode validation (and therefore any attempted brute-force attack) be performed on the physical device itself.
- 14. Each of the features described above is present in the operating system on the device in question in this matter.

The Government's Request

- 15. As I understand it, the government is demanding that Apple build for the FBI a version of Apple's iPhone operating system that does not currently exist, that Apple would not otherwise build, and that can be used to defeat the above-referenced security measures on Apple devices such as the device at issue here. I will refer to this operating system as GovtOS.
- 16. Specifically, I understand that the government wants GovtOS to (1) bypass or disable the Erase Data function on the device, whether or not it has been enabled; (2) enable the FBI to submit passcodes to the device electronically as opposed

to manually, which is how Apple devices are now designed to accept passcodes; and (3) ensure that when the FBI submits passcodes to the device electronically, software running on the device will not introduce additional time delays between passcode attempts beyond what is incurred by Apple's hardware.

- 17. The government wants GovtOS to load and run from Random Access Memory ("RAM"), and not modify the operating system on the actual phone, the user data partition, or the system partition on the device's flash memory.
- 18. I understand that the government wants Apple to cryptographically sign GovtOS to represent that it is a legitimate Apple product, and then load it onto the device in question so that the government can attempt to brute-force hack the device, either directly or remotely.
- 19. Apple's current iPhone operating systems designed for consumer interaction do not run in RAM, but are installed on the device itself. To make them run in RAM, Apple would have to make substantial reductions in the size and complexity of the code.
- 20. Apple's current consumer operating systems do not allow for electronic input of a passcode.

Creating and Testing the Operating System

- 21. The government is asking Apple to do something that, to my knowledge, Apple has never done before. Accordingly, it is difficult to accurately predict exactly the work such a project would entail and how long it would take.
- 22. I would estimate that the design, creation, validation, and deployment of GovtOS would necessitate between six and ten Apple engineers and employees dedicating a very substantial portion of their time for two weeks at a minimum, and likely as many as four weeks. This includes, in addition to myself, at least two engineers from Apple's core operating system group, a quality assurance engineer, a project manager, and either a document writer or a tool writer (depending on whether Apple is writing the tool to submit passcodes electronically or a protocol so that the

government can do so). This does not include the other personnel who would support those individuals.

- 23. These individuals would otherwise be performing engineering tasks related to Apple's products. New employees could not be hired to perform these tasks, as they would have insufficient knowledge of Apple's software and design protocols to be effective in designing and coding the software without significant training.
- 24. The first step in the process would be for Apple to design and create an operating system that can accomplish what the government wants. No such operating system currently exists with this combination of features. Moreover, Apple cannot simply remove a few lines of code from existing operating systems. Rather, Apple will need to design and implement untested functionality in order to allow the capability to enter passcodes into the device electronically in the manner that the government describes.
- 25. Creating the ability to enter passcodes into a device electronically with no software-imposed delays would entail modifying existing code to remove delays as well as writing new code that manages a connection to another device and, using a communications protocol that would also have to be designed, allows the other device to submit test passcodes and receive and process the result of those tests. The means for establishing such connection could include Wi-Fi, Bluetooth, or direct cable connection.
- 26. Apple will also need to either (1) develop and prepare detailed documentation for the above protocol to enable the FBI to build a brute-force tool that is able to interface with the device to input passcode attempts, or (2) design, develop and prepare documentation for such a tool itself. Further, if the tool is utilized remotely (rather than at a secure Apple facility), Apple will also have to develop procedures to encrypt, validate, and input into the device communications from the FBI.

- 27. After GovtOS is designed and implemented, it will need to be compiled and an installable image will need to be created for the type of device in question. Lastly, it will have to be signed with Apple's cryptographic key verifying that it is Apple-authorized software. Absent Apple's proper cryptographic signature, this device will not load GovtOS.
- 28. Apple would not agree to sign GovtOS voluntarily because it is not software that Apple wants created, deployed or released.
- 29. This entire development process would likely be logged and recorded in case Apple's methodology is ever questioned, for example in court.

Quality Assurance and Security Testing

- 30. Once the operating system is created it will need to go through Apple's quality assurance and security testing process.
- 31. The quality assurance and security testing process is an integral part of the development and deployment of any hardware or software product Apple creates. Apple's ecosystem is incredibly complicated. Changing one feature of an operating system often has ancillary or unanticipated consequences. The potential for such consequences increases with the number of changes to the operating system. Thus, quality assurance and security testing requires that the new operating system be tested and validated before being deployed. The quality assurance and security testing process requires that Apple test GovtOS internally on multiple devices with the exact same hardware features and operating system as the device at issue, in order to ensure that GovtOS functions as required by the government's request.
- 32. Here, quality assurance and security testing will be particularly critical because the FBI-commissioned operating system will need to access the data partition of the device in order to test the passcodes. The data partition is where any user data resides. Because the device at issue contains unique data—any damage or modification to which could be irreversible—Apple will have to undertake additional testing efforts to confirm and validate that running this newly developed operating

system to bypass the device's security features will not inadvertently destroy or alter the user data on the data partition.

- 33. To the extent during the quality assurance and security testing process problems are identified (which is almost always the case), solutions will need to be developed and re-coded into the new operating system. Once such solutions are inputted, the quality assurance and security testing process will begin anew.
- 34. The entire quality assurance and security testing process would also likely be logged, recorded, and preserved in case Apple's methodology is ever questioned, for example in court.

Deploying the Operating System on the Subject Device

- 35. Once the new operating system is created and validated, it will need to be deployed on to the subject device.
- 36. The deployment will need to be done at an Apple facility. That is because GovtOS is not intended to run on any consumer device except with the validation of Apple in circumstances where due process is followed. In addition, simply delivering the operating system to the government would impose upon the government full responsibility for securing it from hackers and others looking to get their hands on it.
- 37. Once GovtOS is created, Apple will need to set up a secure, isolated physical facility where the FBI's passcode testing can be conducted without interfering with the investigation or disrupting Apple's operations. At that facility, the FBI can then connect the device to a computer equipped with the passcode testing tool and conduct its tests for as long as that process takes. At the conclusion of the FBI's testing, whether or not successful, the subject device will need to be restarted so that GovtOS is erased from the device's memory, and Apple can confirm that this sensitive software does not ever leave its facility.
- 38. The deployment steps for a particular device outlined above will require additional time beyond the creation and testing of GovtOS, likely at least a day (not including FBI time spent at Apple's facility testing passcodes).

Destroying or Securing the Operating System

- 39. The government's papers suggest that once deployment of GovtOS is completed and the government (presumably) accesses the device, Apple can simply "destroy" GovtOS.
- 40. The government suggests that this would reduce or eliminate any risk of misuse of the new operating system, including potential use on a device other than the device at issue here. I believe this to be a fundamentally flawed premise.
- 41. The virtual world is not like the physical world. When you destroy something in the physical world, the effort to recreate it is roughly equivalent to the effort required to create it in the first place. When you create something in the virtual world, the process of creating an exact and perfect copy is as easy as a computer key stroke because the underlying code is persistent.
- 42. Even if the underlying computer code is completely eradicated from Apple's servers so as to be irretrievable, the person who created the destroyed code would have spent the time and effort to solve the software design, coding and implementation challenges. This process could be replicated. Thus, GovtOS would not be truly destroyed.
- 43. Moreover, even if Apple were able to truly destroy the actual operating system and the underlying code (which I believe to be an unrealistic proposition), it would presumably need to maintain the records and logs of the processes it used to create, validate, and deploy GovtOS in case Apple's methods ever need to be defended, for example in court. The government, or anyone else, could use such records and logs as a roadmap to recreate Apple's methodology, even if the operating system and underlying code no longer exist.
- 44. All told, I would estimate that the process of designing, creating, validating, deploying GovtOS would take two to four weeks, with additional time spent on eradication (assuming that is possible).

Burden of Repeated Requests

45. Given the complexity of designing, creating, validating, deploying, and eradicating a bespoke operating system such as the government demands, the burden on Apple will increase significantly as the number of requests to Apple increase.

- 46. For example, if Apple receives three orders a week similar to the one here from around the United States, the entire process described above—writing, validating, executing, and then completely destroying the code—will have to happen three times every week, week in and week out. Each such commissioned operating system will need to be tailored to the specific combination of hardware and operating system running on the relevant device.
- 47. The other alternative would be for Apple to maintain custody of GovtOS. Doing that creates an entirely different set of burdens. If a purpose-built operating system such as the one the government seeks here got into the wrong hands it would open a significant new avenue of attack, undermining the security protections that Apple spent years developing to protect its customers.
- 48. Apple would thus need to impose the same level of security protections around GovtOS (as well as the source code used to create it and records and logs document its creation, validation, and deployment) that Apple now employs for its most sensitive trade secrets.
- 49. These measures would need to be maintained for as long as Apple was being required to create and deploy specialized operating systems like those demanded here.

Novelty of the Government's Request

- 50. What the government is requesting Apple do is not something that Apple has ever done before or would otherwise do.
- 51. Apple does not create operating systems the purpose of which is to defeat the security measures Apple specifically designs in to its products.

- 52. Apple does not build be spoke operating systems that are only intended to be installed a single time.
- 53. Apple does not create operating systems built to third-party specifications provided uniquely to Apple.

Alternative Ways of Obtaining Information from the Device

- 54. There are several other ways the government could have potentially obtained any data stored on the subject device.
- 55. I understand that the subject device was provided to the user by his employer, the San Bernardino County Public Health Department ("SBCPHD"), which owned the device.
- 56. The FBI would likely have been able to clear the passcode lock on the device without assistance from Apple had the SBCPHD required that Mobile Device Manager ("MDM") be installed and activated on the device before giving it to their employees.
- 57. MDM is an Apple feature that allows employers to exercise control over devices used by employees, whether those devices are owned by the employer and provided to the employees or are the employees' own devices. Using MDM, employers can wirelessly configure and update settings, monitor policy compliance, deploy apps and books, and remotely wipe or lock managed corporate devices.
- 58. Administrative commands available to employers using MDM include changing configuration settings automatically without user interaction and clearing the passcode lock so users can reset forgotten passwords. Had SBCPHD employed MDM in a way that allowed it do those things, SBCHD could simply clear the passcode lock for the government and/or turn off the Erase Data feature for the government.
- 59. The government may also have been able to obtain the latest data from the device through iCloud backup had the FBI not instructed the SBCPHD to change the iCloud password associated with the account.

- 60. Apple iCloud backs up information—including device settings, app data, photos, videos, and conversations in the Messages app—daily over Wi-Fi. In order for an iCloud backup to occur, however, the backup feature must be enabled, and the device must be locked, connected to a power source, signed into iCloud, and have Wi-Fi access to the Internet.
- 61. Shortly after the shooting, in the course of voluntarily providing the FBI with guidance, Apple recommended to the FBI that that the device be connected to a known Wi-Fi network, such as one at the subject's home or at the SBCPHD, and plugged into a power source so it could potentially create a new iCloud backup automatically. If successful, that backup might have contained information between the last backup and the date of the shooting.

Process of Writing Code

- 62. I have been writing computer code for thirty years.
- 63. I started out writing IBM Advanced BASIC.
- 64. In my experience, different people approach writing code in different ways. Some people write a complete design before starting to code. Others start with the code and write it from start to finish. Still others begin with a sketch of what they want to make, which can be a list of features or an actual physical picture.
- 65. Writing code is an exceedingly creative and expressive process, requiring a choice of language (*e.g.*, C, C++, Objective-C, Swift, Javascript, Python, Perl, PHP, etc.), a choice of audience (both in terms of the targeted technology platforms and types of end users), a choice of syntax and vocabulary (*e.g.*, variable names, function names, class definitions, etc.), the creation of complex data structures, algorithms to manipulate and transform data, detailed textual descriptions to help explain what the code is doing (*i.e.*, what are called "comments" to code), methods of communicating information to the user (*e.g.*, through words, icons, pictures, sounds, etc.) and receiving and responding to user input—all expressed through human-readable, expressive (and functional) written work product.

66. There are a number of ways to write code to accomplish a given task, some more efficient and more elegant, than others. Moreover, writing software is an iterative, revision intensive, and mentally challenging task, just like writing essays, whitepapers, memos, and even poems.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 25th day of February 2016 in Redwood City, California.

Erik Neuenschwander Manager of User Privacy

1	THEODORE J. BOUTROUS JR., SBN 132099	
2	tboutrous@gibsondunn.com NICOLA T. HANNA, SBN 130694	
3	nhanna(<i>a</i>)g1bsondunn.com	
	ERIC D. VANDEVELDE, SBN 240699 evandevelde@gibsondunn.com	
4	GIBSON, DUNN & CRUTCHER LLP 333 South Grand Avenue	
5	Los Angeles, CA 90071-3197 Telephone: 213.229.7000 Facsimile: 213.229.7520	
6	Facsimile: 213.229.7520	
7	THEODORE B. OLSON, SBN 38137	
8	tolson@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP	
9	1050 Connecticut Avenue, N.W. Washington, DC 20036-5306	
10	Washington, DC 20036-5306 Telephone: 202.955.8500 Facsimile: 202.467.0539	
11	MARC J. ZWILLINGER*	
12	marc@zwillgen.com JEFFREY G. LANDIS*	
13	jeff@zwillgen.com ZWILLGEN PLLC	
14	1900 M Street N.W., Suite 250 Washington D.C. 20036	
15	Washington, D.C. 20036 Telephone: 202.706.5202 Facsimile: 202.706.5298	
	*Pro Hac Vice Admission Pending	
16		
17		
18	UNITED STATES	S DISTRICT COURT
19	CENTRAL DISTRICT OF CALIFORNIA	
20	EASTER	N DIVISION
21	IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED	ED No. CM 16-10 (SP)
22	DURING THE EXECUTION OF A	[PROPOSED] ORDER GRANTING APPLE INC.'S MOTION TO VACATE
23	SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA	AND DENYING GOVERNMENT'S
24	LICENSE PLÁTE 35KGD203	MOTION TO COMPEL
25		Hearing: Date: March 22, 2016
26		Time: 1:00 p.m. Place: Courtroom 3 or 4
27		Judge: Hon. Sheri Pym
28		

1	On February 16, 2016, upon <i>ex parte</i> application by the government, the Court		
2	issued an Order Compelling Apple to Assist Agents in Search (Case No. ED 15-		
3	0451M, Dkt. 19).		
4	This matter is before the Court on Apple Inc.'s Motion to Vacate Order		
5	Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's		
6	Motion to Compel Assistance ("Motion to Vacate"), and the government's Motion to		
7	Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling		
8	Assistance in Search ("Motion to Compel").		
9	Having considered the files and records in the case, the parties' papers in		
10	support of and opposition to the Motion to Vacate and the Motion to Compel, the		
11	accompanying declarations and exhibits, and the parties' argument at the hearing on		
12	this matter, the Court hereby GRANTS Apple's Motion to Vacate and DENIES the		
13	government's Motion to Compel.		
14			
15	IT IS SO ORDERED.		
16			
17	Dated:, 2016		
18			
19	Honorabla Chari Dum		
20	Honorable Sheri Pym United States Magistrate Judge		
21			
22			
23			
24			
25			
26			
27			
28			