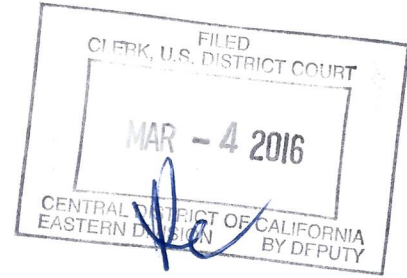


ORIGINAL



1 MAYER BROWN LLP  
2 John Nadolenco (SBN 181128)  
3 jnadolenco@mayerbrown.com  
4 RUTH ZADIKANY (SBN 260288)  
5 rzadikany@mayerbrown.com  
350 South Grand Avenue, 25th Floor  
Los Angeles, California 90071-1503  
Telephone: (213) 229-9500  
Facsimile: (213) 625-0248

6 ANDREW J. PINCUS (*pro hac vice application forthcoming*)  
7 apincus@mayerbrown.com  
8 TRAVIS CRUM (*pro hac vice application forthcoming*)  
9 tcrum@mayerbrown.com  
10 1999 K Street, N.W.  
Washington D.C. 20006-1001  
Telephone: (202) 263-3328  
Facsimile: (202) 263-5328

11 Attorneys for *Amici Curiae* BSA|The Software Alliance, the  
Consumer Technology Association, the Information  
Technology Industry Council, and TechNet

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

12 IN THE MATTER OF THE SEARCH  
13 OF AN APPLE IPHONE SEIZED  
14 DURING THE EXECUTION OF A  
15 SEARCH WARRANT ON A BLACK  
16 LEXUS IS300, CALIFORNIA  
17 LICENSE PLATE 35KGD203

Case No. 5:16-cm-00010-SP

[PROPOSED] ORDER GRANTING  
THE APPLICATION OF BSA|THE  
SOFTWARE ALLIANCE, THE  
CONSUMER TECHNOLOGY  
ASSOCIATION, THE  
INFORMATION TECHNOLOGY  
COUNCIL, AND TECHNET LEAVE  
TO FILE A BRIEF OF *AMICI  
CURIAE*

Hearing Date: March 22, 2016

Time: 1:00 p.m.

Location: Courtroom of the Hon. Sheri  
Pym

LOGGED

2016 MAR 19 PM 2:31

U.S. DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA  
RIVERSIDE

26  
27  
28

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  
28

**ORDER**

The Court, having considered the papers filed in support of the Application of BSA|The Software Alliance, the Consumer Technology Association, the Information Technology Industry Council, and TechNet for Leave to File Brief of *Amici Curiae* hereby **ORDERS** as follow:

The Application of BSA|The Software Alliance, The Consumer Technology Association, The Information Technology Industry Council, And TechNet for Leave to File Brief of *Amici Curiae* in the above-referenced action is hereby **GRANTED.**

**IT IS SO ORDERED**

Dated: March 4, 2016



---

Honorable Sheri Pym  
United States Magistrate

**PROOF OF SERVICE**

I, Janice Austgen, declare:

I am employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Mayer Brown LLP, 350 South Grand Avenue, 25th Floor, Los Angeles, California 90071-1503. On March 3, 2016, I served a copy of the within document(s):

[PROPOSED] ORDER GRANTING THE APPLICATION OF BSA|THE SOFTWARE ALLIANCE, THE CONSUMER TECHNOLOGY ASSOCIATION, THE INFORMATION TECHNOLOGY COUNCIL, AND TECHNET TO FILE A BRIEF OF *AMICI CURIAE*

X by placing the document(s) listed above in a sealed UPS envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a UPS agent for delivery.

SEE ATTACHED SERVICE LIST

I declare under penalty of perjury under the laws of the United States of America that the above is true and correct.

Executed on March 3, 2016, at Los Angeles, California.

  
\_\_\_\_\_  
Janice Austgen

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  
28

1 Eric David Vandavelde, Esq.  
2 Theodore J. Boutrous, Jr., Esq.  
3 Gibson Dunn and Crutcher LLP  
4 333 South Grand Avenue  
5 Los Angeles, CA 90071

6 Jeffrey G. Landis, Esq.  
7 Marc J Zwillinger, Esq.  
8 Zwillgen PLLC  
9 1900 M Street NW Suite 250  
10 Washington, DC 20036

11 Nicola T. Hanna, Esq.  
12 Gibson Dunn and Crutcher LLP  
13 3161 Michelson Drive 12th Floor  
14 Irvine, CA 92612-4412

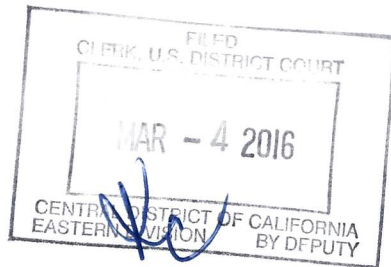
15 Theodore B. Olson, Esq.  
16 Gibson Dunn and Crutcher LLP  
17 1050 Connecticut Avenue NW  
18 Washington, DC 20036-5306

19 Allen W. Chiu, Esq.  
20 Assistant United States Attorney  
21 Office of U.S. Attorney  
22 National Security Section  
23 312 North Spring Street Suite 1300  
24 Los Angeles, CA 90012

25 Tracy L. Wilkison, Esq.  
26 Assistant United States Attorney  
27 Office of U.S. Attorney  
28 Chief, Cyber and Intellectual Property Crimes Section  
312 North Spring Street 11th Floor  
Los Angeles, CA 90012-4700



ORIGINAL



1 MAYER BROWN LLP  
2 JOHN NADOLENCO (SBN 181128)  
3 jnadolenco@mayerbrown.com  
4 RUTH ZADIKANY (SBN 260288)  
5 rzadikany@mayerbrown.com  
6 350 South Grand Avenue, 25th Floor  
7 Los Angeles, California 90071-1503  
8 Telephone: (213) 229-9500  
9 Facsimile: (213) 625-0248

10 ANDREW J. PINCUS (*pro hac vice application forthcoming*)  
11 apincus@mayerbrown.com  
12 TRAVIS CRUM (*pro hac vice application forthcoming*)  
13 tcrum@mayerbrown.com  
14 1999 K Street, N.W.  
15 Washington D.C. 20006-1001  
16 Telephone: (202) 263-3328  
17 Facsimile: (202) 263-5328

18 Attorneys for *Amici Curiae* BSA|The Software Alliance, the  
19 Consumer Technology Association, the Information  
20 Technology Industry Council, and TechNet

21 UNITED STATES DISTRICT COURT

22 CENTRAL DISTRICT OF CALIFORNIA, EASTERN DIVISION

23 IN THE MATTER OF THE SEARCH  
24 OF AN APPLE IPHONE SEIZED  
25 DURING THE EXECUTION OF A  
26 SEARCH WARRANT ON A BLACK  
27 LEXUS IS300, CALIFORNIA  
28 LICENSE PLATE 35KGD203

Case No. 5:16-cm-00010-SP

Brief of BSA|The Software Alliance,  
the Consumer Technology Association,  
the Information Technology Industry  
Council, and TechNet As *Amici Curiae*  
In Support Of Apple's Motion To  
Vacate And In Opposition To The  
Motion To Compel Assistance

Hearing Date: March 22, 2016

Time: 1:00 p.m.

Location: Courtroom of the Hon. Sheri  
Pym

LOGGED

2016 MAR -3 PM 2:32  
CLERK U.S. DISTRICT COURT  
CENTRAL DIST. OF CALIF.  
RIVERSIDE

TABLE OF CONTENTS

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  
28

	<b>Page</b>
TABLE OF AUTHORITIES .....	ii
INTEREST OF <i>AMICI CURIAE</i> .....	1
INTRODUCTION AND SUMMARY OF THE ARGUMENT .....	2
ARGUMENT .....	3
A COURT MAY INVOKE THE ALL WRITS ACT TO COMPEL A THIRD PARTY TO TURN OVER OR PROVIDE ACCESS TO EXISTING INFORMATION THE THIRD PARTY POSSESSES, BUT MAY NOT ORDER A THIRD PARTY TO INVENT A NEW PRODUCT— PARTICULARLY WHEN THE GOVERNMENT’S DEMAND WOULD CREATE SECURITY RISKS AND EFFECTIVELY DICTATE PRODUCT DESIGN .....	3
A. Precedent Prohibits The Order Sought By The Government.....	5
B. The Government’s Expansive Interpretation Of The Act Has No Limiting Principle. ....	12
C. When Congress Intends To Authorize Government Conscription Of Private Parties, It Does So Expressly.....	15
D. The Likely Practical Result of The Government’s Position Will Be De Facto Government-Mandated Design Specifications.....	17
CONCLUSION .....	19

**TABLE OF AUTHORITIES**

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  
28

**Page(s)**

**CASES**

*In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities*, 616 F.2d 1122 (9th Cir. 1980) .....4

*In re Application of United States for an Order Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003) (unpublished) .....4

*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 (S.D.N.Y. Oct. 31, 2014).....5

*In re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court*, No. 15 MC 1902 (E.D.N.Y. Feb. 29, 2016) .....5

*Pennsylvania Bur. of Corr. v. U.S. Marshals*, 474 U.S. 34 (1985).....16

*Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283 (9th Cir. 1979) ..... *passim*

*Riley v. California*, 134 S. Ct. 2473 (2014) .....8

*United States v. Hall*, 583 F. Supp. 717 (E.D. Va. 1984) .....4

*United States v. Jones*, 132 S. Ct. 945 (2012).....18

*United States v. Navarro*, No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013) .....5

*United States v. New York Telephone Co.*, 434 U.S. 159 (1977).....4, 6, 7

*Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579 (1952) .....17

**STATUTES**

28 U.S.C. § 1651(a).....4

47 U.S.C. § 1001 .....15, 16

1 47 U.S.C. § 1002 .....16, 17

2 50 U.S.C. § 4501.....15

3 50 U.S.C. § 4511 .....15

4 50 U.S.C. § 4514(a).....15

5 50 U.S.C. § 4552 .....15

6 50 U.S.C. § 4564.....15

7

8 **OTHER AUTHORITIES**

9 Berkman Center for Internet & Society at Harvard University, *Don't*  
 10 *Panic: Making Progress on the "Going Dark" Debate* (2016).....10

11 Brian Bennett, *FBI Director Calls Apple Case 'Hardest Question' In*  
 12 *Government*, L.A. Times (Feb. 25, 2016).....2

13 Charles Babcock, *NSA's Prism Could Cost U.S. Cloud Computing*  
 14 *Companies \$45 Billion*, InformationWeek (Feb. 25, 2016), .....11

15 Gerry Smith, *'Snowden Effect' Threatens U.S. Tech Industry's Global*  
 16 *Ambitions*, Huffington Post (Jan. 24, 2014).....10, 11

17 James B. Comey, *Statement Before the Senate Comm. On Homeland*  
 18 *Sec. & Governmental Affairs*, Hearing Before the Senate Comm.  
 19 *On Homeland Sec. & Governmental Affairs* (Oct. 8, 2015).....16

20 Lee Rainie & Shiva Maniam, *Americans Feel the Tensions between*  
 21 *Privacy and Security Concerns*, Feb. 19, 2016 .....9, 10

22 Letter from Sen. Charles E. Grassley to Sally Q. Yates, Deputy Att'y  
 23 Gen., and James B. Comey, Jr., Dir., Fed. Bureau of Investigation  
 24 (Feb. 16, 2016) .....16

25 Mary Madden, *Public Perceptions of Privacy and Security in the*  
 26 *Post-Snowden Era*, Pew Research Center (Nov. 12, 2014).....10

27 Matt Apuzzo & Katie Benner, *Apple Is Said To Be Trying To Make It*  
 28 *Harder To Hack iPhone*, N.Y. Times (Feb. 24, 2016).....18

McCConnell et al., *Why The Fear Over Ubiquitous Data Encryption Is*  
*Overblown*, Wash. Post (July 28, 2015) .....17

1 Rebecca Riffkin, *Hacking Tops List of Crimes Americans Worry*  
2 *About Most*, Gallup (Oct. 27, 2014).....10  
3  
4 Sally Quillian Yates and James B. Comey, Jr., *Going Dark:*  
5 *Encryption, Technology, and the Balances Between Public Safety*  
6 *and Encryption*, Hearing before the S. Judiciary Comm. (July 8,  
7 2015) .....16  
8  
9 Susan Landau, *The Encryption Tightrope: Balancing Americans’*  
10 *Security and Privacy*, Hearing before the House Judiciary Comm.,  
11 (Mar. 1, 2016) .....14, 15  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



**INTEREST OF AMICI CURIAE**

1  
2        *Amici* are associations whose members comprise all of the companies that  
3 are leaders in the global technology industry. Because the Court’s decision in this  
4 case could have significant effects on the security of the products created by  
5 *amici*’s members, and on the development of new hardware and software products,  
6 *amici* have a substantial interest in this proceeding.

7        BSA | The Software Alliance is an association of the world’s leading  
8 software and hardware technology companies. BSA promotes policies that foster  
9 innovation, growth, and a competitive marketplace for commercial software and  
10 related technologies.

11        The Consumer Technology Association (CTA), formerly Consumer  
12 Electronics Association (CEA), is a trade association representing the \$287 billion  
13 U.S. consumer electronics industry. CTA also owns and produces CES—the  
14 world’s gathering place for all who thrive on the business of consumer technology.

15        The Information Technology Industry Council (ITI) is the global voice of  
16 the technology sector. As an advocacy and policy organization for the world’s  
17 leading innovation companies, ITI navigates the relationships between  
18 policymakers, companies, and non-governmental organizations, providing creative  
19 solutions that advance the development and use of technology around the world.

20        TechNet is an association of chief executive officers and senior executives  
21 of the Nation’s leading technology companies across the country. TechNet’s  
22 objective is to promote the growth of the technology industry and to advance  
23 America’s global leadership in innovation. Its members are in the fields of  
24 information technology, biotechnology, clean technology, venture capital, e-  
25 commerce, and finance, and represent more than two million employees.



1 whether in our constitutional democracy specific congressional authorization  
2 should be required before courts may determine on an ad hoc basis that a private  
3 individual or company should be forced to assist in government investigations. The  
4 Court accordingly should vacate the order on the ground that it exceeds the  
5 authority conferred by the All Writs Act.

6 Controlling circuit precedent confirms that a company cannot be compelled  
7 to develop a new product—here, new software that does not now exist—  
8 particularly when it will create security risks for all users of the company’s  
9 products. The government’s argument, moreover, has no limiting principle: any  
10 third party could be conscripted to produce new software that would allow the  
11 government to breach security measures. Congress could not have intended that  
12 result when it enacted the All Writs Act in 1789—indeed, when Congress has  
13 authorized conscription of unwilling private parties it has spoken clearly, and  
14 provided specific standards to govern the imposition of such obligations. Finally,  
15 the predictable result of upholding the government’s position will be to force  
16 companies to change the design specifications they might otherwise utilize in  
17 response to the risk that they might be subject to an order such as the one sought  
18 here. A decision with such significant public policy consequences should be made  
19 by the People acting through the political branches—not through the issuance of an  
20 order by this Court.

### 21 ARGUMENT

22 **A Court May Invoke The All Writs Act To Compel A Third Party To**  
23 **Turn Over Or Provide Access To Existing Information The Third Party**  
24 **Possesses, But May Not Order A Third Party To Invent A New**  
25 **Product—Particularly When The Government’s Demand Would Create**  
**Security Risks And Effectively Dictate Product Design.**

26 The general language of the All Writs Act “is not a grant of plenary power to  
27 federal courts.” *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir.  
28

1 1979).<sup>1</sup> In the context here—requiring a third party to assist in a government  
2 investigation—the Act has been invoked in three basic situations:

- 3 • Requiring the third party to turn over information in its possession that the  
4 government has a lawful right to obtain. *See, e.g., United States v. Hall*, 583  
5 F. Supp. 717 (E.D. Va. 1984) (compelling credit card company to turn over  
6 records in its possession); *In re Application of United States for an Order*  
7 *Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL  
8 22053105 (D. Md. Aug. 22, 2003) (unpublished) (directing landlord to turn  
9 over security footage in its possession).
- 10 • Compelling the third party to turn over a password possessed by the third  
11 party that is needed to obtain access to information covered by the  
12 underlying warrant or other legal process.
- 13 • When the information that the government has a legal right to obtain is  
14 possessed by the third party as a result of a government-conferred  
15 monopoly, obligating the third party to enable the government to obtain  
16 access to that information. *United States v. New York Telephone Co.*, 434  
17 U.S. 159 (1977); *In re Application of the United States for an Order*  
18 *Authorizing an In-Progress Trace of Wire Communications Over Telephone*  
19 *Facilities*, 616 F.2d 1122 (9th Cir. 1980).

20 All of the cases cited by the government that involve process directed at third  
21 parties, other than two recent ruling involving the factual situation presented here,  
22 fall into these categories.

23 The government's request here is dramatically different in kind. The  
24 government has possession of the device containing the information at issue. Apple  
25

---

26 <sup>1</sup> The Act provides: "The Supreme Court and all courts established by Act of  
27 Congress may issue all writs necessary or appropriate in aid of their respective  
28 jurisdictions and agreeable to the usages and principles of law." 28 U.S.C.  
§ 1651(a).

1 does not have the password that would unlock the device. The government instead  
2 would require Apple to create a new product, a new software “tool,” meeting the  
3 list of requirements specified by the government. That demand bears no  
4 resemblance to the three situations in which process has previously been  
5 authorized under the All Writs Act.

6 The government cites two district court decisions—one issued *ex parte* and  
7 one without any analysis—that endorse its position.<sup>2</sup> Another court recently  
8 rejected the government’s position in a lengthy opinion. *See In re Order Requiring*  
9 *Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court,*  
10 No. 15 MC 1902 (E.D.N.Y. Feb. 29, 2016), Doc. 29.

11 This Court should hold that the government’s request falls outside the  
12 authority conferred by the All Writs Act.

13 **A. Precedent Prohibits The Order Sought By The Government.**

14 The government is unable to point to a single authoritative precedent in  
15 support of its extraordinarily expansive construction of the Act. Its argument must  
16 be rejected for two reasons. First, the Act simply does not reach beyond the three  
17 situations in which it has routinely been applied. Second, even if the Act *could*  
18 extend more broadly, it cannot apply in the circumstances presented here.

19 1. The Ninth Circuit’s rejection in *Plum Creek* of a similarly unprecedented  
20 application of the All Writs Act demonstrates the flaws in the government’s  
21 analysis here.

22 That case arose in the context of an investigation by the Occupational Safety  
23 and Health Administration (OSHA) of a lumber yard explosion. During its  
24 investigation, OSHA requested that the lumber yard’s employees wear noise-

---

25 <sup>2</sup> See Apple Mem. in Support of Motion to Vacate at 28 (discussing *United States*  
26 *v. Navarro*, No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013), ECF No. 39; *In re*  
27 *Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued*  
28 *by This Court by Unlocking a Cellphone*, 2014 WL 5510865, at \*2 (S.D.N.Y. Oct.  
31, 2014).



1 measuring devices and air containment sampling devices. The company had a  
2 policy barring its employees from wearing such devices, claiming, in relevant part,  
3 that the devices were “dangerous because they could distract employees or cause  
4 them to become entangled in moving equipment.” 608 F.2d at 1286. OSHA sought  
5 an order pursuant to the All Writs Act compelling the company to allow its  
6 employees to wear the devices.

7 The Ninth Circuit held that the Act did not authorize OSHA’s proposed  
8 order—even though the lumber company was the target of the investigation. The  
9 Court relied on a number of factors in concluding that

10 although the use of the personal noise-level and air-  
11 contaminant measuring devices is a reasonable means of  
12 inspecting, there is no statutory or inherent authority in  
13 the district court to order Plum Creek to rescind its policy  
forbidding its employees to wear the OSHA devices.

14 608 F.2d at 1290. The Ninth Circuit held that the All Writs Act “does not authorize  
15 a court to order a party to bear risks not otherwise demanded by law.” *Id.* at 1289-  
16 1290.<sup>3</sup>

17 The Ninth Circuit thus refused to impose upon a private party a duty not  
18 otherwise required by law—a duty that required the creation of information, rather  
19 than merely providing the government with existing information in the possession  
20 of the private party. The court of appeals’ reasoning requires rejection of the  
21 government’s request here. *Cf. New York Telephone*, 434 U.S. at 174 (concluding  
22 that, because telephone monopoly’s own facilities were “being employed to  
23 facilitate a criminal enterprise on a continuing basis,” the company was not “so far  
24 removed from the underlying controversy that its assistance could not permissibly

---

25  
26 <sup>3</sup> The Ninth Circuit also noted that OSHA had less-effective alternative means of  
27 conducting its investigation of Plum Creek, but it did not state that the result would  
28 have been different if those alternatives did not exist. *See Plum Creek Lumber Co.*,  
608 F.2d at 1289.

1 be compelled”).

2 The court of appeals’ conclusion about the limited scope of the All Writs  
3 Act makes sense for an additional reason: a contrary result would embroil the  
4 courts in wholly unguided assessments of the consequences to a third party of  
5 compelling it to perform the tasks demanded by the government. Different courts  
6 could reach different conclusions on that question, but those different results could  
7 have very significant consequences for the security of data held by those  
8 companies—which would be particularly unfair if, as is likely, the companies were  
9 marketplace competitors.

10 Moreover, such ad hoc determinations would leave businesses and other  
11 private parties with no certainty about their potential legal obligations. Businesses  
12 would be unable to anticipate government demands that might be asserted, or how  
13 such demands would be resolved by the courts.

14 2. Even if the Act could in some circumstances extend beyond situations in  
15 which the government seeks disclosure of or access to existing information in the  
16 possession of a third party, an order would be impermissible here.

17 Courts have limited the conscription of third parties under the Act to  
18 situations in which the government’s demand would not subject the third party to  
19 an unreasonable burden. *New York Telephone Co.*, 434 U.S. at 172  
20 (“[U]nreasonable burdens may not be imposed.”); *id.* at 175 (“Nor was the District  
21 Court’s order in any way burdensome. The order provided that the Company be  
22 fully reimbursed at prevailing rates, and compliance with it required minimal effort  
23 on the part of the Company and no disruption to its operations.”); *Plum Creek*  
24 *Lumber Co.*, 608 F.2d at 1289-90 (“[The All Writs Act] does not authorize a court  
25 to order a party to bear risks not otherwise demanded by law.”).

26 The order here would impose very substantial burdens and risks on Apple  
27 and its customers.

28 *First*, the government’s order would create a very real security risk for the

1 millions of Apple products with the same operating system as the iPhone involved  
2 here. That imposes a substantial burden on Apple's customers and on Apple.

3 The Supreme Court recently explained in detail the intensely personal nature  
4 of the information contained on these devices:

5 First, a cell phone collects in one place many distinct  
6 types of information—an address, a note, a prescription,  
7 a bank statement, a video—that reveal much more in  
8 combination than any isolated record. Second, a cell  
9 phone's capacity allows even just one type of  
10 information to convey far more than previously possible.  
11 *The sum of an individual's private life can be*  
12 *reconstructed* through a thousand photographs labeled  
13 with dates, locations, and descriptions . . . . Third, the  
14 data on a phone can date back to the purchase of the  
15 phone, or even earlier. . . . Finally, there is an element of  
16 pervasiveness that characterizes [information contained  
17 in] cell phones.

18 *Riley v. California*, 134 S. Ct. 2473, 2489-90 (2014) (emphasis added).

19 Apparently recognizing the deeply private nature of the data contained on  
20 these devices, and the security risks inherent in circumventing encryption software,  
21 the government argues that there is no danger here because the software that Apple  
22 would be compelled to create would be used only for this one phone—and could  
23 be retained in Apple's possession and then destroyed. That is an unrealistic picture  
24 of the consequences of upholding the government's demand.

25 To begin with, the government itself has made clear that this is not a one-off  
26 request. The Department of Justice has asserted multiple demands for the creation  
27 of this software, and other law enforcement officials have indicated that they too  
28 would utilize the Act or state equivalents to impose the same obligation. *See* Apple  
Mem. In Support of Motion to Vacate at 3. It would hardly make sense for a  
company faced with multiple demands to continuously create and destroy the  
software.

1           Once software is created to circumvent the device's security protections—  
2 both the password-protection feature and the “auto erase” function after ten  
3 incorrect entries—that software could fall into the wrong hands: it could be stolen  
4 by hackers or by a government intelligence agency. *See* Apple Mem. In Support of  
5 Motion to Vacate at 5-8.

6           Moreover, there is a significant risk that multiple uses of such government-  
7 specified software will inevitably lead to public disclosure of information that  
8 would enable hackers (whether private or sponsored by foreign governments) to  
9 produce their own hacking tool. If, for example, the software resulted in access to  
10 evidence that federal or state authorities sought to introduce in a criminal  
11 proceeding, the Apple engineers who created the government-mandated software  
12 could be required to testify about how the software tool worked and to provide  
13 assurance that it merely provided access to, and did not in any way alter, the  
14 information contained on the device in question. That testimony, in turn, could  
15 provide hackers with a roadmap to create their own tool for invading the contents  
16 of the device. *Cf.* Apple Mem. In Support of Motion to Vacate 24-25. The only  
17 effective way to prevent this software from falling into the wrong hands is to  
18 abstain from creating it in the first place.

19           In sum, the significant security risks to all device users that would result  
20 from creation of the software demanded by the government is an unreasonable  
21 burden under the *New York Telephone* standard that bars issuance of the order.

22           *Second*, the government's order would force a company to breach its  
23 assurances to its customers about the security of their information, possibly  
24 subjecting it to liability as well as harm in the marketplace.

25           Customers are intensely concerned about maintaining control over their most  
26 intimate and personal information. “[P]eople now are more anxious about the  
27 security of their personal data and are more aware that greater and greater volumes  
28 of data are being collected about them.” Zadikany Decl. Ex. B [Lee Rainie & Shiva

1 Maniam, *Americans Feel the Tensions between Privacy and Security Concerns*,  
2 Pew Research Center (Feb. 19, 2016)]. Eighty percent of adults “agree” or  
3 “strongly agree” that Americans should be concerned about the government’s  
4 monitoring of phone calls and internet communications. Zadikany Decl. Ex. C  
5 [Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden*  
6 *Era*, Pew Research Center (Nov. 12, 2014)].

7 These concerns have been heightened by the revelations by Edward  
8 Snowden about U.S. government access to personal information. Consumers are  
9 also very sensitive to and concerned by the threats to security of their private  
10 information posed by an array of criminals and bad actors, including hackers,  
11 fraudsters, and identity thieves. *See* Zadikany Decl. Ex. D [Rebecca Riffkin,  
12 *Hacking Tops List of Crimes Americans Worry About Most*, Gallup (Oct. 27,  
13 2014)].

14 Many technology companies have announced changes to their operating  
15 systems specifically designed to provide customers with greater security for their  
16 personal information. *See, e.g.*, Hanna Decl. Ex. M [Berkman Center for Internet &  
17 Society at Harvard University, *Don’t Panic: Making Progress on the “Going*  
18 *Dark” Debate*, at 3-4 (2016)].

19 The order sought by the government would force Apple to undermine the  
20 hard-earned trust of its customers. That will subject the company to substantial  
21 reputational and marketplace injury, leading customers to lose confidence in the  
22 company’s willingness to protect their security and seek trustworthy alternatives  
23 that provide greater protection.

24 These harms could be particularly pronounced in other nations where  
25 protection of personal information in general, and distrust of the U.S. government  
26 in particular, is highly relevant in the marketplace. Indeed, some U.S. technology  
27 companies suffered substantial economic and reputational harm in the wake of the  
28 revelations about U.S. government access to personal information. *See* Zadikany



1 Decl. Ex. E [Gerry Smith, *'Snowden Effect' Threatens U.S. Tech Industry's Global*  
2 *Ambitions*, Huffington Post (Jan. 24, 2014)] (noting that in the wake of Snowden's  
3 revelations, approximately ten percent of non-U.S. companies cancelled contracts  
4 with U.S. companies out of fear of NSA surveillance).

5 Foreign competitors in particular would argue that devices or software  
6 created by U.S. companies are less secure because of the risk that the U.S.  
7 government would demand creation of a "tool" to enable access to personal  
8 information—and that customers should therefore purchase only from non-U.S.  
9 technology companies. This is not speculation: these very arguments were  
10 advanced in the wake of the Snowden revelations. *See* Zadikany Decl. Ex. F  
11 [Charles Babcock, *NSA's Prism Could Cost U.S. Cloud Companies \$45 Billion*,  
12 *InformationWeek* (Aug. 14, 2013)] (Neelie Kroes—at the time, the European  
13 Commissioner for Digital Affairs—observed: "If European cloud customers cannot  
14 trust the United States government, then maybe they won't trust U.S. cloud  
15 providers either. . . . If I were an American cloud provider, I would be quite  
16 frustrated with my government right now.").

17 If Congress wants to subject American businesses to these burdens, it can do  
18 so explicitly; but this Court should not interpret the All Writs Act implicitly to  
19 authorize courts to inflict such consequences based on ad hoc decisions without  
20 any guidance from Congress.

21 *Third*, foreign nations, including repressive regimes, would argue that they,  
22 too, may compel Apple—and other companies—to use their technical expertise to  
23 access locked phones and other devices, including those seized from political and  
24 religious dissidents or journalists. Companies that refuse assistance might well be  
25 told: the United States government compels this assistance, we may do so as well.  
26 And these foreign governments could refuse to impose the same safeguards the  
27 U.S. government proposes in this case, thereby making it far more likely that  
28 repressive regimes could use unrestricted access to cellphones' content to

1 persecute their own citizens for exercising free speech and similar human rights.

2 \* \* \* \* \*

3 In *Plum Creek*, the Ninth Circuit held that the government's request fell  
4 outside the All Writs Act because the order would subject the lumber company to  
5 risk. It observed that as a "private employer," the company "bears all safety risks.  
6 The safety factor cannot be eliminated. [The employer] pays the cost of all  
7 industrial accidents. OSHA cannot guarantee that these devices would cause  
8 none." *Id.* at 1289. The court of appeals held that "in the absence of law specifying  
9 [the devices] use, we cannot order [the employer] to bear the added risks the  
10 devices would bring." *Id.*

11 The Department of Justice here, like OSHA in *Plum Creek*, cannot guarantee  
12 that the foreseeable security risks—borne by Apple's customers and Apple itself—  
13 will not be realized. Just as the All Writs Act did not give "court[s] a roving  
14 commission to order a party subject to an investigation to accept additional risks at  
15 the bidding of OSHA inspectors," *id.*, the Act also does not authorize the  
16 government to force Apple to create a massive security vulnerability for its  
17 devices, causing serious and potentially irreparable economic and reputational  
18 harm to the company, as well as potentially infringing the fundamental human  
19 rights of individuals using its products around the world.

20 **B. The Government's Expansive Interpretation Of The Act Has No**  
21 **Limiting Principle.**

22 The order should be vacated for the additional reason that it rests on a  
23 construction of the All Writs Act that has no limiting principle. Under the  
24 government's approach, any private party may be forced against its will to assist  
25 the government in any way, subject only to the vague "unreasonable burden"  
26 limitation. Courts would be obliged to apply this standard on an ad hoc basis in  
27 numerous cases—involving different devices, device manufacturers, and software  
28 creators—that inevitably will follow this one if the government is successful. The

1 Court should refuse to interpret the statute to produce such a substantial intrusion  
2 on liberty in the absence of express congressional authorization.

3 The target of the government's request in this case is Apple, but the  
4 government's theory would just as easily extend to any third-party developer of  
5 software that has as one of its functions collecting and storing personal information  
6 about the device's owner. All such software includes security measures to protect  
7 the owner's personal information—and the government's theory would empower it  
8 to require the software creator to develop a "tool" to enable the government to  
9 access that information. The authority sought by the government would therefore  
10 extend not only to phones, laptop computers, and tablets, but also to automobiles  
11 that store information regarding location and times of use; insulin pumps that store  
12 information about blood sugar levels; and the myriad other devices that collect and  
13 store personal information.

14 Creation of government-required software tools providing access to the  
15 information stored on any such device would multiply the security risks and other  
16 burdens described above. These burdens would fall most heavily on smaller,  
17 younger technology companies—such as start-ups—that will have fewer  
18 employees and less resources.

19 The government's decisions regarding which companies to target—and  
20 courts' case-specific decisions regarding which government requests could grant—  
21 could have significant marketplace consequences. Companies forced to invent new  
22 tools to facilitate government access would have to take on risks and could be  
23 disadvantaged in the marketplace vis-à-vis competitors not forced to do so. And  
24 the uncertainty over the scope of the government's authority itself would impose  
25 significant costs on all businesses.

26 Importantly, although the government focuses on the horrific nature of the  
27 underlying crime here, nothing in the government's interpretation of the statute  
28 would limit such orders to crimes of great magnitude. Indeed, as discussed above

1 (see page 8, *supra*), the federal government and state and local prosecutors have  
2 already made clear that they believe their interpretation extends broadly to any  
3 criminal investigation.<sup>4</sup>

4 The government's theory, moreover, is not limited to digital technology.  
5 What if the government were unable to break into an "unbreakable" safe? Could  
6 the government force the company that made the safe to design a way to defeat its  
7 own product? Or suppose the government seized encoded records. Could the  
8 government conscript MIT graduate students to break the code?

9 The government can of course employ its own resources—its own  
10 employees and its own funds—to accomplish the ends it desires. But the All Writs  
11 Act does not confer a broad license upon the government to force unwilling private  
12 companies and individuals to accede to its demands.<sup>5</sup>

13 \_\_\_\_\_  
14 <sup>4</sup> In addition, nothing in the All Writs Act limits the statute's scope to criminal  
15 cases. It is not inconceivable that private plaintiffs will argue that they may invoke  
16 the All Writs Act in the same manner that the government attempts here, but in  
17 furtherance of civil discovery orders.

18 <sup>5</sup> An expert on cybersecurity issues, testifying before the House Judiciary  
19 Committee, urged Congress to address this issue by giving the FBI the resources  
20 needed to "[b]ring FBI investigative capacity into the twenty-first century":

21 The Bureau has some expertise in this direction, but it  
22 will need more, much more, both in numbers and in  
23 depth. The FBI will need an investigative center with  
24 agents with a deep technical understanding of modern  
25 telecommunications technologies; this means from the  
26 physical layer to the virtual one, and all the pieces in  
27 between. Since all phones are computers these days, this  
28 center will need to have the same level of deep expertise  
in computer science. In addition, there will need to be  
teams of researchers who understand various types of  
fielded devices. This will include not only where  
technology is and will be in six months, but where it may  
be in two to five years. This center will need to conduct  
research as to what new surveillance technologies will

(cont'd)

1           **C.    When Congress Intends To Authorize Government Conscription**  
 2           **Of Private Parties, It Does So Expressly.**

3           The absence from the All Writs Act of any express authority for conscripting  
 4 third parties provides another reason for rejecting the government's request.  
 5 Congress in other contexts has acted clearly and expressly when authorizing the  
 6 federal government to force private parties to do the government's bidding.

7           For example, the Defense Production Act, 50 U.S.C. § 4501 *et seq.*, confers  
 8 authority on the President to require private persons or companies to accept  
 9 contracts necessary for the national defense. *Id.* § 4511. That authority is explicit,  
 10 specific, and subject to a variety of restrictions, including narrow definitions of  
 11 when the statute may be invoked, *see id.* § 4552. The Defense Production Act also  
 12 has provisions requiring specific congressional authorization, *see id.* § 4514(a)  
 13 (wage and price controls), as well as a sunset provision, *see id.* § 4564.

14           Similarly, the Communications Assistance for Law Enforcement Act  
 15 (CALEA), 47 U.S.C. § 1001 *et seq.*, establishes a detailed statutory scheme  
 16 governing the assistance that telecommunications providers are obligated to  
 17 provide to the government. And CALEA expressly distinguishes between

18 \_\_\_\_\_  
 (... cont'd)

19           need to be developed as a result of the directions of new  
 20 technologies. I am talking deep expertise here and strong  
 21 capabilities, not light.

22           This expertise need not be in house. The FBI could  
 23 pursue a solution in which they develop some of their  
 24 own expertise and closely manage contractors to do some  
 25 of the work. But however the Bureau pursues a solution,  
 26 it must develop modern, state-of-the-art capabilities for  
 surveillance.

27           Zadikany Decl. Ex. G [Susan Landau, *The Encryption Tightrope: Balancing*  
 28 *Americans' Security and Privacy*, Hearing before the House Judiciary Comm.  
 (Mar. 1, 2016)].



1 “telecommunications carriers” and “information services” providers, requiring  
2 only the former to enable the government to intercept communications pursuant to  
3 a court order. *Id.* §§ 1001(8), 1002. Apple plainly is not a “telecommunications  
4 carrier.” Thus, when Congress enacted CALEA in 1994, it made a considered  
5 judgment to exclude information services providers such as Apple from the  
6 statute’s obligations.

7 Indeed, Congress in 2015 held hearings on whether CALEA should be  
8 amended to require technology companies like Apple to assist law enforcement’s  
9 requests for decryption. *See* Hanna Decl. Ex. L [Sally Quillian Yates and James B.  
10 Comey, Jr., *Going Dark: Encryption, Technology, and the Balances Between*  
11 *Public Safety and Encryption*, Hearing before the Senate Judiciary Comm. (July 8,  
12 2015)].

13 The Executive Branch publicly decided not to seek legislation, however. *See*  
14 Hanna Decl. Ex. S [James B. Comey, *Statement Before the Senate Comm. On*  
15 *Homeland Sec. & Governmental Affairs*, Hearing Before the Senate Comm. On  
16 *Homeland Sec. & Governmental Affairs* (Oct. 8, 2015)]. And the Chairman of the  
17 Senate Judiciary Committee has criticized the Administration for failing to give  
18 Congress the information it needs to consider these important policy questions.  
19 Zadikany Decl. Ex. H [Letter from Sen. Charles E. Grassley to Sally Q. Yates,  
20 Deputy Att’y Gen., and James B. Comey, Jr., Dir., Fed. Bureau of Investigation,  
21 (Feb. 16, 2016)].

22 This Court should not transform the general language of the All Writs Act  
23 into all-purpose authority for compelling the very sorts of assistance from private  
24 companies that Congress has required only pursuant to detailed laws that carefully  
25 balance all of the relevant interests. To hold otherwise would violate the Supreme  
26 Court’s instruction that the All Writs Act is designed only to “fill statutory  
27 interstices.” *Pennsylvania Bur. of Corr. v. U.S. Marshals*, 474 U.S. 34, 42 n.7  
28 (1985). It would confer upon the courts plenary, unguided authority to resolve a

1 policy issue so complex that the FBI Director has characterized it as the “hardest  
2 question” he has ever seen in government. And it would be inconsistent with the  
3 Supreme Court’s ruling in the *Steel Seizure Cases* rejecting the federal  
4 government’s analogous argument that the general language of the Constitution  
5 somehow authorized the President to seize and operate steel mills. *Youngstown*  
6 *Sheet and Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

7 **D. The Likely Practical Result of The Government’s Position Will Be**  
8 **De Facto Government-Mandated Design Specifications.**

9 Congress has explicitly refused to subject technology companies to  
10 government-imposed design specifications. CALEA expressly prohibits the  
11 government from requiring any “provider of . . . electronic communication  
12 service” to adopt a “specific design of equipment, facilities, services, features, or  
13 systems configuration.” *Id.* §1002(b)(1). Granting the order sought here—and the  
14 large numbers of requests that are sure to follow in its wake—will have the  
15 practical effect of doing just that, circumventing Congress’s intent in passing  
16 CALEA.

17 If Apple is compelled to develop the new software that the government  
18 demands, it is inevitable that the federal government, and state and local law  
19 enforcement, will seek to impose the same obligation on creators of other operating  
20 systems. Companies will then face a choice: continue to be burdened by such  
21 government demands, and design products in a manner that such demands can be  
22 more easily satisfied; or configure new versions of their operating systems to make  
23 development of such software “tools” impossible.

24 The first option would mean products intentionally designed to be less  
25 secure. That would not only subject customers to a greater risk of privacy  
26 intrusions, but also harm long-term U.S. economic interests and national security.  
27 *See, e.g.*, Hanna Decl. Ex. O [McConnell et al., *Why The Fear Over Ubiquitous*  
28 *Data Encryption Is Overblown*, Wash. Post (July 28, 2015)]. It would leave

1 ordinary citizens less secure, while malevolent actors would retain the ability to  
2 purchase completely-secure devices.

3 The second option—encouraging companies to configure products in a way  
4 that makes orders such as the one sought here impossible to implement—could  
5 have the result of making it even more difficult for law enforcement and national  
6 security agencies to access information. Indeed, it has been reported that Apple is  
7 already working on encryption software that would not be susceptible to the work-  
8 around sought by the government in this case. *See Zadikany Decl. Ex. I [Matt*  
9 *Apuzzo & Katie Benner, Apple Is Said To Be Trying To Make It Harder To Hack*  
10 *iPhone*, N.Y. Times (Feb. 24, 2016)]. The Court should not fuel that self-defeating  
11 result.

12 \* \* \* \* \*

13 As Justice Alito has explained: “In circumstances involving dramatic  
14 technological change, the best solution to privacy concerns may be legislative. A  
15 legislative body is well situated to gauge changing public attitudes, to draw  
16 detailed lines, and to balance privacy and public safety in a comprehensive way.”  
17 *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the  
18 judgment). The All Writs Act plainly does not address this complex question. This  
19 Court should therefore reject the government’s request, and leave resolution of  
20 these complex questions to policymakers.

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  
28

**CONCLUSION**

The motion to vacate should be granted and the motion to compel assistance should be denied.

Dated: March 3, 2016

MAYER BROWN LLP  
JOHN NADOLENCO  
RUTH ZADIKANY  
ANDREW J. PINCUS  
TRAVIS CRUM

By: John Nadolenco  
John Nadolenco

Attorneys for *Amici Curiae* BSA|The  
Software Alliance, the Consumer  
Technology Association, the Information  
Technology Industry Council, and TechNet

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  
28

**PROOF OF SERVICE**

I, Janice Austgen, declare:

I am employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Mayer Brown LLP, 350 South Grand Avenue, 25th Floor, Los Angeles, California 90071-1503. On March 3, 2016, I served a copy of the within document(s):

BRIEF OF *AMICI CURIAE* BSA|THE SOFTWARE ALLIANCE, THE CONSUMER TECHNOLOGY ASSOCIATION, THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL, AND TECHNET

X by placing the document(s) listed above in a sealed UPS envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a UPS agent for delivery.

SEE ATTACHED SERVICE LIST

I declare under penalty of perjury under the laws of the United States of America that the above is true and correct.

Executed on March 3, 2016, at Los Angeles, California.

  
\_\_\_\_\_  
Janice Austgen

1 Eric David Vandavelde, Esq.  
2 Theodore J. Boutrous, Jr., Esq.  
3 Gibson Dunn and Crutcher LLP  
4 333 South Grand Avenue  
5 Los Angeles, CA 90071

6 Jeffrey G. Landis, Esq.  
7 Marc J Zwillinger, Esq.  
8 Zwillgen PLLC  
9 1900 M Street NW Suite 250  
10 Washington, DC 20036

11 Nicola T. Hanna, Esq.  
12 Gibson Dunn and Crutcher LLP  
13 3161 Michelson Drive 12th Floor  
14 Irvine, CA 92612-4412

15 Theodore B. Olson, Esq.  
16 Gibson Dunn and Crutcher LLP  
17 1050 Connecticut Avenue NW  
18 Washington, DC 20036-5306

19 Allen W. Chiu, Esq.  
20 Assistant United States Attorney  
21 Office of U.S. Attorney  
22 National Security Section  
23 312 North Spring Street Suite 1300  
24 Los Angeles, CA 90012

25 Tracy L. Wilkison, Esq.  
26 Assistant United States Attorney  
27 Office of U.S. Attorney  
28 Chief, Cyber and Intellectual Property Crimes Section  
312 North Spring Street 11th Floor  
Los Angeles, CA 90012-4700



ORIGINAL

1 MAYER BROWN LLP  
2 JOHN NADOLENCO (SBN 181128)  
3 *jnadolenco@mayerbrown.com*  
4 RUTH ZADIKANY (SBN 260288)  
5 *rzadikany@mayerbrown.com*  
6 350 South Grand Avenue, 25th Floor  
7 Los Angeles, California 90071-1503  
8 Telephone: (213) 229-9500  
9 Facsimile: (213) 625-0248



10 ANDREW J. PINCUS (*pro hac vice application forthcoming*)  
11 *apincus@mayerbrown.com*  
12 TRAVIS CRUM (*pro hac vice application forthcoming*)  
13 *tcrum@mayerbrown.com*  
14 1999 K Street, N.W.  
15 Washington D.C. 20006-1001  
16 Telephone: (202) 263-3328  
17 Facsimile: (202) 263-5328

18 Attorneys for *Amici Curiae* BSA|The Software Alliance, The  
19 Consumer Technology Association, The Information Technology  
20 Industry Council, and TechNet

21 **UNITED STATES DISTRICT COURT**  
22 **CENTRAL DISTRICT OF CALIFORNIA**  
23 **EASTERN DIVISION**

24 **IN THE MATTER OF THE SEARCH**  
25 **OF AN APPLE IPHONE SEIZED**  
26 **DURING THE EXECUTION OF A**  
27 **SEARCH WARRANT ON A BLACK**  
28 **LEXUS IS300, CALIFORNIA**  
**LICENSE PLATE 35KGD203**

Case No. 5:16-cm-00010-SP

Declaration Of Ruth Zadikany In Support Of Brief of *Amici Curiae* BSA|The Software Alliance, The Consumer Technology Association, The Information Technology Industry Council, And TechNet

Hearing Date: March 22, 2016

Time: 1:00 p.m.

Location: Courtroom 3 or 4

Judge: Hon. Sheri Pym

LODGED

2016 MAR 3 PM 2:32

CLERK U.S. DISTRICT COURT  
CENTRAL DIST. OF CALIF.  
RIVERSIDE

**DECLARATION OF RUTH ZADIKANY**

I, Ruth Zadikany, declare as follows:

1. I am an attorney licensed to practice law in the State of California. I am an associate in the law firm of Mayer Brown LLP. I submit this declaration in support of the Brief of *Amici Curiae* BSA|The Software Alliance, the Consumer Technology Association, the Information Technology Industry Council, and TechNet in the above-referenced matter. I have personal knowledge of the matters stated herein and could and would competently testify thereto if called as a witness.

2. Attached hereto as **Exhibit A** is a true and correct copy of the Los Angeles Times article, *FBI Director Calls Apple Case 'Hardest Question' In Government*, by Brian Bennett, originally published on February 25, 2016, available at <http://www.latimes.com/nation/la-na-intel-threats-20160225-story.html>. The article was printed on March 3, 2016.

3. Attached hereto as **Exhibit B** is a true and correct copy of a Pew Research Center report, *Americans Feel the Tensions between Privacy and Security Concerns*, by Lee Rainie and Shiva Maniam, originally published on February 19, 2016, available at <http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns>. The report was printed on March 3, 2016.

4. Attached hereto as **Exhibit C** is a true and correct copy of a Pew Research Center report, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, by Mary Madden, originally published on November 12, 2014, available at <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>. The report was printed on March 3, 2016.

5. Attached hereto as **Exhibit D** is a true and correct copy of a Gallup report, *Hacking Tops List of Crimes Americans Worry About Most*, by Rebecca Riffkin, originally published on October 27, 2014, available at

1 [http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-](http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx)  
2 [worry.aspx](http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx). The report was printed on March 3, 2016.

3 6. Attached hereto as **Exhibit E** is a true and correct copy of a  
4 Huffington Post article, *'Snowden Effect' Threatens U.S. Tech Industry's Global*  
5 *Ambitions*, by Gerry Smith, originally published on January 24, 2014, available at  
6 [http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-](http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html)  
7 [industry\\_n\\_4596162.html](http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html). The article was printed on March 3, 2016.

8 7. Attached hereto as **Exhibit F** is a true and correct copy of an  
9 InformationWeek article, *NSA's Prism Could Cost U.S. Cloud Companies \$45*  
10 *Billion*, by Charles Babcock, originally published on August 14, 2013, available at  
11 [http://www.informationweek.com/cloud/infrastructure-as-a-service/nsas-prism-](http://www.informationweek.com/cloud/infrastructure-as-a-service/nsas-prism-could-cost-us-cloud-companies-$45-billion/d/d-id/1111178?)  
12 [could-cost-us-cloud-companies-\\$45-billion/d/d-id/1111178?](http://www.informationweek.com/cloud/infrastructure-as-a-service/nsas-prism-could-cost-us-cloud-companies-$45-billion/d/d-id/1111178?). The article was  
13 printed on March 3, 2016.

14 8. Attached hereto as **Exhibit G** is a true and correct copy of testimony  
15 of Susan Landau before the House Judiciary Committee entitled *The Encryption*  
16 *Tightrope: Balancing Americans' Security and Privacy*, originally published on  
17 March 1, 2016, available at [http://judiciary.house.gov/\\_cache/files/b3af6e9e-b599-](http://judiciary.house.gov/_cache/files/b3af6e9e-b599-4216-b2f9-1aee6a1d90cd/landau-written-testimony.pdf)  
18 [4216-b2f9-1aee6a1d90cd/landau-written-testimony.pdf](http://judiciary.house.gov/_cache/files/b3af6e9e-b599-4216-b2f9-1aee6a1d90cd/landau-written-testimony.pdf). The testimony was printed  
19 on March 3, 2016.

20 9. Attached hereto as **Exhibit H** is a true and correct copy of a letter  
21 from Senator Charles E. Grassley, Chairman of the Senate Judiciary Committee, to  
22 Deputy Attorney General Sally Q. Yates and FBI Director James B. Comey, Jr.,  
23 originally published on February 16, 2016, and available at  
24 [http://www.grassley.senate.gov/sites/default/files/judiciary/upload/Encryption,%20](http://www.grassley.senate.gov/sites/default/files/judiciary/upload/Encryption,%2002-16-16,%20Going%20Dark%20QFR%20Response%20Letter.pdf)  
25 [02-16-16,%20Going%20Dark%20QFR%20Response%20Letter.pdf](http://www.grassley.senate.gov/sites/default/files/judiciary/upload/Encryption,%2002-16-16,%20Going%20Dark%20QFR%20Response%20Letter.pdf). The letter  
26 was printed on March 3, 2016.

27 10. Attached hereto as **Exhibit I** is a true and correct copy of a New York  
28 Times article, *Apple Is Said To Be Trying To Make It Harder To Hack iPhone*, by

1 Matt Apuzzo and Katie Benner, originally published on February 24, 2016,  
2 available at [http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-](http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html)  
3 [working-on-an-iphone-even-it-cant-hack.html](http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html). The article was printed on March 3,  
4 2016.

5  
6 Dated: March 3, 2016

7  
8 By:   
9 Ruth Zadikany

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

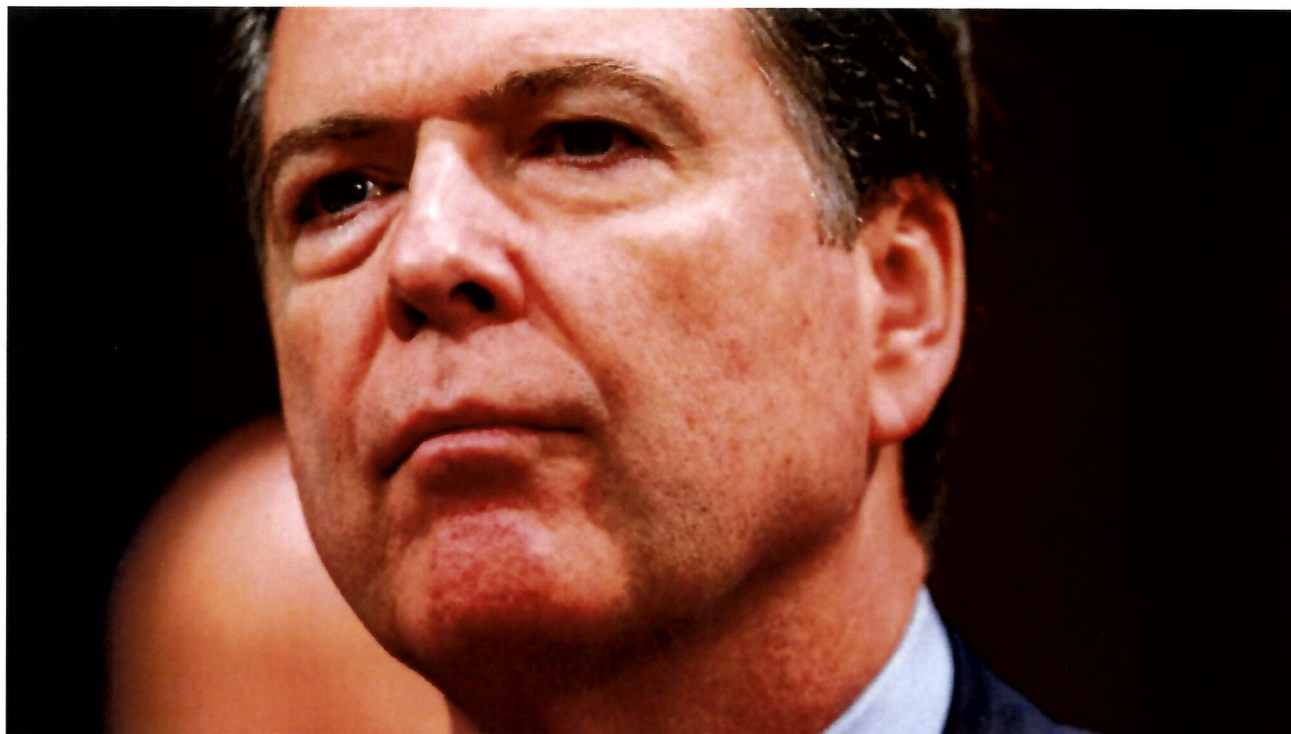


# **Exhibit A**



NATION

# FBI director calls Apple case 'hardest question' in government



FBI Director James Comey appears at a House Intelligence Committee hearing on worldwide threats on Capitol Hill in Washington. (Andrew Harnik / Associated Press)



By **Brian Bennett** · Contact Reporter

FEBRUARY 25, 2016, 9:37 AM | REPORTING FROM WASHINGTON

**T**he legal fight between the FBI and Apple over unlocking an iPhone in the San Bernardino mass murder case will impact other investigations in which law enforcement is seeking access to encrypted devices, FBI Director James Comey said Thursday.

The FBI has asked Apple for help opening 13 other devices in cases across the country. Since the fall, Apple lawyers have balked at taking additional steps, including writing software, to unlock password-protected phones and tablets.

“This is the hardest question I’ve ever seen in government,” Comey told the House Intelligence Committee at a hearing on national security threats facing the United States.

## **Join the conversation on Facebook >>**

The public needs to debate whether law enforcement should be able to access encrypted communications with a court order, and how to balance that with technological advances designed to protect customers' privacy from hackers and unwarranted government surveillance, he said.

Comey said the central question is "who do we want to be, and how do we want to govern ourselves?"

Apple has refused to comply with a federal magistrate judge's order to build a software program that would circumvent the password protection on the work phone used by Syed Rizwan Farook before the Dec. 2 massacre at the Inland Regional Center that killed 14 people.

U.S. Magistrate Judge Sheri Pym of the U.S. District Court for the Central District of California in Riverside, Calif., has given Apple until Friday to respond to her order.

"Whatever the judge's decision in California, however it ends up, will be instructive for other courts," Comey said.

Privacy advocates and Apple executives argue that agreeing to hack Apple's security features in this case would establish a precedent that federal, state and local law enforcement could use in other investigations.

Meeting the FBI's demand "could expose people to incredible vulnerabilities" and "also set a bad precedent that I think many people in America would be offended by," Apple Chief Executive Tim Cook told ABC's "World News Tonight" on Wednesday.

The FBI cannot unlock the iPhone on its own, Comey said.

"Sometimes we are not as attractive or as technologically talented as we appear on TV," he said.

The FBI "must do a competent investigation" of the mass shooting in San Bernardino, Comey said, and "we will use whatever lawful tools are available to us."

Apple has been "very helpful" in the investigation, Comey said, but the company balked when the FBI asked its technicians to write special software so the FBI could obtain the password to open Farook's iPhone 5c.

In court papers, the FBI has said the device may contain text messages, photographs, location data and other information from Oct. 19, when it was last backed up to the iCloud, until the shooting nearly seven weeks later.

Court documents filed in a separate drug case in Brooklyn, N.Y., show Apple faces federal court orders to access data on at least 13 other locked devices around the country.

Twelve of the devices were listed in a Feb. 17 filing by Apple in the U.S. District Court in the Eastern District of New York. The Justice Department added another device to the list in a letter to the court.

The requests include federal courts in California, Illinois, Massachusetts and New York. Eleven of the devices are iPhones, one is an iPad 2 Wifi, and another device wasn't identified.

The list does not include any devices in local law enforcement investigations. Manhattan Dist. Atty. Cyrus Vance has said that his criminal investigators have possession of 175 Apple devices they are unable to open.

**[brian.bennett@latimes.com](mailto:brian.bennett@latimes.com)**

**Follow me @ByBrianBennett on Twitter**

**MORE ON APPLE VS. FBI**

**Chinese tech execs side with Apple -- or maybe just against the FBI**

**In the fight to unlock iPhones, the U.S. government has more to lose than Apple**

**Apple's Tim Cook disappointed with Justice Department's handling of San Bernardino case**

Copyright © 2016, Los Angeles Times

**This article is related to:** Apple Inc., FBI, Apple iPhone, San Bernardino Terror Attack, Syed Rizwan Farook, Tim Cook, U.S. Department of Justice



# Exhibit B



# PewResearchCenter

FEBRUARY 19, 2016

## Americans feel the tensions between privacy and security concerns

BY LEE RAINIE ([HTTP://WWW.PEWRESEARCH.ORG/STAFF/LEE-RAINIE/](http://www.pewresearch.org/staff/lee-rainie/)) AND SHIVA MANIAM ([HTTP://WWW.PEWRESEARCH.ORG/AUTHOR/SMANIAM/](http://www.pewresearch.org/author/smaniam/))

Americans have long been divided in their views about the trade-off between security needs and personal privacy. Much of the focus has been on government surveillance, though there are also significant concerns about how businesses use data. The issue flared again this week when a federal court ordered Apple to help the FBI unlock an iPhone (<http://www.nytimes.com/2016/02/18/technology/explaining-apples-fight-with-the-fbi.html>) used by one of the suspects in the terrorist attack in San Bernardino, California, in December. Apple challenged the order (<http://www.apple.com/customer-letter/>) to try to ensure that security of other iPhones remained protected, and also to provoke a wider national conversation about how far people would like technology firms to go ([http://www.nytimes.com/2016/02/18/technology/apples-stance-highlights-a-more-confrontational-tech-industry.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&\\_r=0](http://www.nytimes.com/2016/02/18/technology/apples-stance-highlights-a-more-confrontational-tech-industry.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0)) in protecting their privacy or cooperating with law enforcement.

([http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ft\\_16-02-09\\_concerns\\_security2/](http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ft_16-02-09_concerns_security2/)) Events have had a major impact on public attitudes on this issue. Terrorist attacks generate increased anxieties. For instance, the San Bernardino and Paris shootings in late 2015 had a striking impact. A Pew Research Center survey (<http://www.people-press.org/2015/12/15/views-of-governments-handling-of-terrorism-fall-to-post-911-low/#views-of-how-the-government-is-handling-the-terrorist-threat>) in December found that 56% of Americans were more concerned that the government's anti-terror policies have not gone far enough to protect the country, compared with 28% who expressed concern that the policies have gone too far in restricting the average person's civil liberties. Just two years earlier, amid the furor over Edward Snowden's revelations (<http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/>) about National Security Agency surveillance programs, more said their bigger concern was that anti-terror programs had gone too far in restricting civil liberties (47%) rather than not far enough in protecting the country (35%).

At the same time, there are other findings suggesting that Americans are becoming more anxious (<http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/>) about their privacy, especially in the context of digital technologies that capture a wide array of data about them. Here is an overview of the state of play as the iPhone case moves further into legal proceedings.



**How people have felt about government anti-terror policies**

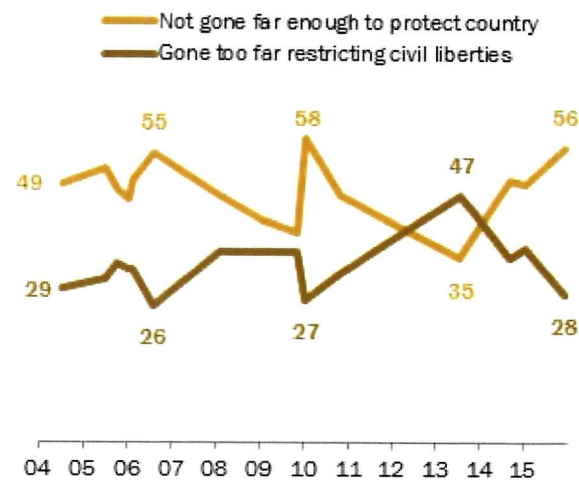
Pew Research Center surveys since the 9/11 terrorist attacks have generally shown that in the periods when high-profile cases related to privacy vs. security first arise, majorities of adults favor a “security first” approach

(<http://www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/>  
<http://www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/>  
<http://www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/>) to these issues,

while at the same time urging that dramatic sacrifices on civil liberties be avoided. New incidents often result in Americans backing at least some extra steps by the law enforcement and intelligence communities to investigate terrorist suspects, even if that might infringe on the privacy of citizens. But many draw the line at deep interventions into their personal lives.

**Public’s shifting concerns on security and civil liberties**

*Bigger concern about govt anti-terrorism policies? (%)*



Source: Survey conducted Dec. 8-13, 2015. Don't know responses not shown.

PEW RESEARCH CENTER

**Civil liberties and anti-terrorism policies**

	Sept 2001	Aug 2002	Dec 2006	Aug 2011
<i>Percent who favor each as a measure to curb terrorism</i>	%	%	%	%
Requiring that all citizens carry a national ID card at all times	70	59	57	57
Extra airport checks on passengers who appear to be of Middle-Eastern descent	--	59	57	53
Government monitoring credit card purchases	--	43	42	42
Government monitoring personal phone calls and emails	--	33	34	29

PEW RESEARCH CENTER Aug 17-21, 2011 Q77.

([http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ft\\_16-02-20-civilliberties-antiterrorism/](http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ft_16-02-20-civilliberties-antiterrorism/)) For instance, our survey shortly after the 9/11 attacks (<http://www.people-press.org/2001/09/19/other-important-findings-and-analyses-48/>) found that 70% of adults favored requiring citizens to carry national ID cards. At the same time, a majority balked at government monitoring of their own emails and personal phone calls or their credit card purchases.

It should be noted that surveys have also found that people’s immediate concerns about security can subside over time. In a poll conducted in 2011 (<http://www.people-press.org/2011/09/01/united-in-remembrance-divided-over-policies/1/>), shortly before the 10th anniversary of 9/11, 40% said that “in order to curb terrorism in this country it will be necessary for the average person to give up some civil liberties,” while 54% said it would not. A decade earlier, in the aftermath of 9/11 and before the passage of the Patriot Act, opinion was nearly the reverse (55% necessary, 35% not necessary).

When The New York Times reported in late 2005 that President George W. Bush authorized the NSA to eavesdrop on Americans (<http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>), subsequent Pew Research Center surveys found that 50% of Americans were concerned that the government hadn’t yet gone far enough (<http://www.people-press.org/2006/02/07/iran-a-growing-danger-bush-gaining-on-spy-issue/>) in protecting the country against terrorism, and 54% said it was generally right for the government to monitor (<http://www.people-press.org/2006/09/14/democrats-hold-solid-lead-strong-anti-incumbent-anti-bush-mood/>) the telephone and email communications of Americans suspected of having ties with terrorists without first obtaining court permission. Some 43% said such surveillance was generally wrong. Quite similar numbers were found in a survey (<http://www.people-press.org/2009/02/18/obama-faces-familiar-divisions-over-anti-terror-policies/>) at when President Barack Obama took office in 2009.

([http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ft\\_16-02-19-snowden-surveillance/](http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ft_16-02-19-snowden-surveillance/)) Right after the Snowden revelations in June 2013, a Pew Research Center poll found that 48% of Americans approved of the government’s collection of telephone and internet data as part of anti-terrorism efforts. But by January 2014, approval had declined to 40%.

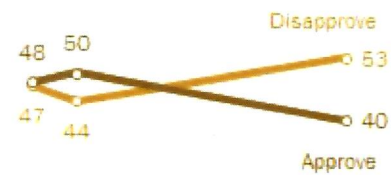
And many Americans continue to express concern about the government’s surveillance program. In an early 2015 online survey, 52% of Americans described themselves as “very concerned” (<http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>) or “somewhat concerned” about government surveillance of Americans’ data and electronic communications, compared with 46% who described themselves as “not very concerned” or “not at all concerned” about the surveillance.

**How people feel about corporate practices**

As businesses increasingly mine data about consumers, Americans are concerned about preserving their privacy when it comes to their personal information and behaviors. Those views have intensified in recent years, especially after big data breaches (<http://money.cnn.com/2013/12/18/news/companies/target-credit-card/>) at companies such as Target (<http://money.cnn.com/2013/12/18/news/companies/target-credit-card/>), eBay (<https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/eBay-asks-145-million-users-to-change-passwords-after-data-breach/>) and Anthem (<http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/>) as well as of federal employee personnel files

**Post-Snowden, increased opposition to gov’t surveillance**

*The government’s collection of telephone and internet data as part of anti-terrorism efforts*



Jun Jul Aug Sep Oct Nov Dec Jan  
 2013 2014

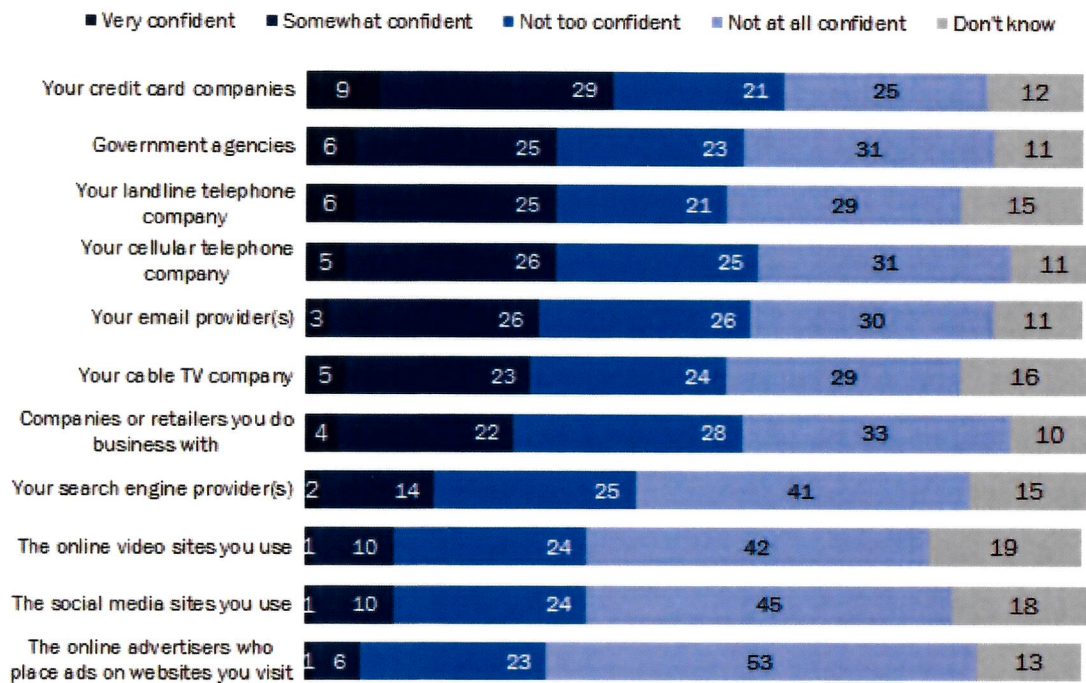
Survey conducted Jan 15-19, 2014.  
 PEW RESEARCH CENTER/USA TODAY



(<http://federalnewsradio.com/cybersecurity/2015/10/opm-notifies-3-7-million-cyber-attack-victims-about-data-protection-services/>) . Our surveys show that people now are more anxious about the security of their personal data and are more aware that greater and greater volumes of data are being collected about them. The vast majority feel they have lost control of their personal data (<http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>) , and this has spawned considerable anxiety (<http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>) . They are not very confident that companies collecting their information will keep it secure.

### Few express confidence that their records will remain private and secure

*% of adults who express varying levels of confidence that the records of their activity maintained by various companies and organizations will remain private and secure*



Source: Survey conducted August 5, 2014-September 2, 2014. Refused responses are not shown.

PEW RESEARCH CENTER

(<http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/>)

### In assessing public attitudes, context matters – and so does how the question is framed

One consistent finding over the years about public attitudes related to privacy and societal security is that people’s answers often depend on the context. The language of the questions we ask sometimes affects the way people respond.

A recent Pew Research Center study (<http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>) showed that, in commercial situations, people’s views on the trade-off between offering information about themselves in exchange for something of value are shaped by both the conditions of the deal and the

circumstances of their lives. People indicated that their interest and overall comfort level in sharing personal information depends on the company or organization with which they are bargaining and how trustworthy or safe they perceive the firm to be. It also depends on what happens to their data after they are collected, especially if the data are made available to third parties, and on how long the data are retained.

A study in the wake of the Snowden revelations showed that there was notable change in public attitudes (<http://www.people-press.org/2013/07/26/government-surveillance-a-question-wording-experiment/>) about NSA surveillance programs when questions were modified. For instance, only 25% favored NSA surveillance when there was no mention of court approval of the program. But 37% favored it when the program was described as being approved by courts. Similarly, characterizing the government's data collection "as part of anti-terrorism efforts" garnered more support than not mentioning this (35% favored vs. 26% favored).



Lee Rainie (<http://www.pewresearch.org/author/lrainie/>) is director of internet, science and technology research at Pew Research Center.

[POSTS](#) | [EMAIL](#) | [BIO](#) | [@LRAINIE](#)

Shiva Maniam (<http://www.pewresearch.org/author/smaniam/>) is a research assistant focusing on U.S. politics and policy at Pew Research Center.

[POSTS](#) | [EMAIL](#)

---

## 1 Comment



**Red Flag Target** • 2 weeks ago (#comment-665146)

+

The FBI, DHS and NSA are engaged in a hard-core, extra-judicial "disruption" campaign which targets innocent Americans as "potential domestic terrorists," and robs them of their constitutional rights in the process.

Tens of thousands of Americans have been illegally targeted and terrorized by the NSA, FBI, DHS and private security contractors (think of a domestically-run "Blackwater").

They engage in cyber-harassment, warrantless entries into homes and vehicles, destruction of careers and families through defamation of character and false accusations, overt and covert harassment.

They are utilizing tactics developed by the East German Stasi referred to as "Zersetzung." This is a multi-billion dollar operation run out of the DoJ, with the help of the DHS. Retired FBI, DEA, and DHS employees open up private security companies and rake in huge money to help "monitor" (harass and destroy) innocent Americans who have been watch-listed without any due process.

It is a sadistic program which is being illegally run in the shadows.

Reply

Share this selection





# **Exhibit C**



about telephone calls, emails, and other online communications as part of efforts to monitor terrorist activity,” and another 44% have heard “a little.” Just 5% of adults in our panel said they have heard “nothing at all” about these programs.

### **Widespread concern about surveillance by government and businesses**

Perhaps most striking is Americans’ lack of confidence that they have control over their personal information. That pervasive concern applies to everyday communications channels and to the collectors of their information—both in the government and in corporations. For example:

- 91% of adults in the survey “agree” or “strongly agree” that consumers have lost control over how personal information is collected and used by companies.
- 88% of adults “agree” or “strongly agree” that it would be very difficult to remove inaccurate information about them online.
- 80% of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites.
- 70% of social networking site users say that they are at least somewhat concerned about the government accessing some of the information they share on social networking sites without their knowledge.

Yet, even as Americans express concern about government access to their data, they feel as though government could do more to regulate what advertisers do with their personal information:

- 80% of adults “agree” or “strongly agree” that Americans should be concerned about the government’s monitoring of phone calls and internet communications. Just 18% “disagree” or “strongly disagree” with that notion.
- 64% believe the government should do more to regulate advertisers, compared with 34% who think the government should not get more involved.
- Only 36% “agree” or “strongly agree” with the statement: “It is a good thing for society if people believe that someone is keeping an eye on the things that they do online.”

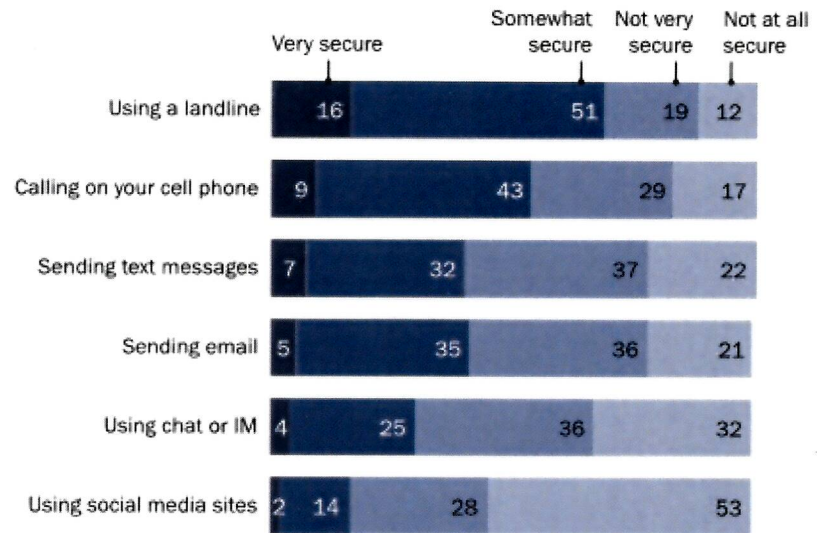
In the commercial context, consumers are skeptical about some of the benefits of personal data sharing, but are willing to make tradeoffs in certain circumstances when their sharing of information provides access to free services.

- 61% of adults “disagree” or “strongly disagree” with the statement: “I appreciate that online services are more efficient because of the increased access they have to my personal data.”
- At the same time, 55% “agree” or “strongly agree” with the statement: “I am willing to share some information about myself with companies in order to use online services for free.”

**There is little confidence in the security of common communications channels, and those who have heard about government surveillance programs are the least confident**

**The public feels most secure using landline phones, least secure on social media**

*% of adults who feel varying degrees of security when sharing private info with another trusted person or organization*



Source: Pew Research Privacy Panel Survey, January 2014. N=607 adults, ages 18 and older.

**PEW RESEARCH CENTER**

([http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/pi\\_2014-11-12\\_privacy-perceptions\\_02/](http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/pi_2014-11-12_privacy-perceptions_02/))

Across the board, there is a universal lack of confidence among adults in the security of everyday communications channels—particularly when it comes to the use of online tools. Across six different methods of mediated communication, there is not one mode through which a majority of the American public feels “very secure” when sharing private information with another trusted person or organization:

- 81% feel “not very” or “not at all secure” using social media sites when they want to share private information with another trusted person or organization.
- 68% feel insecure using chat or instant messages to share private information.
- 58% feel insecure sending private info via text messages.
- 57% feel insecure sending private information via email.
- 46% feel “not very” or “not at all secure” calling on their cell phone when they want to share private information.

- 31% feel “not very” or “not at all secure” using a landline phone when they want to share private information.

Americans’ lack of confidence in core communications channels tracks closely with how much they have heard about government surveillance programs. For five out of the six communications channels we asked about, those who have heard “a lot” about government surveillance are significantly more likely than those who have heard just “a little” or “nothing at all” to consider the method to be “not at all secure” for sharing private information with another trusted person or organization.

**Most say they want to do more to protect their privacy, but many believe it is not possible to be anonymous online**

When it comes to their own role in managing the personal information they feel is sensitive, most adults express a desire to take additional steps to protect their data online: When asked if they feel as though their own efforts to protect the privacy of their personal information online are sufficient, 61% say they feel they “would like to do more,” while 37% say they “already do enough.”

When they want to have anonymity online, few feel that is easy to achieve. Just 24% of adults “agree” or “strongly agree” with the statement: “It is easy for me to be anonymous when I am online.”

**Not everyone monitors their online reputation very vigilantly, even though many assume others will check up on their digital footprints**

Some people are more anxious than others to keep track of their online reputation. Adults under the age of 50 are far more likely to be “self-searchers” than those ages 50 and older, and adults with higher levels of household income and education stand out as especially likely to check up on their own digital footprints.

- 62% of adults have ever used a search engine to look up their own name or see what information about them is on the internet.
- 47% say they generally assume that people they meet will search for information about them on the internet, while 50% do not.
- However, just 6% of adults have set up some sort of automatic alert to notify them when their name is mentioned in a news story, blog, or elsewhere online.

**Just 24% of adults “agree” or “strongly agree” with the statement: “It is easy for me to be anonymous when I am online.”** (<https://twitter.com/intent/tweet?url=http://pewrsr.ch/1w1EbYR&text=24%25%20of%20adults%20say%20%27It%20is%20easy%20for%20me%20to%20be%20anonymous%20when%20I%20am%20online.%27>)



### **Context matters as people decide whether to disclose information or not**

One of the ways that people cope with the challenges to their privacy online is to employ multiple strategies for managing identity and reputation across different networks and transactions. As previous findings (<http://www.pewinternet.org/2013/09/05/part-1-the-quest-for-anonymity-online/>) from the Pew Research Center have suggested, users bounce back and forth between different levels of disclosure depending on the context. This survey also finds that when people post comments, questions or other information, they do so using a range of identifiers—using a screen name, their actual name, or posting anonymously.

Among all adults:

- 59% have posted comments, questions or other information online using a user name or screen name that people associate with them.
- 55% have done so using their real name.
- 42% have done so anonymously.

In some cases, the choices people make about disclosure may be tied to work-related policies. Among employed adults:

- 24% of employed adults say that their employer has rules or guidelines about how they are allowed to present themselves online.
- 11% say that their job requires them to promote themselves through social media or other online tools.

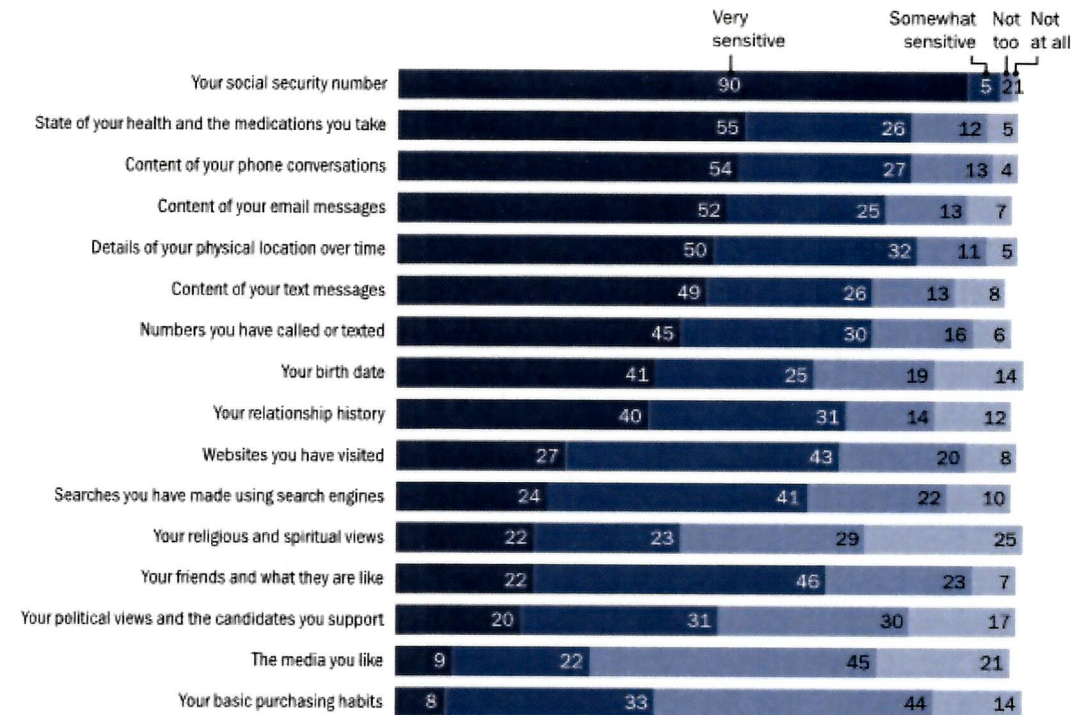
### **Different types of information elicit different levels of sensitivity among Americans**

Social security numbers are universally considered to be the most sensitive piece of personal information, while media tastes and purchasing habits are among the least sensitive categories of data.



## Social security numbers, health info and phone conversations among the most sensitive data

% of adults who report varying levels of sensitivity about the following kinds of info



Source: Pew Research Privacy Panel Survey, January 2014. N=607 adults, ages 18 and older.

PEW RESEARCH CENTER

([http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/pi\\_2014-11-12\\_privacy-perceptions\\_03/](http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/pi_2014-11-12_privacy-perceptions_03/))

At the same time that Americans express these broad sensitivities toward various kinds of information, they are actively engaged in negotiating the benefits and risks of sharing this data in their daily interactions with friends, family, co-workers, businesses and government. And even as they feel concerned about the possibility of misinformation circulating online, relatively few report negative experiences tied to their digital footprints.

- 11% of adults say they have had any bad experiences because embarrassing or inaccurate information was posted about them online.
- 16% say they have asked someone to remove or correct information about them that was posted online.

### About this Report

This report is the first in a series of studies that examines Americans' privacy perceptions and behaviors following the revelations about U.S. government surveillance programs by government contractor Edward Snowden that began in June of 2013. To examine this topic in depth and over an extended period of time,

the Pew Research Center's Internet Project commissioned a representative online panel of 607 adults who are members of the GfK Knowledge Panel. These panelists have agreed to respond to four surveys over the course of one year. The findings in this report are based on the first survey, which was conducted in English and fielded online January 11-28, 2014. In addition, a total of 26 panelists also participated in one of three online focus groups as part of this study during August 2013 and March 2014.

This report is a collaborative effort based on the input and analysis of the following individuals:

Mary Madden, *Senior Researcher, Internet Project*  
Lee Rainie, *Director, Internet, Science and Technology Research*  
Kathryn Zickuhr, *Research Associate, Internet Project*  
Maeve Duggan, *Research Analyst, Internet Project*  
Aaron Smith, *Senior Researcher, Internet Project*

Other reports from the Pew Research Center Internet Project on the topic of privacy and security online can be found at: <http://www.pewinternet.org/topics/privacy-and-safety/pages/2/>  
(<http://www.pewinternet.org/topics/privacy-and-safety/pages/2/>)

### **About this survey**

The analysis in this report is based on a survey conducted January 10-27, 2014 among a sample of 607 adults, 18 years of age or older. The survey was conducted by the GfK Group using KnowledgePanel, its nationally representative online research panel. GfK selected a representative sample of 1,537 English-speaking panelists to invite to join the subpanel and take the first survey. Of the 935 panelists who responded to the invitation (60.8%), 607 agreed to join the subpanel and subsequently completed the first survey (64.9%). This group has agreed to take four online surveys about "current issues, some of which relate to technology" over the course of a year and possibly participate in one or more 45-60-minute online focus group chat sessions. A random subset of the subpanel receive occasional invitations to participate in these online focus groups. For this report, a total of 26 panelists participated in one of three online focus groups conducted during August 2013 and March 2014. Sampling error for the total sample of 607 respondents is plus or minus 4.6 percentage points at the 95% level of confidence.<sup>1</sup>

For more information on the GfK Privacy Panel, please see the Methods section at the end of this report.

### **Acknowledgements**

The authors would like to acknowledge the generous contributions of the various outside reviewers who offered their insights at various stages of this project. In particular, we would like to thank: Tiffany Barrett, danah boyd, Mary Culnan and all of the attendees of the Future of Privacy Forum Research Seminar Series, Urs Gasser, Chris Hoofnagle, Michael Kaiser, Kirsten Martin and Katie Shilton. In addition, the authors are grateful for the ongoing editorial, methodological and production-related support provided by the staff of the Pew Research Center.

While we greatly appreciate all of these contributions, the authors alone bear responsibility for the presentation of these findings, as well as any omissions or errors.

1. The original margin of error provided by the vendor and published here (3.98) used a less conservative design effect. However, the analysis in the report was based on the more conservative design effect and the significance of the findings is not affected by this change. →

Share this selection



# **Exhibit D**

E

OCTOBER 27, 2014

# Hacking Tops List of Crimes Americans Worry About Most

by Rebecca Riffkin

---

## STORY HIGHLIGHTS

- Theft of one's credit card info from stores is most common worry
- 62% of Americans worry about computer and smartphone hacking
- One-quarter report credit card info was hacked through a store

---

WASHINGTON, D.C. -- As the list of major U.S. retailers hit by credit card hackers continues to grow this year, Americans are more likely to worry about having credit card information they used in stores stolen by computer hackers than any other crime they are asked about. Sixty-nine percent of Americans report they frequently or occasionally worry about this happening to them. Having a computer or smartphone hacked (62%) is the only other crime that worries the majority of Americans.



*Crime Worries in U.S.*

How often do you, yourself, worry about the following things -- frequently, occasionally, rarely or never? How about ...

	<b>% Frequently or occasionally worry</b>
Having the credit card information you have used at stores stolen by computer hackers	69
Having your computer or smartphone hacked and the information stolen by unauthorized persons	62
Your home being burglarized when you are not there	45
Having your car stolen or broken into	42
Having a school-aged child physically harmed attending school	31
Getting mugged	31
Your home being burglarized when you are there	30
Being the victim of terrorism	28
Being attacked while driving your car	20
Being a victim of a hate crime	18
Being sexually assaulted	18
Getting murdered	18
Being assaulted/killed by a coworker/employee where you work	7

Oct. 12-15, 2014

**GALLUP**

Less than half of Americans worry at least occasionally about other crimes, ranging from 45% who worry about their home being burglarized when they are not there to 7% who worry about being assaulted by a coworker on the job.

Gallup updated its measure of Americans' worry about a number of crime scenarios in its annual Crime poll, conducted Oct. 12-15. Trends on Americans' worries about most of these crimes extend back to 2000, although this was the first year Gallup asked Americans about having credit card information stolen or a smartphone or computer hacked.

Upper-income Americans, those whose household incomes are \$75,000 or more a year, are more likely than lower-income Americans to worry frequently or occasionally about hacking of their credit card information, 85% to 50%. Americans between the ages of 30 and 64 worry about this more than younger and older Americans do.

*Upper-Income More Likely Than Lower-Income Americans to Worry About Hacking*

% Frequently or occasionally worry

	<b>Credit card info hacking at stores</b>	<b>Computer/ Smartphone hacking</b>
	<b>%</b>	<b>%</b>
Annual household income less than \$30,000	50	46
Annual household income \$30,000 to \$74,999	71	64
Annual household income \$75,000+	85	76
18 to 29 years old	62	55
30 to 49 years old	72	69
50 to 64 years old	77	63
65+ years old	62	53

Oct. 12-15, 2014

GALLUP

Higher levels of worry about credit card and computer-related crimes among upper-income Americans may result from their higher daily spending. Additionally, lower-income Americans are less likely to own credit cards or smartphones. In April, 58% of Americans whose annual household incomes are less than \$30,000 said they owned no credit cards, compared with 11% of upper-income Americans. In December 2013, Gallup found that upper-income Americans are also more likely than lower-income Americans to own a smartphone, 84% vs. 46%.

**More Than One in Four Americans Say They Have Been Hacked**

Americans may be more worried about hacking because a relatively high percentage of them say they have had their information hacked. A quarter of Americans, 27%, say they or another household member had information from a credit card used at a store stolen by computer hackers during the last year -- making this the most frequently experienced crime on a list of nine crimes. Eleven percent say they or a household member have had their computer or smartphone hacked in the last year, also in the top half of crimes on the list.

Although a relatively high percentage of Americans say they have been hacking victims, relatively low percentages say they reported it to the police. Slightly less than half of Americans (45%) who say they had credit card information stolen say they reported it to the police. And about a quarter of victims say they notified police

about their computer or smartphone being hacked. Of Americans who say they were victims of other crimes in the last year, including stolen cars, muggings, or burglaries, an average of two-thirds say they reported them to police, higher than what Gallup finds for hacking crimes.

One reason reporting of credit card information theft may be lower is that some Americans who are victims of these crimes may not have seen monetary losses. The Department of Homeland Security estimates that more than 1,000 U.S. businesses have been hit by cyberattacks similar to the one that hit U.S. retailer Target; the Target breach alone is estimated to have affected 40 million credit and debit card accounts. Although this is a large proportion of Americans whose information could have been affected, it is unknown how many actually saw these cards used for fraudulent purchases.

### **Bottom Line**

Americans today are more worried about their credit card information being hacked from stores than about any other crimes they are asked about, and a relatively high percentage say they have been victims of this hacking. Many high-profile and popular stores and restaurants have had major hacking problems in 2013 and 2014, something that no doubt has helped kindle such fears.

With credit card hacking clearly a concern to many Americans, it may affect their shopping habits as they take measures to protect their identities and finances. Consumers may avoid stores that have been hacked, and begin paying more frequently with cash or prepaid cards to protect their identities. To protect their customers and themselves, some credit card companies are switching to security chips, which are more secure than the magnetic strips currently common in the U.S., and are cautioning customers to check their accounts for suspicious activity.

### **Survey Methods**

Results for this Gallup poll are based on telephone interviews conducted Oct. 12-15, 2014, with a random sample of 1,017 adults, aged 18 and older, living in all 50 U.S. states and the District of Columbia.

For results based on the total sample of national adults, the margin of sampling error is  $\pm 4$  percentage points at the 95% confidence level.

Each sample of national adults includes a minimum quota of 50% cellphone respondents and 50% landline respondents, with additional minimum quotas by time zone within region. Landline and cellular telephone numbers are selected using random-digit-dial methods.


[View survey methodology, complete question responses, and trends.](#)

Learn more about how the [Gallup Poll Social Series](#) works.

RELEASE DATE: October 27, 2014

SOURCE: Gallup <http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx>

CONTACT: Gallup World Headquarters, 901 F Street, Washington, D.C., 20001, U.S.A

+1 202.715.3030 

---

Copyright © 2016 Gallup, Inc. All rights reserved.

Gallup, Inc. maintains several registered and unregistered trademarks that include but may not be limited to: A8, Accountability Index, Business Impact Analysis, BE10, CE11, CE11 Accelerator, Clifton StrengthsExplorer, Clifton StrengthsFinder, Customer Engagement Index, Customer Engagement Management, Dr. Gallup Portrait, Employee Engagement Index, Enetrrix, Engagement Creation Index, Follow This Path, Gallup, Gallup Brain, Gallup Business Journal, GBJ, Gallup Consulting, Gallup-Healthways Well-Being Index, Gallup Management Journal, GMJ, Gallup Panel, Gallup Press, Gallup Tuesday Briefing, Gallup University, Gallup World News, HumanSigma, HumanSigma Accelerator, ICE11, I10, L3, ME25, NurseInsight, NurseStrengths, Patient Quality System, Performance Optimization, Power of 2, PrincipallInsight, Q12, Q12 Accelerator, Q12 Advantage, Selection Research, Inc., SE25, SF34, SRI, Soul of the City, Strengths Spotlight, Strengths-Based Selling, StatShot, StrengthsCoach, StrengthsExplorer, StrengthsFinder, StrengthsInsight, StrengthsQuest, SupportInsight, TX(R+E+R)=P3, TeacherInsight, The Gallup Path, The Gallup Poll, The Gallup School, VantagePoint, Varsity Management, Wellbeing Finder, Achiever, Activator, Adaptability, Analytical, Arranger, Belief, Command, Communication, Competition, Connectedness, Consistency, Context, Deliberative, Developer, Discipline, Empathy, Fairness, Focus, Futuristic, Harmony, Ideation, Includer, Individualization, Input, Intellection, Learner, Maximizer, Positivity, Relator, Responsibility, Restorative, Self-Assurance, Significance, Strategic, and Woo. All other trademarks are the property of their respective owners. These materials are provided for noncommercial, personal use only. Reproduction prohibited without the express permission of Gallup, Inc.







# **Exhibit E**

# THEWORLDPOST

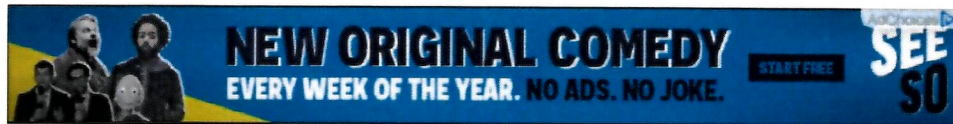
A PARTNERSHIP OF THE HUFFINGTON POST AND BERGGRUEN INSTITUTE

Edition: US ▾

Like 6.2M

Follow

US EDITION INDIA BRASIL U.K. MAGHREB JAPAN DEUTSCHLAND CANADA KOREA FRANCE ESPANA ALL SECTIONS



AdChoices ▶

## 'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions

01/24/2014 05:01 pm ET | Updated Jan 24, 2014

1.1K



Gerry Smith  
Technology reporter, The Huffington Post



ASSOCIATED PRESS

Election officials in India canceled a deal with Google to improve voter registration. In China, sales of Cisco routers dropped 10 percent in a recent quarter. European regulators threatened to block AT&T's purchase of the wireless provider Vodafone.

The technology industry is being roiled by the so-called Snowden Effect, as disclosures by former National Security Agency contractor Edward Snowden about the extent of American spying worldwide prompt companies to avoid doing business with U.S. firms. The recent setbacks for Google, Cisco and AT&T overseas have been attributed, in part, to the international outcry over the companies' role in the NSA scandal.

TAKE THE GOP  
PRESIDENTIAL  
STRAW POLL

VOTE NOW

GOP.COM

PAID FOR BY THE REPUBLICAN NATIONAL COMMITTEE. NOT AUTHORIZED BY ANY CANDIDATE OR CANDIDATE'S COMMITTEE. WWW.GOP.COM

AdChoices ▶

FOLLOW HUFFPOST

Empty input field for following Huffington Post.

Fred Cate, a law professor at Indiana University, said criticism over Silicon Valley's involvement in the government surveillance program was initially limited to European politicians "taking advantage of this moment to beat up on the U.S."

"But the reports from the industry are showing that it is more than that," he added. "This is more than just a flash in the pan. This is really starting to hurt."

The impact of the Snowden leaks could threaten the future architecture of the modern Internet. In recent years, computing power has shifted from individual PCs to the so-called cloud -- massive servers that allow people to access their files from anywhere.

The Snowden revelations undermined trust in U.S.-based cloud services by revealing how some of the largest American tech companies using cloud computing -- including Google and Yahoo -- had their data accessed by the NSA. About 10 percent of non-U.S. companies have canceled contracts with American cloud providers since the NSA spying program was disclosed, according to [a survey by the Cloud Security Alliance](#), an industry group.

U.S. cloud providers could lose as much as \$35 billion over the next three years as fears over U.S. government surveillance prompt foreign customers to transfer their data to cloud companies in other countries, [according to a study by the Information Technology and Innovation Foundation](#), a nonpartisan think tank based in Washington, D.C.

"If European cloud customers cannot trust the United States government, then maybe they won't trust U.S. cloud providers either," Neelie Kroes, European commissioner for digital affairs, [said last summer](#) after the NSA revelations were made public. "If I am right, there are multibillion-euro consequences for American companies. If I were an American cloud provider, I would be quite frustrated with my government right now."

European officials and companies have been especially troubled by the Snowden leaks because European privacy laws are more stringent than those in the United States.

After documents from Snowden [revealed](#) that the NSA had tapped German Chancellor Angela Merkel's phone calls, she said Europeans should [promote domestic Internet companies](#) over American ones in order to avoid U.S. surveillance. German Interior Minister Hans-Peter Friedrich [has suggested](#) that people who are worried about government spying should stop using Google and Facebook altogether.

"Whoever fears their communication is being intercepted in any way should use services that don't go through American servers," Friedrich said after Snowden leaked the NSA documents.

Chris Lamoureux, the executive vice president of the company Veriday, told The WorldPost that some of his customers have requested that the company avoid storing their information in U.S.-based data centers, hoping to make it more difficult for the NSA to gain access.



HuffPost Like 6.2M

WorldPost Like 740K

### HUFFPOST NEWSLETTERS

Get top stories and blog posts emailed to me each day. Newsletters may offer personalized content or advertisements. [Learn More.](#)

### SUGGESTED FOR YOU

?

- 1. [Obama Showed Us How To Take Down Donald Trump 5 Years Ago, And The Video Is Just As Brutal Today](#)



2 days ago [huffingtonpost.com NationalJournal.com Ryan Grim](#) Ryan Grim obama

- 2. [Trump Supporter Has The Best Reason For Why The GOP Front-runner Hasn't Offered Specific Policies](#)



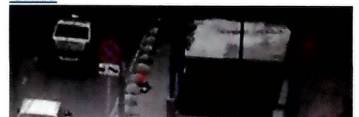
a day ago [huffingtonpost.com Wow.com Sam Levine](#) Sam Levine elections 2016

- 3. [San Francisco Hippies Prepare To Make Canada Great Again If Trump Wins](#)



a day ago [huffingtonpost.com NationalJournal.com Jennifer Bendery](#) Jennifer Bendery elections 2016

- 4. [Moscow Police Arrest Woman Carrying Decapitated Head Of Young Child](#)





"They've said, 'We don't want you to put our data in the U.S. because we're worried about what we're seeing and hearing over there right now,'" said Lamoureux, whose Ottawa-based company develops web applications for banks, governments and retailers.

Some argue that President Barack Obama has added to the tech industry's troubles abroad by emphasizing how the NSA surveillance program focused on people outside the United States, where most of Silicon Valley's customers are located.

"Those customers, as well as foreign regulatory agencies like those in the European Union, were being led to believe that using US-based services meant giving their data directly to the NSA," journalist Steven Levy wrote in a recent article in Wired magazine.

Hoping to reassure overseas customers, major tech companies (including AOL, which owns The Huffington Post Media Group) have asked the Obama administration for permission to be more open about how they responded to past requests for data from the U.S. government. They argue the government snooped on their networks without their knowledge. Recent reports based on documents provided by Snowden revealed that the NSA spied on Google and Yahoo customers, unbeknownst to the companies, by secretly tapping cables that connect data centers around the world.

"The impression is that the tech industry is in league with the U.S. government," Cate said. "But the industry would like to give the impression that they're victims of the U.S. government, too."

On Wednesday, Microsoft said it would offer customers who are wary about NSA surveillance the ability to store their data outside the United States.

Meanwhile, some foreign tech companies are trying to capitalize on the distrust between U.S. tech firms and their customers around the world. Swisscom, a cloud provider in Switzerland, is developing a service that would attract customers looking to store data under the country's strict privacy laws and away "from the prying eyes of foreign intelligence services," Reuters reported.

Germany's three largest email providers have also created a new service, called "Email Made in Germany," designed to thwart the NSA by encrypting messages through servers located within the country, The Wall Street Journal reported.

But Cate said that any businesses that try to avoid surveillance by boycotting U.S. tech companies are not really protecting their data from the NSA. After all, intelligence agencies in France and Spain also spied on their own citizens, and passed on that information to the NSA, according to documents from Snowden.

"It doesn't make a difference what you do with your data -- the NSA is going break into it," Cate said. "But that doesn't mean U.S. industry isn't going to get hurt along the way."

MORE: NSA, Edward Snowden, Smarter Ideas, National Security Agency, Edward Snowden Nsa

## FOLLOW WORLDPOST

[Suggest a correction](#)



GET THE NEWSLETTER

Subscribe!

### YOU MAY LIKE

Sponsored Links by Taboola

**Your 401(k) Isn't Growing as Fast as It Should - Here's Why**  
Mint | Future Advisor

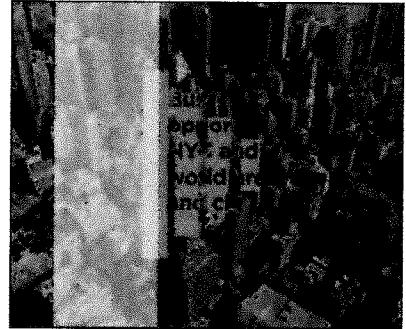
**Forget The iPhone 7. Next Apple Sensation Leaked**  
The Motley Fool

**How To Watch 500+ Hours of Quality, Ad-Free Documentaries**  
Mashable | Curiosity Stream

**The Top 6 Reasons Kate Hudson's New Activewear Is A Game Changer**  
Fabletics

**This Is Why You Don't Mess With The US! Watch What Happens**  
HolyHorsepower

**Librarians Love It - The One Website Book Lovers Need to Know**  
BookBub



AdChoices

## CONVERSATIONS

0 Comments

Sort by



Add a comment...

Facebook Comments Plugin

[Advertise](#) [User Agreement](#) [Privacy](#) [Comment Policy](#) [About Us](#) [About Our Ads](#) [Contact Us](#) [FAQ](#)

Copyright © 2016 TheHuffingtonPost.com, Inc. | "The Huffington Post" is a registered trademark of TheHuffingtonPost.com, Inc. All rights reserved.

Part of HuffPost on HPMG News





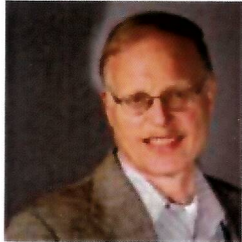
# **Exhibit F**

# InformationWeek

CONNECTING THE BUSINESS  
TECHNOLOGY COMMUNITY

NEWS

8/14/2013  
07:47 PM



Charles Babcock

News

Connect Directly



10 COMMENTS

COMMENT NOW

Tweet



32

G+1

19

RELATED EVENTS

**The Analytics Job and Salary Outlook for 2016**

Jan 28, 2016

With data science and big data top-of-mind for all types of organizations, hiring analytics profes ...[Read More>>](#)

RELATED CONTENT

Breaking Through WAN Performance Barriers and Deploying the Right Tools

Top 7 Reasons to Create Agile Business Communications

CrowdStrike Global Threat Intelligence Report

**NSA's Prism Could Cost U.S. Cloud Companies \$45 Billion**

**Losses may total between \$35 billion and \$45 billion in next three years due to lost business stemming from disclosure of NSA monitoring, new research predicts.**



9 Android Apps To Improve Security, Privacy

(click image for larger view)

The revelations about the monitoring of phone calls, emails and Internet traffic by the National Security Agency's Prism program will cost U.S. cloud suppliers either \$35 billion, \$45 billion, or maybe not so much, depending on how you interpret recent data on the continued use of hosting services, according to analysts looking at the aftermath of the Edward Snowden leaks.

The \$35 billion figure springs from a recent survey by the **Cloud Security Alliance**, which found that 56% of 500 respondents said the disclosures by the fugitive NSA systems administrator would cause them to lose non-U.S. business. Canada, plus Germany, France and other European countries, have rules that require companies to guarantee the privacy of data that originates within their borders. Most comply by keeping the data on storage inside its country of origin.

Daniel Castro, an analyst at the Information Technology and Innovation Institute, a technology think tank, used that figure to project that U.S. cloud service suppliers are likely to lose \$22 billion to \$35 billion in business to European rivals over the next three years. The rivalry is already well entrenched, with European governments investing in future competitors of U.S. companies.

Castro reported that Jean-Francois Audenard, the cloud security advisor to France Telecom, "said with no small amount of nationalistic hyperbole, 'It's extremely important to have the governments of Europe take care of this issue. ... If all the data of enterprises is going to be under the control of the U.S., it's not really good for the future of the European people.'" France recently invested 135 million Euros in a joint cloud venture with French business.

**[ What can you learn from the NSA? See The NSA And Big Data: What IT Can Learn. ]**

The losses by U.S. companies could be greater, concluded James Staten, lead cloud analyst at Forrester Research, after reviewing Castro's report. Castro's analysis looked only at the business that might be withdrawn from U.S. providers by foreign companies and concluded that 20% of that business was at risk of going away regardless of security questions. Staten said some cloud users in the U.S. will also have to bypass U.S. cloud providers and move part of their business overseas to satisfy their international units and customers. That would add \$10 billion to Castro's total, he said.

"European Union rules require data about EU citizens be stored and retained in the EU ... so seeking an EU-based cloud provider or non-cloud IT provider would be a prudent tactic for a U.S. business," Staten noted in a **lengthy blog post** dated Aug. 14.

Staten wrote that Neelie Kroes, European Commissioner for Digital Affairs, summarized the problem: "If European cloud customers cannot trust the United States government, then maybe they won't trust U.S. cloud providers either. ... If I were an American cloud provider, I would be quite frustrated with my government right now." Between now and 2020, the consequences may be a shift in billions of dollars worth of business away from American suppliers to European suppliers, Kroes predicted.

The data privacy rules don't only apply in European countries. Canada has strict requirements on its citizen's medical records. Since the U.S. Patriot Act was passed, Canada has forbidden medical information on its citizens to be stored on U.S. servers. It's unlikely that concern would be eased by the Snowden revelations.

Pat O'Day, co-founder of the VMware-compatible cloud service, Bluelock, said there are many VMware customers in Canada that have an interest in a cloud supplier for backup and recovery purposes. Bluelock offers such a service, geared to work with the VMware product set. But he finds Toronto customers moving their data across the continent to suppliers in Vancouver "just to keep it on the north side of the border," rather than turn to a closer provider in Indianapolis.

"Both data and IP concerns were already driving decision-making behavior for our northern neighbors due to the Patriot Act. But the recent NSA situation is unfortunately underscoring and exacerbating the issue," O'Day said in an email.

Staten pointed out that the U.S. isn't the only country conducting government surveillance of traffic flowing through Facebook, Google, Microsoft, Yahoo, Apple and other big Internet-based services -- but it's the only one in the news. Germany has its own equivalent to the NSA, the BND, but little is known about what its surveillance practices are. The U.K. maintains a strong surveillance system



over public transit and city centers and is likely to have one over its Internet pathways as well. India reportedly mounts its own electronic watch against potential intruders and terrorists.

Staten said the fallout from the Prism news on U.S. companies is likely to be "particularly acute because cloud computing is a rapidly growing industry. This means that cloud computing vendors not only have to retain existing customers, they must actively recruit new customers to retain market share."

Global spending on the cloud will grow 100% between 2012 and 2016. The global IT market is growing 3%, he pointed out. "If U.S. companies lose market share in the short term, this will have long-term implications on their competitive advantage in this new industry," he concluded.

But it may be too soon to estimate the long term effects of Snowden's revelations and subsequent flight to Hong Kong and Russia. Data Center Knowledge, a news site devoted to the latest data center technology, pointed to a survey by Netcraft, a U.K. firm that tracks Internet servers. It found the number of websites hosted in the U.S. from overseas has grown since the Snowden disclosures. In the month of July, 3.6 million websites left the U.S. to hosts overseas. That sounds like a large number, but about 3.9 million moved into the U.S. from other countries, for a net gain of 270,000 additional sites.

Germany, with its strict rules on data privacy, was the most popular point of departure for websites moving to the U.S. "Nearly 1.2 million sites moved from German hosting companies. This was followed by Canada, where 803,000 sites hopped across the border to the US," Netcraft reported.

"Netcraft's monthly Web Server Survey suggests that if multi-national customers have concerns about being hosted in the U.S., they're not acting on them -- at least not yet," wrote Data Center Knowledge editor in chief Rich Miller.

Netcraft also reported that of the 10,000 most popular websites in the world, 40 had moved away from the U.S. since the Snowden revelations. But 47 moved into the U.S., leaving the U.S. with a net gain of seven.

It may take more than 30 days for major cloud customers to decide to move their business, or the sensitive parts of their business, away from U.S. providers. The Netcraft Web server and website data is one indicator. But Netcraft doesn't look down into the repositories of business data, customer data and international patient data that may in fact be starting an outward migration, one that will make Staten's projection of a \$45 billion loss by 2016 a reality.

Staten and others agree with the ITIF recommendation that the U.S. must state what data it has access to and the rules that govern that access. It must also establish a judicial check on what security agencies may do to obtain data.

He also recommended that the U.S. lobby other nations at the next G30 economic summit to jointly draft "international surveillance transparency rules that will take any potential chill off the burgeoning cloud computing market."

COMMENT | EMAIL THIS | PRINT | RSS

#### **MORE INSIGHTS**

##### **Webcasts**

BYOD: And it's impact on your bottom line





The Analytics Job and Salary Outlook for 2016

**MORE WEBCASTS**

**White Papers**

Breaking Through WAN Performance Barriers and Deploying the Right Tools  
Top 7 Reasons to Create Agile Business Communications

**MORE WHITE PAPERS**

**Reports**

[Survey Report] The Value of Threat Intelligence in Protecting against Cybercrime  
The Forrester Wave: Web Content Management Systems, Q1 2015

**MORE REPORTS**

Copyright © 2016 UBM Electronics, A UBM company, All rights reserved. Privacy Policy | Terms of Service



# **Exhibit G**

**Testimony for  
House Judiciary Committee Hearing on  
“The Encryption Tightrope: Balancing Americans’ Security and Privacy”  
March 1, 2016**

**Susan Landau, PhD  
Professor of Cybersecurity Policy  
Worcester Polytechnic Institute  
100 Institute Road  
Worcester MA 01609**

Testimony for  
House Judiciary Committee Hearing on  
“The Encryption Tightrope: Balancing Americans’ Security and Privacy”  
March 1, 2016

Mr. Chairman and Members of the Committee:

Thank you very much for the opportunity to testify today on “The Encryption Tightrope: Balancing Americans’ Security and Privacy.” My name is Susan Landau, and I am professor of cybersecurity policy at Worcester Polytechnic Institute. I have previously been a Senior Staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems. I am the author of two books on the issues of today’s hearing: *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) and *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998); the latter is co-authored with Whitfield Diffie. I have written about these issues in the *Washington Post*, the *Chicago Tribune*, *Scientific American*, and other venues. I am a Fellow of the Association for Computing Machinery and of the American Association for the Advancement of Science, and I was recently inducted into the Cybersecurity Hall of Fame.<sup>1</sup>

My comments represent my own views and not those of the institutions with which I am affiliated.

Today I will speak on security threats, encryption, and securing smartphones.

It would seem to be a fairly straightforward issue: the smartphone of one of the two San Bernardino terrorists had its data encrypted. Because Apple designed the phone to be secure—and to destroy its data if there were ten incorrect tries of the PIN to unlock it—the FBI cannot unlock the smartphone (or at least cannot without risking destroying the data). The court has ordered Apple to create a phone update that

---

<sup>1</sup> Additional biographical information relevant to the subject matter to the hearing: I am also a Visiting Professor of Computer Science at University College London. For over two decades I have been studying encryption policy and the risks that occur when wiretapping capabilities are embedded in communications infrastructures. At Sun I was involved in issues related to cryptography and export control, security and privacy of federated identity management systems, and in developing our policy stance in digital rights management. I serve on the National Research Council Computer Science and Telecommunications Board, and recently participated in an Academies study on *Bulk Signals Intelligence Collection: Technical Alternatives* (2015). I have served on the advisory committee for the National Science Foundation’s Directorate for Computer and Information Science and Engineering (2009-2012), the Commission on Cyber Security for the 44th Presidency (2009-2011), and the National Institute of Standards and Technology’s Information Security and Privacy Advisory Board (2002-2008). I hold a PhD in applied math/theoretical computer science from MIT.



will undo this and other security aspects of the software, thus enabling the FBI to brute force the key to reveal whatever information is on the phone.

But little in cyber is straightforward. Despite appearances, this is not a simple story of national security versus privacy. It is, in fact, a security versus security story although there are, of course, aspects of privacy embedded in it as well.

The way we use our phones is very different than a decade ago; they are, as the Supreme Court observed in *Riley v. California*,<sup>2</sup> “minicomputers that also happen to have the capacity to be used as a telephone. [The phones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers’.” Smartphones are already holders of account information (financial and otherwise), and are poised to become authenticators to a wide variety of services we access via the Internet.

And that is why we have a security versus security story. The Internet has brought huge benefits, but it has also vastly simplified attacks and exploits.<sup>3</sup> Cyberespionage netted Chinese military a “huge amount of design and electronics data on the F-35,”<sup>4</sup> Russian intrusions<sup>5</sup> into law firms<sup>6</sup> (the target here likely to be patent filings), an Iranian hacker probing US critical infrastructure (with possible intent to attack)<sup>7</sup> are examples. Each day brings more news of such attacks and exploits.

The cyberexploitation of US companies, in which attackers from overseas have reaped vast amounts of intellectual property, threatens the US economic strength. In the last decade, the United States has been under an unprecedented attack, one that NSA Director Keith Alexander has called “the greatest transfer of wealth in history.”<sup>8</sup>

---

<sup>2</sup> 134 S. Ct. 2473 (2014).

<sup>3</sup> It might be hard to understand why a network on which society has become so dependent is so insecure. The short answer is history. The ARPANet, the precursor to the Internet, began as a research network on which everyone was a trusted partner. When the NSFnet, the follow-on network to the ARPANet, was opened up to commercial traffic, it relied on the same protocols. These assumed a trusted user body, which was not really sensible for a network that would support financial transactions, manage critical infrastructure, and the like.

<sup>4</sup> David Alexander, “Theft of F-35 design data is helping US adversaries—Pentagon,” *Reuters*, June 19, 2013.

<sup>5</sup> Director of National Intelligence James Clapper views Russia as the top cyber threat. See, e.g., Siobhan Gorman, “Intel Chief: Russia Tops China as Cyber Threat,” *Wall Street Journal*, October 17, 2014.

<sup>6</sup> Mandiant Consulting, “M-Trends 2016: Special Report,” p. 45, <https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf>

<sup>7</sup> Stephanie Gosk, Tom Winter, and Tracy Connor, “Iranian Hackers Claim Cyber Attack on US Dam,” NBC News, December 23, 2015.

<sup>8</sup> Josh Rogin, “NSA Chief: Cybercrime constitutes ‘greatest transfer of wealth in history’,” *The Cable*, July 9, 2012.

Stealing your login credentials provides criminals and nation states the most effective way into your system—and a smartphone provides one of the best ways of securing ourselves.

That's why Apple's approach to securing phone data is so crucial.

But law enforcement continues to see electronic surveillance in twentieth century terms, and it is using twentieth-century investigative thinking in a twenty-first century world. Instead of celebrating steps industry takes to provide security to data and communications, the FBI fights it.

I should note that this response is different from NSA's, which over the last two decades, has, despite public perception, both encouraged and aided industry's efforts in securing communications.<sup>9</sup>

Instead of embracing the communications and device security we so badly need for securing US public and private data, law enforcement continues to press hard to undermine security in the misguided desire to preserve simple, but outdated, investigative techniques.

There is another way. Law enforcement should embrace the protections that industry is implementing to secure private—and, because of wide adoption, also government—sector data and develop substantive advanced capabilities to conduct investigations when needed. In the late 1990s, the NSA faced similar challenges and overcame them.<sup>10</sup>

We need twenty-first century technologies to secure the data that twenty-first century enemies—organized crime and nation-state attackers—seek to steal and exploit. Twentieth century approaches that provide law enforcement with the ability to investigate but also simplify exploitations and attacks are not in our national-security interest.<sup>11</sup> Instead of laws and regulations that weaken our protections, we should enable law enforcement to develop twenty-first century capabilities for conducting investigations.

Now I should note that the FBI already has some excellent capabilities in this area. But FBI investment and capacity in this area is not at the scale and level necessary to be as effective as it needs to be.

---

<sup>9</sup> This is true despite the fact that the NSA has also sought to undermine some protections; see later in this testimony as well as Susan Landau "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy*, Vol. 7, No. 3 (2014).

<sup>10</sup> See, e.g., Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6, 1999.

<sup>11</sup> For a humorous take on these issues, see The Strip, *New York Times*, February 28, 2016, <http://www.nytimes.com/slideshow/2012/07/08/opinion/sunday/the-strip.html#1>

That's where Congress can help. Law enforcement must develop the capability for conducting such investigations themselves (or through a combination of in house and carefully managed contracting). Though there have been nascent steps in this direction by law enforcement, a much larger and complete effort is needed. Help the FBI build such capabilities, determine the most efficient and effective way that such capabilities can be utilized by state and local law enforcement, and fund it.

This is the way forward that does not put our national security at risk. It enables law enforcement investigations while encouraging industry to do all it can to develop better, more effective technologies for securing data and devices. This is a win/win, and where we should be going.

The rest of my testimony presents details of these concerns. Thank you very much for the opportunity to address you on this critical national-security topic.

### **Understanding our Security Threat**

When terrorists wearing tactical gear and black masks and armed with guns and bombs attack a concert hall or Christmas party, our immediate emotional reaction is that we must move heaven and earth to prevent future such attacks. The role of leadership includes making choices. Here we are faced with a situation where logic and analysis lead to a different calculus on safety and security than do emotions. So while FBI Director James Comey has argued that, "We could not look the survivors in the eye if we did not follow this lead,"<sup>12</sup> this view is a mistaken view of where our most serious risks as a nation lie. Page one of the 2016 Department of Defense Threat Assessment states: "Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems."<sup>13</sup>

This is why securing communications and devices is so very crucial, and it is where the situation grows complicated. Despite our deeply human tendency to react to the attack that is occurring right now, we must focus and analyze to determine what our most dangerous threats are. This can be difficult. Yet measured, carefully considered responses will be what secures this nation and its people.

In the last decade, the United States has been under an unprecedented attack. . In 2010, Department of Defense Deputy Under Secretary William Lynn said the theft of US intellectual property "may be the most significant cyberthreat that the United

---

<sup>12</sup> Lawfareblog, February 21, 2016, <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>.

<sup>13</sup> James Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," February 9, 2016, p. 1.

States will face over the long term.”<sup>14</sup> The cyberexploitation of US companies, in which attackers from overseas have reaped vast amounts of intellectual property, threatens the US economic strength. Make no mistake about it: this is an extremely serious national-security threat.

Protecting US intellectual property is critical for US economic and national security. In a July 2015 *Washington Post* op-ed, former NSA Director Mike McConnell, former DHS Secretary Michael Chertoff, 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.”<sup>15</sup>

Messers Chertoff, McConnell, and Lynn concluded that the security provided by encrypted communications was more important than the difficulties encryption present to law enforcement.

As the Court noted in *Riley*,<sup>16</sup> the smartphones in our pockets are computers. They are, in fact, the most common device for accessing the network. So the cybersecurity threat applies as much to smartphones as it does to laptops, servers, and anything in between.

## Securing Society

I'd like to turn now to encryption. I alluded earlier to NSA's efforts over the last two decades to secure private-sector telecommunications. Let me now present some detail.

Since the mid 1990s the NSA has actively been promoting the use of encryption in the private sector. This began with a 1995 incident in which NSA helped private-sector adoption of a new, more efficient cryptographic algorithm for securing low-powered, small devices.<sup>17</sup>

---

<sup>14</sup> William J. Lynn III, “Defending a New Domain,” *Foreign Affairs*, September/October 2010.

<sup>15</sup> Mike McConnell, Michael Chertoff, and William Lynn, “Why the fear over ubiquitous data encryption is overblown,” *Washington Post*, July 28, 2015.

<sup>16</sup> 134 S. Ct. 2473 (2014).

<sup>17</sup> An NSA representative present at an ANSI standards meeting spoke up to note that a new public-key cryptographic algorithm, whose security had been sharply questioned by the current provider of such algorithms, was in fact, secure. He said that it was sufficiently secure that the US government was adopting it for communications among all U.S. government agencies, including the Federal



NSA participated in the Advanced Encryption Standards (AES) effort by vetting submitted proposals. This algorithm was chosen through an international effort run by the National Institute of Standards and Technology, and is an extremely strong system. In November 2001, two months after the attacks of September 11<sup>th</sup>, NSA concurred in the approval of AES as a Federal Information Processing Standard (FIPS). Designation as a FIPS means an algorithm or protocol must be in systems sold to the U.S. government or contractors; such a designation increases industry and international acceptance.

A year and a half later, the NSA approved the use of AES to protect classified information as long as it was in an NSA-certified implementation.<sup>18</sup> The decision had great impact, for it vastly increases the market for products running the algorithm, thus ensuring wider availability for non-classified users as well. From there the NSA went on to approve a set of publicly available algorithms for securing a network.<sup>19</sup>

Why would the NSA go to such great efforts to support the deployment of strong cryptography in the private sector? Since the mid 1990s the Department of Defense (DoD) has relied on Commercial Off the Shelf (COTS) products for DoD communications and computer equipment. Use of COTS is required by law, but it is also good security practice.<sup>20</sup> The speed of innovation by industry means that DoD must use COTS products in order to be cutting edge. iPhones and iPads have been cleared for DoD use since 2013.<sup>21</sup>

This is not to say every soldier must carry a locked iPhone, but rather, on balance, the US government has had much to gain from the security improvements of private-sector communications technologies. It is thus no surprise that the NSA supported many of these, including the widespread use of strong encryption technologies.

---

Reserve. The result was that the algorithm was approved, and is now widely used. It was the first time anyone could recall the NSA endorsing a private-sector system in this way. See Ann Hibner Koblitz, Neal Koblitz & Alfred Menezes, "Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift," *Journal of Number Theory*, Vol. 131 (2011), pp. 781-814.

<sup>18</sup> Committee on National Security Systems, National Security Agency, Policy No. 15, Fact Sheet No. Sheet No. 1, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, 2003.

<sup>19</sup> Center for Secure Services, Information Assurance Directorate, National Security Agency, Suite B Algorithms, [http://www.nsa.gov/ia/programs/suiteb\\_cryptography/](http://www.nsa.gov/ia/programs/suiteb_cryptography/) (accessed by searching the archived copy of an older version of the website, available at: <http://archive.today/mFaN>)

<sup>20</sup> The Clinger-Cohen Act requires that DoD purchases of information technology use COTS whenever possible. See, more generally, Susan Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy*, Vol. 7, No. 3 (2014).

<sup>21</sup> Defense Information Systems Agency, "DISA Approves STIG for Government-Issued Apple iOS 6 Mobile Devices," May 17, 2013, <http://www.disa.mil/News/PressResources/2013/STIG-Apple>

## Are We “Going Dark”?

Our hearing concerns whether the wiretapping world is actually “going dark.” And here the story does not appear to be quite the way the FBI sees it. For although the FBI has been expressing great concern since the early 1990s that encryption would prevent law enforcement from wiretapping,<sup>22</sup> the sky has apparently not fallen—at least for the NSA.

In the wake of the San Bernardino shootings, the *Washington Post* reported that,

Mike McConnell, who headed the NSA in the 1990s during the first national debate over federal encryption policy, recalled how 20 years ago, he was for back-door access to encrypted communications for the government.

“NSA argued publicly, ‘We’re going deaf’ because of encrypted calls, said McConnell, who now serves on the board of several cybersecurity companies. The agency wanted a third party to hold a key to unlock coded calls. But the resulting outcry — similar to the one heard in today’s debate over smartphone and text message encryption — caused the government to back down.

“We lost,” McConnell said simply. And what happened? “From that time until now, NSA has had better ‘sigint’ than any time in history,” he said.<sup>23</sup>

Nor is Director McConnell an outlier in this view. In the same article, former NSA Director Michael Hayden<sup>24</sup> was quoted as saying that, “this is far more of a law enforcement issue than it is intelligence.”<sup>25</sup> Hayden noted, “I’m not saying that NSA should not try to bust what Apple thinks is unbreakable encryption. All I’m saying is Apple should not be required” [to hold keys to decrypt data for the government].<sup>26</sup>

Now it is not surprising that some of the ex-NSA directors might hold this opinion. The NSA has two roles: signals intelligence and information assurance. The NSA has grown more concerned about the latter as the theft of US IP has reached

---

<sup>22</sup> In 1992 the FBI’s Advanced Telephony Unit warned that within three years Title III wiretaps would no longer work: at least 40% would be intelligible and in the worst case all might be rendered useless (Advanced Telephony Unit, Federal Bureau of Investigation, “Telecommunications Overview, slide on Encryption Equipment,” 1992. FOIAed document available at <https://www.cs.columbia.edu/~smb/Telecommunications Overview 1992.pdf>).

<sup>23</sup> Ellen Nakashima, “Former national security officials urge government to embrace rise of encryption,” *Washington Post*, December 15, 2015.

<sup>24</sup> Director Michael Hayden was, also, of course Director of the CIA.

<sup>25</sup> Nakashima, “Former national security officials urge government to embrace rise of encryption,” *Ibid.*

<sup>26</sup> *Ibid.*



astronomical levels. The FBI continues to remain focused on investigations rather than prevention—a very serious mistake, in my opinion.

The other reason for the split, of course, is that the NSA has far more resources and capabilities for conducting signals intelligence than law enforcement has. But that is exactly the point. In a technological world in which virtually every crime has a cyber component, the FBI needs technical expertise; it needs vastly more technical expertise than it has at present.

### **The Role of Smartphones**

Not so long ago everyone in an important job with confidential information carried a Blackberry. This was the communication device of choice for those in high positions in government and the corporate world. Unlike the recent iPhones and Androids, Research in Motion, the manufacturer of Blackberrys, enables the phone's owner (the corporation for whom the user works) to have access to the unencrypted text of communications. If Syed Farook had been carrying a Blackberry,<sup>27</sup> there wouldn't be a break-into-the-phone issue.

But in the last decade Blackberrys lost popularity, losing the market to iPhones and Androids (that's because apps drive the smartphone business). Most people don't like to carry two devices. So instead of a Blackberry *and* an iPhone or Android, consumers choose to use a single consumer device for *all* their communications—and it happens to be a personal one. (Of course, that's not true for everyone. I am sure that many on this committee do carry two devices, one for government work, one for their personal stuff. People who work in the Department of Defense, or for defense contractors, the financial or other industries where keeping proprietary work data secure is crucial, may carry two devices.)

As a society we have largely moved to a world of BYOD (Bring Your Own Device) to work. And what that means is not only is your personal stuff—your notes and calendars and contacts—on your smartphone, so is proprietary information from work. And so access to US intellectual property lies not only on corporate servers —

---

<sup>27</sup> If the FBI had not asked the San Bernardino Health Department to reset the password on the phone's iCloud account, there would not be a break-into-the-phone issue (Paresh Dave, "Apple and feds reveal San Bernardino's iCloud password was reset hours after the attack," *Los Angeles Times*, February 19, 2016). It is also the case that if the San Bernardino Health Department had installed "Mobile Device Management" on the phone it gave to Farook, there would not be a break-into-the-phone issue. (Tami Abdollah, "Apple CEO: Feds Should Withdraw Demand for iPhone Hack Help," ABC News, February 22, 2016, <http://abcnews.go.com/Technology/wireStory/basic-software-held-key-shooters-iphone-unused-37106947>)

which may or may not be well protected — but on millions of private communication devices.

Smartphones bear little relation to the simple rotary dial devices that once sat on hallway tables. Not only are smartphones the recipients of “our photos, our music, our notes, our calendars and contacts,”<sup>28</sup> much of it sensitive data (this is often especially true of photos). Our smartphones are used for conducting transactions of monetary value— ordering and paying for Uber rides and extra moves on Candy Crush, transferring balances between bank accounts, etc. People are also increasingly using their personal smartphones for business, and as a result, these smartphones store important proprietary information.

Smartphones are increasingly becoming wallets, providing access to accounts (not only financial, but also various online accounts, such as Dropbox), and storing emails and notes, including ones from meetings or design drawings and the like. For many people their personal smartphone acts as a convenient temporary repository for proprietary work information, information they know they ought to protect but rarely do as carefully as they ought. There are other ways of using phones for authentication; these rely on the device’s security.”

These smartphones are also used for authentication, that is, as a form of authentication to a device, an account, etc. And that means that the authentication information itself must be highly secured. Otherwise people in possession of the phone and with access to the data on it can break into other accounts. In short, smartphones are rapidly becoming a data repository of highly sensitive information, information that must be secured.

Thus Apple’s secure by default provides an important improvement in security.

### **Smartphones and Long-Term Strategies for Security**

Data theft through the Internet began three decades ago, starting with break-ins into military sites and the Defense Industrial Base.<sup>29</sup> As US companies began connecting their systems to the Internet, they, too, became targets. The scale of cyberexploitation (data theft through networked systems) is what matters here. That scale is huge, and greatly worries General Alexander, Deputy Secretary Lynn, and many others in our government.

---

<sup>28</sup> Tim Cook, “A Message to Our Customers,” February 16, 2016, <https://www.apple.com/customer-letter/>

<sup>29</sup> See, for example, Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, CCSA Publication, 2013.

In the early days of the network, systems were poorly secured and data exfiltration was often the work of unsophisticated hackers. While aspects of that world still exist, the thieves are now far more sophisticated. Virtually every nation has its version of Cyber Command whose purpose includes spying via the network.

How do the spies get in? In a public presentation in January,<sup>30</sup> the Chief of NSA's Tailored Access Operations organization, Rob Joyce, observed that the most valuable data for attackers is your login credentials. Once an attacker has your login credentials—however briefly—he or she can establish a beachhead on your system that they can later use to exfiltrate data.

What has this got to do with securing phones? Everything. Using phones for secure login has the potential to rescue us from much of the mess created by the ease with which login credentials—typically passwords—are stolen. Currently our smartphones are our date books and our wallets, but they are well poised to become our authentication devices.

Smartphones already act as a “second factor” for authentication to accounts (e.g., Gmail); you log onto your email account with a password and an SMS to your phone provides a one-time PIN that you also type in. The security advantage is that someone needs two things to log into your account: your password and the SMS message.<sup>31</sup>

There are tremendous advantages to this approach. First, a smartphone is something you have, which makes it more secure than the “something you know” of a password. (The latter is easily used without your being aware that someone else has the authenticator—while you'd notice quickly that your phone is missing.) As Google explains, “It's an extra layer of security.”<sup>32</sup> And a phone is something you already carry *all the time*, which means you're not carrying an extra device for authentication.

A Michigan start-up, Duo, provides two-factor authentication apps for companies that need fast, easy ways to ensure secure logins for their employees. Facebook is a good example. Its software engineers needed a *very secure* way to log on their development servers to write and submit code. The login process had to be fast—

---

<sup>30</sup> USENIX ENIGMA, <https://www.youtube.com/watch?v=bDJb8WOJYdA>, January 28, 2016.

<sup>31</sup> In fact, someone could intercept the SMS and, if they knew your password, log in instead of you. That would be a relatively highly targeted attack, meaning that Gmail's two-factor authentication system substantially improves on the more frequently used single factor of a password. There are other alternatives, including a “Security Key,” that would be even stronger.

<sup>32</sup> Google, “Stronger Security for Your Google Account,” <https://www.google.com/landing/2step/#tab=how-it-protects>.



and simple; programmers have little patience and will find workarounds if a process is complicated.<sup>33</sup>

There were various potential solutions: time-based tokens, one-time passwords, biometrics, smart cards and public keys. Each had serious problems,<sup>34</sup> and Facebook instead chose the Duo phone-based authentication solution for its developers.

Smartphones are used for security in other ways as well. Some of you have experienced Google's notification system that informs you about logins to your email account that are outside your normal behavior. The "Duo authentication feed" takes this security effort to a new level; it allows you to authenticate a transaction—for example, a login to an account—through a notification on your phone. You can respond while continuing your normal phone activity. This is security with convenience, meaning it is usable and effective security.

New technology means that smartphones are beginning to be used in even more creative ways to provide better security for authentication. This solves the problem that Rob Joyce says is his (and presumably other nations') most valuable way to gain access to your system.

Google is experimenting with a project where you log on by responding to a notification from a smartphone.<sup>35</sup> The holder of the smartphone gets the notification, responds, and then logs on to their account.

The private sector is not the only place using these approaches. Some high-placed agencies within the government are also adopting such solutions (and no, no details are available). Where security matters, authenticating through the device that is always in your pocket and owned by you is a much more secure way to handle your login credentials than the systems we've been using up until now.

If the information on the phone is accessible to Apple, it will be accessible to others—and this promising and important solution to protecting login credentials (which is, by NSA's description the most valuable way to break into systems)—will be ineffective. That's why locking down the data is so crucial for security. Rather than providing us with better security, the FBI's efforts will torpedo it.

---

<sup>33</sup> If only for this reason alone, security must be built in so that trusted but careless programmers don't make it easy to breach a system.

<sup>34</sup> Time-based tokens timed out when a developer was authenticating to two machines at once; one-time passwords had synchronization problems; biometrics are not trustworthy if the user is remote; and the smart card solution had interception problems. See: Facebook's Security Philosophy, and How Duo Helps, <https://duo.com/assets/ebooks/Duo-Security-Facebook-Security-Philosophy.pdf>

<sup>35</sup> Sarah Perez, "Google Begins Experimenting with Password-Free Logins," February 22, 2015, <http://techcrunch.com/2015/12/22/google-begins-testing-password-free-logins/>

## Securing the Smartphones Does Not Prevent Investigations

Even though Apple has engineered excellent security for the iPhone, there are workarounds to access the encrypted data that do not involve Apple creating an update that circumvents its security protections.

If a locked iPhone is brought to a WiFi network it knows, then the phone will automatically sync its contents with Apple's iCloud if the phone is charging and the phone and iCloud passwords match. Unfortunately the San Bernardino Health Department changed the iCloud password on Farook's phone the evening of the attack, and so the mismatching passwords (the ones on the iPhone and iCloud account) eliminated this potential solution. Synchronization won't occur if the passwords for the phone and iCloud account differ. The iCloud password reset was done at the behest of the FBI, which was concerned that someone else might try to access or otherwise affect the phone's iCloud backup.<sup>36</sup>

But there are other solutions.

There are, of course, lots of sites that discuss jailbreaking the phone.<sup>37</sup>

The Chaos Computer Club is a well established group of European hackers that has, for over thirty years, exposed security flaws in well-known systems. Their technical expertise is well respected. They ran a meeting last summer in which they demonstrated physical means, including the use of electron microscopes, to recover the data on security chips. Such techniques may well enable the recovery of the data on the iPhone, and would come cheap (as in well under fifty thousand dollars).

The security in the iPhone stems from the DMA chip, a piece of hardware that can access main memory without going through the CPU. The iPhone DMA is using AES; what the FBI really wants is the key. There are firms that do forensic work in "decapping" chips to expose information on them. Rough estimate of costs are around half a million dollars. I've heard other estimates that come in much lower, say in the one hundred thousand dollar range.

The point is that solutions to accessing the data *already exist within the forensic analysis community.*

There's another way of addressing the issue about whether Apple is impeding an investigation. That's to look at what information might be only be on the phone,

---

<sup>36</sup> Paresh Dave, "Apple and feds reveal San Bernardino's iCloud password was reset hours after the attack," *Los Angeles Times*, February 19, 2016.

<sup>37</sup> Breaking into a locked iPhone would likely require technical skills at the level of a signals-intelligence agency.



keeping in mind that this phone was Farook's work phone and that he and Malik had destroyed their personal phones.

Let's start with what might be only on the smartphone. There are likely to be text messages between Farook and his wife, there might be photos that Farook took of documents or people that might be of interest to the FBI, there might be communications between Farook and some of the Health Department employees he attacked.

Now I understand due diligence, and I especially understand due diligence in a terrorist attack that could conceivably have connections with other potential terrorists. But aside from self-professed statements in support of terrorist organizations, Farook and Malik do not appear to have been communicating with other terrorists. If they had been, the information about whom they are communicating with was available not only on their phones (personal or work), but also at the phone company and/or the ISP. (Farook might have been communicating via iMessage on his work phone. In that case, if the FBI made the request of Apple, they would have gotten iMessage metadata available from Apple servers.<sup>38</sup>) It is, however, extremely unlikely that Farook used his work phone rather than his personal one to conduct the private communications of interest.

Farook's communications with his coworkers are presumably available on their smartphones; one assumes these did not have passwords reset and their contents are accessible. It would thus appear that the only useful information that is potentially on Farook's smartphone is his communications with Malik.

In weighing the FBI request, one has to look at the potential gain and weigh it against the potential cost. In this case, the gain appears to be the possibility of developing a greater understanding of these self-radicalized terrorists.

### **The Security Risks Arising from Apple's Unlocking the Phone**

Beginning with iOS 8, Apple iPhones encrypt by default, that is, all data on the smartphone is automatically encrypted unless the phone is unlocked. The key to unlock the phone data consists of an "entanglement" of the smartphone PIN and a hardware key physically embedded in the device. That means to get at the data, one has to have the phone. Apple's operating system protects the security of the data in other ways as well: with each incorrect guess of the phone PIN, the phone delays the

---

<sup>38</sup> The Manhattan DA report on smartphones notes that "iMessage detail (dates, times, phone numbers involved") does not appear at the phone company (Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, p. 12). That's correct. It is because an iMessage is an IP-based communication that goes through Apple servers.

time until the next guess is allowed. In addition, iOS may wipe the smartphone clean after too many incorrect tries. The system is designed to “protect user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it.”<sup>39</sup>

Farook’s work phone, an iPhone 5c, is an earlier device, but many of these protections are present on it as well. So at the FBI’s request, the Central California District Court ordered Apple to create software that provides the FBI with:

a Software Image File (SIF) that can be loaded onto [Farook’s phone]. The SIF will load and run from Random Access Memory (“RAM”) and will not modify the iOS on the actual phone, the user data partition or system partition on the device’s flash memory. The SIF will be coded by Apple with a unique identifier of the phone so that the SIF would only load and execute on [Farook’s phone]. The SIF will be loaded via Device Firmware Upgrade (“DFU”) mode, recovery mode, or other applicable mode available to the FBI.<sup>40</sup>

The software is to:

by-pass or disable the auto-erase function whether or not it has been enabled, ... enable the FBI to submit passcodes to [Farook’s phone] via the physical device port,<sup>41</sup> ... and ensure that when the FBI submits passcodes to the [phone], software running on the device will not purposefully introduce any additional delay beyond what is incurred by Apple’s hardware.<sup>42</sup>

In other words, the judge was asking Apple to create an Apple-signed device-specific software update tied to Farook’s work phone.<sup>43</sup> The update would enable brute-force testing of PINs without erasing the content of the smartphone.

Let me briefly explain signing. Any complex digital device—a smartphone, a laptop, a thermostat, a car—will need software updates. Such updates are particularly important for patching newly discovered software vulnerabilities, but they have other functions as well. They provide new functionality (which means you don’t need a new phone every six months). They also patch errors (all large software

---

<sup>39</sup> Apple Inc., *iOS Security: iOS 9.0 or Later*, September 2015, p. 4.

<sup>40</sup> United States District Court for the Central District of California, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant of a Black Lexus IS300 California License Plate 35KGD203, No ED15-0451M, Order Compelling Apple to Assist Agents in Search, February 16, 2016, p.2.

<sup>41</sup> This would vastly speed up the time to try different PINs.

<sup>42</sup> Order Compelling Apple to Assist Agents in Search, p.2.

<sup>43</sup> Signing is a cryptographic operation that validates the authenticity of a digital object; in this case, it is that the code came from Apple.

systems have errors). And they keep complex digital systems working as the other systems around them change as they themselves are updated and improved.

In order to assure your device that the smartphone software update is coming from Apple, the company “signs” the update, employing a cryptographic process using information only Apple has. This enables a smartphone (or laptop, thermostat, car, etc.) to know that the update is coming from a legitimate provider and prevents malicious actors from presenting so-called “updates” to your machine that are actually attempts to install malware.

The FBI has argued that there is no security risk in Apple building and signing a device-specific software update tied to Farook’s work phone. The update will be fully under Apple’s control and will be tailored to work only on the smartphone in question.

These statements are both true and incorrect at the same time. That is, the FBI statements that the update will be under Apple’s control and can be tied to work only on Farook’s phone are factually correct. But they miss the point of the risks involved.

The fact is that the software cannot be developed, used, and deleted. Given that the phone’s data may be used in investigations and court cases, the “break-in” software must remain available for examination. The longevity of the update code constitutes the first risk for Apple’s iPhone users.

While the FBI affidavit says this is a one-time use, other cases make that highly unlikely. A November 2015 report from the Manhattan District Attorney’s Office states that, “Between September 17, 2014 and October 1, 2015, the District Attorney’s Office was unable to execute approximately 111 search warrants for smartphones.”<sup>44</sup> Were Apple to develop the code that the FBI is requesting, shortly afterwards the company would be inundated with requests from state and local law enforcement for the same capability.

The frequent use that the code may be expected to have gives rise to the risk that Apple CEO Tim Cook described in a recent Q&A with the Apple employees:

Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the FBI wins this case. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks. Of course Apple would do our best to protect that key, but in a world where all of our data is

---

<sup>44</sup> 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%20Public%20Safety.pdf> p. 9. The 111 phones were all running iOS 8.

under constant threat, *it would be relentlessly attacked by hackers and cybercriminals.*<sup>45</sup> (emphasis added)

At present each OS and firmware update is signed by Apple, enabling an Apple device to recognize the proffered update is approved by Apple and not We-Break-into-You.com. This signing key ensures the integrity of Apple updates, but it seems very likely that US law enforcement will frequently want to search locked iPhones. Each search will be targeted to a particular phone, which means Apple must update the code to include the serial number of the target. Each particularized version of the code will need to be signed by Apple. That's where the risk arises.

Signing code is not technically hard. But a process that happens relatively rarely (e.g., when signing updates to the OS or firmware occur) is very different from the process for an event that occurs routinely (e.g., signing updates to accommodate frequent law-enforcement requests for access to the smartphones). Everyday use of signing updates to unlock smartphones means the signing process must become routinized. Though that doesn't sound like much of an issue, it actually presents a serious problem.

I am concerned that routinizing the signing process will make it too easy to subvert Apple's process and download malware onto customers' devices. My concern is not that the FBI will download rogue software updates onto unsuspecting customers; there is a rigorous wiretap warrant process to prevent government wiretaps from being abused. Rather I am concerned that routinization will make it too easy for a sophisticated enemy, whether organized crime or a nation attempting an Advanced Persistent Threat attack, to mislead the Apple signing process.

A process that is used rarely—such is now the case in signing updates—is a process that can be carefully scrutinized each time it occurs; the chance for malfeasance is low. But make things routine, and instead of several senior people being involved in the signing process, a web form is used, and a low-level employee is placed in charge of code signing. Scrutiny diminishes. No one pays a great deal of attention, and it becomes easy for rogue requests to be slipped into the queue.

All it takes for things to go badly wrong is a bit of neglect in the process or the collaboration of a rogue employee. And if the FBI, CIA, and NSA can suffer from rogue employees, then certainly Apple can as well. A phone that an unfriendly government, a criminal organization, or a business competitor wants to examine receives a signed security update from Apple. This enables the government, criminal group, or competitor to probe the smartphone and read its data when the

---

<sup>45</sup> Matthew Panzarino, "In Employee Email, Apple CEO Tim Cook Calls for Commission on Interaction of Technology and Intelligence Gathering," Techcrunch, February 22, 2016, <http://techcrunch.com/2016/02/22/in-employee-email-apple-ceo-tim-cook-calls-for-commission-on-interaction-of-technology-and-intelligence-gathering/>



smartphone is taken during a customs inspection, a theft, or a meeting in which all electronic devices are kept outside the room.

A different issue is that smartphone owners may begin to distrust the automatic update process. One of the greatest improvements to consumer device security has been automatic security updates, what we in the trade call a “push” instead of a “pull.” Would people stop automatic updates if they were concerned that law enforcement were using the updates as a surreptitious technique to search their devices, not for terrorist activity but, say, for tax fraud?

Using updates that appear to have been signed by the company to deliver malware or surveillance technologies is likely to undermine one of the few success stories of cybersecurity: automatic updates to correct flaws. How many people would stop automatic smartphone updates from Apple if they knew that the update could steal their bank account information? How many people would stop using virus scanners on their PCs if they knew that these programs were sometimes used by law enforcement to spy on their users? If this activity were to cause people to back away from using automatic updates for patching and the like, the impact on security is likely to be disastrous.

Cryptography—and security technologies in general—protect data. Within that obvious statement lies a conundrum for the FBI. It would appear, that in its effort to use all tools to conduct investigations, the FBI has not fully considered the impact of its efforts on technologies that secure data (the lifeblood of the information economy).

There are potentially severe adverse cybersecurity consequences of the FBI approach. Apple has been carefully working to secure the data on customers’ phones. Most security experts consider iOS to be the most secure platform—the last things we should be doing is seeking to weaken it. Were the District Court decision to be upheld, it will seriously undermine industry efforts in security. I don’t doubt that Apple will continue to further engineering work to further secure the data on the smartphones<sup>46</sup> (and other devices), but the government’s actions would give serious pause to other companies pursuing that direction.

### **International Impact of Forcing Apple to Unlock its Secured Phones**

There are also serious international consequences that would stem from Apple’s developing code to unsecure its iPhone’s operating system. As I’m sure members of the committee are aware, when members of the US government and businesspeople

---

<sup>46</sup> Matt Apuzzo and Katie Benner, “Security ‘Arms Race’ as Apple Is Said to Harden iPhone,” *New York Times*, February 25, 2016.

travel to certain countries, they bring “loaner” devices with them—phones and laptops that are wiped clean before they leave the US and wiped clean on return.<sup>47</sup> That’s the case even though the devices never have their network connections turned on, at least by the owner. Recommendations for security include such steps as removing batteries from a phone when at meetings (in order to prevent a microphone being turned on remotely)<sup>48</sup> and keeping the device with you at all times.<sup>49</sup>

Apple’s efforts to secure the data on the iPhone should be viewed in this light.

There is another international aspect to the FBI’s efforts to unsecure the phone. United States support of human rights is a cornerstone of US foreign policy. It includes strong support for private and secure communications, for such capabilities are a necessity for human rights workers in repressive nations.

There is no question that authoritarian governments in such countries as Russia and China will demand Apple deliver the same software that it has been ordered to develop to handle Farook’s work phone.<sup>50</sup> Apple’s ability to resist such demands is made much more difficult if it has already created the code for US government use.

Securing the iPhone follows in US government tradition of developing secure communication and data storage solutions for private-sector use. The US Naval Research Laboratories developed Tor, The Onion Router, an Internet-based tool for obscuring communications metadata (thus hiding who is communicating with whom). At first glance, this might seem counterproductive; after all, criminals hide their tracks that way. But Tor is also remarkably useful for the military (obscuring that personnel in safe houses are communicating with US command), for law-enforcement investigators (obscuring that a participant in a child porn chat room is actually an investigator from fbi.gov), enabling human-rights workers and journalists working in repressive regimes a modicum of safety, etc. Tor functions most effectively in protecting users’ identities if more users are on the system (and if not all users are government employees).

Another project, one that has resonances with the iPhone, is a US Department of State Bureau of Democracy, Human Rights, and Labor supported program that

---

<sup>47</sup> Nicole Perlroth, “Traveling Light in a Time of Digital Thievery,” *New York Times*, February 20, 2012.

<sup>48</sup> *Ibid.*

<sup>49</sup> See, for example, North Dakota State University, “Cyber Security Tips for Traveling Abroad with Mobile Electronic Devices,” [https://www.ndsu.edu/its/security/traveling\\_abroad\\_with\\_electronic\\_devices/](https://www.ndsu.edu/its/security/traveling_abroad_with_electronic_devices/)

<sup>50</sup> “And once developed for our government, it is only a matter of time before foreign governments demand the same tool.” United States District Court for the Central District of California, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant of a Black Lexus IS300 California License Plate 35KGD203, No ED15-0451M, Order Compelling Apple to Assist Agents in Search, February 16, 2016, p.2.



developed an information management tool, Martus.<sup>51</sup> Martus enables a group to create a searchable, encrypted database (say of human rights violations), and *this database provides access only to members of the group that created the account.*<sup>52</sup>

Given the threats to US businesspeople traveling overseas, and the strong interest and support of the US government to secure communication and data storage tools for human-rights workers abroad, the FBI stance makes no sense. If the FBI succeeds in having Apple develop software to unlock the phone, the bureau will, in effect, have provided our enemies with tools to use against us. But this is not the first time that the law enforcement has mistaken difficulties in conducting investigations with technology that must be changed to accommodate its needs. That approach mistakes where actual solutions should lie.

### **We Have Been Down this Route Before — and It is Dangerous**

Five years ago I testified to a House Judiciary Subcommittee, the Subcommittee on Crime, Terrorism, and Homeland Security. At the time, FBI General Counsel Valerie Caproni expressed grave concern that due to encryption being used for communications (as opposed to for devices), the FBI was “going dark.” At the time, the FBI sought to extend the *Communications Assistance for Law Enforcement Act* (CALEA) to Internet, or IP-based, communications.

Now CALEA is a very problematic law. Wiretapping is a way for an unauthorized third party to listen in to a communication. By requiring that wiretapping capabilities be built into telephone switches, the government created a security breach. Indeed there are many ways for nefarious sorts to take advantage of the opening afforded by law enforcement.

The story of the ten-month wiretapping of the cellphones of one hundred senior members of the Greek government including the Prime Minister, the heads of the ministries of national defense, foreign affairs, and justice is well known.<sup>53</sup> Less well known is the fact that an IBM researcher found multiple security problems in a Cisco architecture for the equivalent type of switch for wiretapping IP-based communications.<sup>54</sup> *But much more disturbing than either of these stories is the fact that when the NSA tested CALEA-compliant switches that had been submitted prior to*

---

<sup>51</sup> The Department of State supported deployment and training, particularly in Uganda and Zambia where LGBTQ activists use Martus for contact lists, testimonies, and similar information.

<sup>52</sup> “Martus 4.5: Strong Security, Easy Configuration, Enhanced Usability,” <https://benetech.org/2014/06/17/martus-4-5-strong-security-easy-configuration-enhanced-usability/>. Benetech does not hold the keys and could not decrypt the data if requested to.

<sup>53</sup> Vassilis Prevelakis and Diomidis Spinellis, “The Athens Affair,” *IEEE Spectrum*, Vol. 44, No. 7 (July 2007), pp. 26-33.

<sup>54</sup> Tom Cross, “Exploiting Lawful Intercept to Wiretap the Internet,” Black Hat DC 2010.

*use in DoD systems, NSA found security problems in every single switch submitted for testing.*<sup>55</sup>

CALEA did not apply to “information services,” but in 2010, the FBI proposed that the law be extended to IP-based communications. As the world, knows, the Internet is remarkably insecure. Building wiretapping capabilities into switches and routers is a move that would make things substantively worse. And it is unnecessary, for there are other solutions that would provide law enforcement with the capabilities it needs without introducing new security flaws.

Many Internet communications, such as those using Google or Facebook services, are available to the companies in the clear. Thus, these communications services, while not falling precisely under the CALEA umbrella, remain easy for law enforcement to access (as indeed they have under court order).

Instead of requiring by law that communications systems be built “wiretap capable,” it is possible to take advantage of the vulnerabilities of any large software system—and these include phones and computers—to install a remote wiretap.<sup>56</sup> Called “lawful hacking” because it is legal (done under a court order) and “hacking” because it involves hacking into the devices, is a method that has been successfully adopted by the FBI. In fact, it is an approach that has been used by the Bureau since at least 2001.<sup>57</sup>

The idea is simple—and relied on by attackers all the time. Using a wiretap warrant to probe a suspect’s smartphone—or other communications device you wish to wiretap—and find a vulnerability on the device. Unfortunately such vulnerabilities are easy to find. Then law enforcement will need a second wiretap warrant to install the actual wiretap; the wiretap is installed by taking advantage of the vulnerability to download onto the device.<sup>58</sup>

Now this is an ugly sounding business, and indeed, civil libertarians have expressed concern about a wiretap solution that involves breaking into peoples’ devices. But the fact is that if law enforcement is to continue to wiretap, it can do so either by

---

<sup>55</sup> Private communication with Richard George, Former Technical Director for Information Assurance, National Security Agency (Dec. 1, 2011).

<sup>56</sup> See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, “Going Bright: Wiretapping without Weakening Communications Infrastructure,” *IEEE Security and Privacy*, Vol. 11, No. 1, January/February 2013, pp. 62-72 and also Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet,” *Northwestern Journal of Technology and Intellectual Property*, Vol. 12, Issue 1, (2014).

<sup>57</sup> In the 2001 case, the FBI used software dubbed “Magic Lantern” to inject a virus into a remote computer and obtain the device’s encryption keys. See B. Sullivan, “FBI Software Cracks Encryption Wall,” NBC News, 20 Nov. 2001; [www.nbcnews.com/id/3341694/ns/technology\\_and\\_science-security/t/fbi-software-cracks-encryption-wall](http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall).

<sup>58</sup> This is the process by which criminals and other attackers download malware to extract data (of course, they do so without wiretap warrants).

taking advantage of vulnerabilities already present in the system to wiretap or by requiring all systems be made vulnerable (the CALEA solution). *Either you encourage security solutions that protect everyone by taking advantage of the security problems that already exist in the system, or you push everyone into less secure systems.* The former strengthens society's security while still enabling investigations; the latter only serves to weaken us badly.

A lawful hacking approach to wiretap investigations means that law enforcement must work a little harder.<sup>59</sup> Wiretapping investigations must be individually designed for each target (sometimes the same solution may work against more than one target). This is expensive, but that is not necessarily a bad thing; it means that we are not encouraging widespread wiretapping. I know that this is a value the Judiciary Committee holds dear.

The lawful hacking approach to wiretapping provides a roadmap for the locked smartphone situation.

### **Solutions for Locked Phones: FBI Investigatory Capabilities for the Twenty-first Century**

Wiretap and search are extremely important tools for law enforcement, but encryption and locking down devices are extremely important security solutions for our data-driven, data-dependent society. But instead of embracing such technologies as an important and crucial security advance, law enforcement has largely seen such technologies as an impediment to lawfully authorized searches. This is a twentieth-century approach to a twenty-first century problem—but in that fact lies the possibility of a solution.

In the late 1990s, the NSA faced a similar crisis. Seymour Hersh detailed the situation in the *New Yorker*,

The NSA, whose Cold War research into code breaking and electronic eavesdropping spurred the American computer revolution, has become a victim of the high-tech world it helped to create. Senior military and civilian bureaucrats ... have failed to prepare fully for today's high-volume flow of E-mail and fibre-optic transmissions—even as nations throughout Europe, Asia, and the Third World have begun exchanging diplomatic and national-security messages encrypted in unbreakable digital code ...<sup>60</sup>

---

<sup>59</sup> An NSA colleague once remarked to me that his agency had the right to break into certain systems, but no one ever guaranteed the right that it would be easy to do so.

<sup>60</sup> Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6, 1999.

As we all know, the NSA adapted.

The FBI is where the NSA was in 1999, and it has been there for quite some time (certainly since well before CALEA's passage).

Given the types of adversaries the US faces, and the skills they have, we should be strengthening and securing all forms of cyber, including those in consumer hands. That's exactly what Apple has done. We should be praising Apple for this direction, and at the same time, we should help law enforcement to adopt a twenty-first century approach.

The Bureau has some expertise in this direction, but it will need more, much more, both in numbers, but also in the depth.

The FBI will need an investigative center with agents with a deep technical understanding of modern telecommunications technologies; this means from the physical layer to the virtual one, and all the pieces in between. Since all phones are computers these days, this center will need to have the same level of deep expertise in computer science. In addition, there will need to be teams of researchers who understand various types of fielded devices. This will include not only where technology is and will be in six months, but where it may be in two to five years. This center will need to conduct research as to what new surveillance technologies will need to be developed as a result of the directions of new technologies. I am talking deep expertise here and strong capabilities, not light.

This expertise need not be in house. The FBI could pursue a solution in which they develop some of their own expertise and closely manage contractors to do some of the work. But however the Bureau pursues a solution, it must develop modern, state-of-the-art capabilities for surveillance.

Such capabilities will not come cheap, but the cost annually will be in the hundreds of millions, not in the billions. But given the alternatives—insecure communications technologies that preserve law-enforcement's ability to search and wiretap at the cost of enabling others to do so as well—the cost is something we not only can afford, but must.

Developing such capabilities will involve deep change for the Bureau, which remains agent based, not technology based. But just as the NSA had to change in the late 1990s, so must the FBI. In fact, that change is long overdue. As many in law enforcement have said, many if not most crimes now have a cyber component. The FBI must develop advanced capabilities for such investigations, moving to a technology based investigation agency. It is not there now.

Because of the complexity involved, state and local law enforcement will not be able to develop their own solutions for some, or perhaps many, cases. They will need to rely on outsiders, either contractors or an effort put together by the FBI.



It is neither the time nor place to exactly map out the full solution of how such a law-enforcement advanced technologies surveillance center will work. That will take the expertise of law enforcement, technical leaders, and Congress to study and determine. But I place this before you not only as a solution to the conundrum that Director Comey and District Attorney Vance present you, but as *the only solution that protects our security and enables law enforcement to do its job in the face of advanced communications technologies.*

What we as a nation, and you as lawmakers, need to do is enable the Bureau to develop that expertise and, also, to simultaneously determine the best way to develop structures to enable state and local law enforcement to take advantage of that expertise.

Encryption and other protections (such as time delays as incorrect PINs are entered) secure our systems, and should never be undermined. Instead, the FBI must learn to investigate smarter; you, Congress, can provide it with the resources and guidance to help it do so. Bring FBI investigative capabilities into the twenty-first century. That's what is needed here—and not undermining the best security that any consumer device has to date. For that's what Apple's iOS is.

### **Summing Up**

Privacy is a deeply held human value; it is what enables us to laugh, to love, to tell embarrassing stories about ourselves, to take risks and expose ourselves, and to be deeply human. But while I care very deeply about privacy, I think that the business of securing communications and devices is ultimately a security versus security story, not a security versus privacy story.

We have become highly dependent on our devices for conducting all parts of our lives, and this will only expand in the future. But instead of going forward, for a moment I want to look back, quite far back. I want to end by noting what the preamble to the Constitution says,

We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence [sic], promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Note that important phrase: "ensure the blessing of Liberty to ourselves and our Posterity." In the wake of the terrorist attacks in San Bernardino, it is easy to make a decision that argues in favor of short-term security by enabling this week's



investigation. It is much harder to make the decision that provides for long-term safety. But the preamble tells us to do so.

We have the option to press companies to develop as secure and private devices as they can, or to press them to go the other way. Let us make the right decision, for our safety, long-term security, and humanity.

Thank you.



# **Exhibit H**

CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA  
DAVID VITTER, LOUISIANA  
DAVID A. PERDUE, GEORGIA  
THOM TILLIS, NORTH CAROLINA

PATRICK J. LEAHY, VERMONT  
DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

KOLAN L. DAVIS, *Chief Counsel and Staff Director*  
KRISTINE J. LUCIUS, *Democratic Chief Counsel and Staff Director*

February 16, 2016

### Via Electronic Transmission

The Honorable Sally Q. Yates  
Deputy Attorney General  
U.S. Department of Justice  
950 Pennsylvania Ave., NW  
Washington, DC 20530

The Honorable James B. Comey, Jr.  
Director  
Federal Bureau of Investigation  
935 Pennsylvania Ave., NW  
Washington, DC 20535

Dear Deputy Attorney General Yates and Director Comey:

I write today in response to your answers to my Questions for the Record (QFRs) from the Judiciary Committee's July 8, 2015 hearing entitled "Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy." At that hearing, you both testified about the public safety threat resulting from widespread inviolable encryption. Various senators expressed similar concerns about the problem, but numerous experts and outside commentators have also noted the benefits of encryption and raised issues with advancing legislative solutions.

Your recent QFR responses appear to indicate that this problem may be getting worse. For instance, Director Comey stated that as a consequence of widespread encryption, "the data on the vast majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant." On February 9, 2016, Director Comey highlighted an example of this problem when he testified before the Select Committee on Intelligence that a cellular telephone from one of the terrorists who killed 14 people in San Bernardino, California in December 2015 remains encrypted today. Moreover, as Director Comey referenced in response to another QFR, Apple Inc. is now claiming that complying with court orders – even when it has the technical

capability to do so and has regularly done so in the past – “would cause reputational harm.”

Nevertheless, I have yet to see any concrete progress on the Going Dark problem from the Obama Administration. When pressed for solutions at the July 8 hearing, Deputy Attorney General Yates stated that the Administration intended to pursue a collaborative and cooperative approach with technology providers. She further stated in response to my QFRs that “[t]he Department of Justice continues to work with companies and industry groups to address these issues, and those efforts have intensified in the last few months.” But at the same time, the Department of Justice (DOJ) has been unwilling to establish a deadline or timetable to assess the effectiveness of its case-by-case approach. Deputy Attorney General Yates’s QFR response in fact stated both that “we do not have a deadline in mind for any particular action” and “[t]he Administration is not seeking legislation at this time” to address the problem. Such statements only reinforce the concerns I set forth in a letter to the Department dated October 8, 2015, which cited two *Washington Post* articles from September of last year casting doubt on the Administration’s commitment to address this problem. And, as noted above, the Administration’s current posture appears to have encouraged at least one technology provider to go out of its way to refuse to assist law enforcement even in circumstances where it once helped to provide lawful access to encrypted devices in response to court orders.

In order to better understand and assess this problem, Congress needs accurate information. This was a point on which there was bipartisan agreement at our hearing in July. But here your responses to my QFRs are woefully inadequate. In order to more fully understand the nature and scope of this problem, I submitted questions that called for specific information from DOJ and the FBI about the providers that have refused to comply with court orders. I also explained the importance of the Administration providing Congress with any and all quantitative data on the Going Dark problem – including all available statistical data concerning the impact of encryption on access to both “data-in-motion” and “data-at-rest.” But rather than providing specific information and quantitative data, your QFR responses merely indicate that DOJ and the FBI are “improving enterprise-wide quantitative data collection” to “improve and streamline data collection metrics.” Yet your responses imply that some data has already been or can readily be collected and that information related to the “data-at-rest” problem is readily available.

I therefore request that DOJ and FBI immediately provide any and all currently available quantitative data concerning the scope and impact of encryption on both the “data-in-motion” and “data-at-rest” problems. Congress and the American people need this information to understand the effect of widespread inviolable



encryption on the government's ability to investigate and prosecute criminal offenses and to prevent terrorist attacks. In addition, Congress and the American people have a right to know whether any providers have changed their mind as a result of the Administration's strategy of engaging companies and industry groups directly. Therefore, please provide a list of all the providers that the Administration has approached since July 2015 pursuant to this strategy, and identify whether each one has responded and in what way.

As I have stated before, I strongly believe that the Administration should use every lawful tool at its disposal and vigorously investigate each and every potential solution to this serious issue. Members of the Committee have offered their support and personal assistance in your ongoing efforts with technology providers, and I ask to continue to be regularly advised – quarterly, at a minimum – of the status of those negotiations. I understand that any single solution – including any single legislative solution – to this problem may be imperfect. But I request that the Administration keep Congress apprised of any progress, or lack thereof, in its efforts to maintain its ability to execute lawful, court-authorized investigative techniques, such as warrants and wiretaps, which are essential to enforcing the rule of law and protecting the American people.

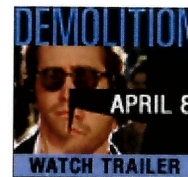
Sincerely,



Charles E. Grassley  
Chairman



# **Exhibit I**



**The New York Times** | <http://nyti.ms/21hvBiH>

TECHNOLOGY

# Apple Is Said to Be Trying to Make It Harder to Hack iPhones

By **MATT APUZZO** and **KATIE BENNER** FEB. 24, 2016

WASHINGTON — Apple engineers have begun developing new security measures that would make it impossible for the government to break into a locked iPhone using methods similar to those now at the center of a court fight in California, according to people close to the company and security experts.

If Apple succeeds in upgrading its security — and experts say it almost surely will — the company will create a significant technical challenge for law enforcement agencies, even if the Obama administration wins its fight over access to data stored on an iPhone used by one of the killers in last year’s San Bernardino, Calif., rampage. If the Federal Bureau of Investigation wanted to get into a phone in the future, it would need a new way to do so. That would most likely prompt a new cycle of court fights and, yet again, more technical fixes by Apple.

The only way out of this scenario, experts say, is for Congress to get involved. Federal wiretapping laws require traditional phone carriers to make their data accessible to law enforcement agencies. But tech companies like Apple and Google are not covered, and they have strongly resisted legislation that would place similar requirements on them.

“We are in for an arms race unless and until Congress decides to clarify who has what obligations in situations like this,” said Benjamin Wittes, a senior fellow at the Brookings Institution.

Companies have always searched for software bugs and patched holes to keep their code secure from hackers. But since the revelations of government surveillance made by Edward J. Snowden, companies have been retooling their products to protect against government intrusion.

For Apple, security is also a global marketing strategy. New security measures would not only help the company in its fight with the government, but also reassure investors and customers.

“For all of those people who want to have a voice but they’re afraid, we are standing up, and we are standing up for our customers because protecting them we view as our job,” Apple’s chief executive, Timothy D. Cook, said on Wednesday in an interview with ABC News.

The company first raised the prospect of a security update last week in a phone call with reporters, who asked why the company would allow firmware — the software at the heart of the iPhone — to be modified without requiring a user password.

One senior executive, speaking on the condition of anonymity, replied that it was safe to bet that security would continue to improve. Separately, a person close to the company, who also spoke on the condition of anonymity, confirmed this week that Apple engineers had begun work on a solution even before the San Bernardino attack. A company spokeswoman declined to comment on what she called rumors and speculation.

Independent experts say they have held informal conversations with Apple engineers over the last week about the vulnerability. Exactly how Apple will address the issue is unclear. Security experts who have been studying Apple’s phone security say it is technically possible to fix.

“There are probably 50 different ideas we have all sent to Apple,” said Jonathan Zdziarski, a security researcher.



Apple built its recent operating systems to protect customer information. As Mr. Cook wrote in a recent letter to customers, “We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.”

But there is a catch. Each iPhone has a built-in troubleshooting system that lets the company update the system software without the need for a user to enter a passcode. Apple designed that feature to make it easier to repair malfunctioning phones.

In the San Bernardino case, the F.B.I. wants to exploit that troubleshooting system by forcing Apple to write and install new software that strips away several security features, making it much easier for the government to hack into the phone. The phone in that case is an old model, but experts and former Apple employees say that a similar approach could also be used to alter software on newer phones. That is the vulnerability Apple is working to fix.

Apple regularly publishes security updates and gives credit to researchers who hunt for bugs in the company’s software. “Usually, bug reports come in an email saying, ‘Dear Apple Security, we’ve discovered a flaw in your product,’ ” said Chris Soghoian, a technology analyst with the American Civil Liberties Union. “This bug report has come in the form of a court order.”

The court order to which Mr. Soghoian referred was issued last week by a federal magistrate, and tells Apple to write and install the code sought by the F.B.I. Apple has promised to challenge that order. Its lawyers have until Friday to file its opposition in court.

In many ways, Apple’s response continues a trend that has persisted in Silicon Valley since Mr. Snowden’s revelations. Yahoo, for instance, left its email service unencrypted for years. After Mr. Snowden revealed the National Security Agency surveillance, the company quickly announced plans to encrypt email. Google similarly moved to fix a vulnerability that the government was using to hack into company data centers.

Apple's showdown with the Justice Department is different in one important way. Now that the government has tried to force Apple to hack its own code, security officials say, the company must view itself as the vulnerability.

"This is the first time that Apple has been included in their own threat model," Mr. Zdziarski said. "I don't think Apple ever considered becoming a compelled arm of the government."

The F.B.I. director, James B. Comey Jr., signaled this week that he expected Apple to change its security, saying that the phone-cracking tool the government sought in the San Bernardino case was "increasingly obsolete." He said that supported the government's argument that it was not seeking a skeleton key to hack into all iPhones.

Apple, though, says the case could set a precedent for forcing company engineers to write code to help the government break into any iPhone. "The U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create," Mr. Cook said in his letter.

The heated back-and-forth between the government and technology companies is, at least in part, a function of the Obama administration's strategy. The White House has said it will not ask Congress to pass a law requiring tech companies to give the F.B.I. a way to gain access to customer data. That has left the Justice Department to fight for access one phone at a time, in court cases that often go unnoticed.

While it is generally accepted that Silicon Valley's tech giants can outgun the government in a technical fight, the companies do face one important limitation. Security features often come at the expense of making products slower or clunkier.

Apple's brand is built around creating products that are sleek and intuitive. A security solution that defeats the F.B.I. is unworkable if it frustrates consumers. One of the impediments to encrypting all the data in Apple's iCloud servers, for instance, has been finding a way to ensure that customers can easily retrieve and recover photos and other information stored there.

“Telling a member of the public that they’re going to lose all the family photos they’ve ever taken because they forgot their password is a really tough sell,” Mr. Soghoian said. “A company wants to sell products to the public.”

Matt Apuzzo reported from Washington and Katie Benner from San Francisco.

*Follow The New York Times’s politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.*

A version of this article appears in print on February 25, 2016, on page A1 of the New York edition with the headline: Security ‘Arms Race’ as Apple Is Said to Harden iPhone Tech.

---

© 2016 The New York Times Company

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  
28

**PROOF OF SERVICE**

I, Janice Austgen, declare:

I am employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Mayer Brown LLP, 350 South Grand Avenue, 25th Floor, Los Angeles, California 90071-1503. On March 3, 2016, I served a copy of the within document(s):

DECLARATION OF RUTH ZADIKANY IN SUPPORT OF BRIEF OF *AMICI CURIAE* BSA|THE SOFTWARE ALLIANCE, THE CONSUMER TECHNOLOGY ASSOCIATION, THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL, AND TECHNET

X by placing the document(s) listed above in a sealed UPS envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a UPS agent for delivery.

SEE ATTACHED SERVICE LIST

I declare under penalty of perjury under the laws of the United States of America that the above is true and correct.

Executed on March 3, 2016, at Los Angeles, California.

  
\_\_\_\_\_  
Janice Austgen

1 Eric David Vandavelde, Esq.  
2 Theodore J. Boutrous, Jr., Esq.  
3 Gibson Dunn and Crutcher LLP  
4 333 South Grand Avenue  
5 Los Angeles, CA 90071

6 Jeffrey G. Landis, Esq.  
7 Marc J Zwillinger, Esq.  
8 Zwillgen PLLC  
9 1900 M Street NW Suite 250  
10 Washington, DC 20036

11 Nicola T. Hanna, Esq.  
12 Gibson Dunn and Crutcher LLP  
13 3161 Michelson Drive 12th Floor  
14 Irvine, CA 92612-4412

15 Theodore B. Olson, Esq.  
16 Gibson Dunn and Crutcher LLP  
17 1050 Connecticut Avenue NW  
18 Washington, DC 20036-5306

19 Allen W. Chiu, Esq.  
20 Assistant United States Attorney  
21 Office of U.S. Attorney  
22 National Security Section  
23 312 North Spring Street Suite 1300  
24 Los Angeles, CA 90012

25 Tracy L. Wilkison, Esq.  
26 Assistant United States Attorney  
27 Office of U.S. Attorney  
28 Chief, Cyber and Intellectual Property Crimes Section  
312 North Spring Street 11th Floor  
Los Angeles, CA 90012-4700



ORIGINAL  
LOGGED

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  
28

MAYER BROWN LLP  
JOHN NADOLENCO (SBN 181128) PH 2: 31  
jnadolenco@mayerbrown.com  
RUTH ZADIKANY (SBN 260288)  
rzadikany@mayerbrown.com  
350 South Grand Avenue, 25th Floor  
Los Angeles, California 90071-1503  
Telephone: (213) 229-9500  
Facsimile: (213) 625-0248

FILED  
CLERK, U.S. DISTRICT COURT  
MAR - 4 2016  
CENTRAL DISTRICT OF CALIFORNIA  
EASTERN DIVISION  
BY DEPUTY

ANDREW J. PINCUS (*pro hac vice application forthcoming*)  
apincus@mayerbrown.com  
TRAVIS CRUM (*pro hac vice application forthcoming*)  
terum@mayerbrown.com  
1999 K Street, N.W.  
Washington D.C. 20006-1001  
Telephone: (202) 263-3328  
Facsimile: (202) 263-5328

Attorneys for *Amici Curiae* BSA|The Software Alliance, the  
Consumer Technology Association, the Information  
Technology Industry Council, and TechNet

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA  
EASTERN DIVISION**

LOGGED

2016 MAR - 3 PM 2:31  
CLERK U.S. DISTRICT COURT  
CENTRAL DIST. OF CALIF.  
RIVERSIDE  
BY

IN THE MATTER OF THE SEARCH  
OF AN APPLE IPHONE SEIZED  
DURING THE EXECUTION OF A  
SEARCH WARRANT ON A BLACK  
LEXUS IS300, CALIFORNIA  
LICENSE PLATE 35KGD203

Case No. 5:16-cm-00010-SP  
Corporate Disclosure Statement Of  
*Amici Curiae* BSA|The Software  
Alliance, the Consumer Technology  
Association, the Information  
Technology Industry Council, and  
TechNet  
Hearing Date: March 22, 2016  
Time: 1:00 p.m.  
Location: Courtroom of the Hon. Sheri  
Pym

1 Pursuant to Federal Rule of Criminal Procedure 12.4(a)(1), the undersigned  
2 hereby certifies that (1) *amicus curiae* BSA|The Software Alliance has no parent  
3 company and no publicly held company owns 10% or more of its stock; (2) *amicus*  
4 *curiae* the Consumer Technology Association has no parent company and no  
5 publicly held company owns 10% or more of its stock; (3) *amicus curiae* the  
6 Information Technology Industry Council has no parent company and no publicly  
7 held company owns 10% or more of its stock; and (4) *amicus curiae* TechNet has  
8 no parent company and no publicly held company owns 10% or more of its stock.

9  
10 Dated: March 3, 2016

MAYER BROWN LLP  
JOHN NADOLENCO  
RUTH ZADIKANY  
ANDREW J. PINCUS  
TRAVIS CRUM

11  
12  
13 By: John Nadolenco/122  
14 John Nadolenco

15 Attorneys for BSA|The Software Alliance,  
16 the Consumer Technology Association, the  
17 Information Technology Industry Council,  
18 and TechNet.  
19  
20  
21  
22  
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  
20  
21  
22  
23  
24  
25  
26  
27  
28

**PROOF OF SERVICE**

I, Janice Austgen, declare:

I am employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Mayer Brown LLP, 350 South Grand Avenue, 25th Floor, Los Angeles, California 90071-1503. On March 3, 2016, I served a copy of the within document(s):

CORPORATE DISCLOSURE STATEMENT OF *AMICI CURIAE* BSA|THE SOFTWARE ALLIANCE, THE CONSUMER TECHNOLOGY ASSOCIATION, THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL, AND TECHNET

X by placing the document(s) listed above in a sealed UPS envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a UPS agent for delivery.

SEE ATTACHED SERVICE LIST

I declare under penalty of perjury under the laws of the United States of America that the above is true and correct.

Executed on March 3, 2016, at Los Angeles, California.

  
\_\_\_\_\_  
Janice Austgen

1 Eric David Vandavelde, Esq.  
2 Theodore J. Boutrous, Jr., Esq.  
3 Gibson Dunn and Crutcher LLP  
4 333 South Grand Avenue  
5 Los Angeles, CA 90071

6 Jeffrey G. Landis, Esq.  
7 Marc J Zwillinger, Esq.  
8 Zwillgen PLLC  
9 1900 M Street NW Suite 250  
10 Washington, DC 20036

11 Nicola T. Hanna, Esq.  
12 Gibson Dunn and Crutcher LLP  
13 3161 Michelson Drive 12th Floor  
14 Irvine, CA 92612-4412

15 Theodore B. Olson, Esq.  
16 Gibson Dunn and Crutcher LLP  
17 1050 Connecticut Avenue NW  
18 Washington, DC 20036-5306

19 Allen W. Chiu, Esq.  
20 Assistant United States Attorney  
21 Office of U.S. Attorney  
22 National Security Section  
23 312 North Spring Street Suite 1300  
24 Los Angeles, CA 90012

25 Tracy L. Wilkison, Esq.  
26 Assistant United States Attorney  
27 Office of U.S. Attorney  
28 Chief, Cyber and Intellectual Property Crimes Section  
312 North Spring Street 11th Floor  
Los Angeles, CA 90012-4700