

1 Peter Bibring (SBN 223981)  
pbibring@aclusocal.org  
2 AMERICAN CIVIL LIBERTIES UNION  
3 OF SOUTHERN CALIFORNIA  
1313 West Eighth Street  
4 Los Angeles, CA 90017  
5 Telephone: (213) 977-9500

6 Alex Abdo  
7 Esha Bhandari  
Eliza Sweren-Becker\*  
8 Brett Max Kaufman  
9 aabdo@aclu.org  
10 AMERICAN CIVIL LIBERTIES UNION FOUNDATION  
125 Broad Street, 18th Floor  
11 New York, NY 10004  
12 Telephone: (212) 549-2500

13 *\*Admission to the bar pending*  
14 Additional counsel listed on signature page  
Attorneys for Proposed *Amici Curiae*

15 **UNITED STATES DISTRICT COURT**  
16 **CENTRAL DISTRICT OF CALIFORNIA**

17 IN THE MATTER OF THE SEARCH ) ED No. CM 16-10 (SP)  
18 OF AN APPLE IPHONE SEIZED )  
19 DURING THE EXECUTION OF A ) **BRIEF OF AMICI CURIAE**  
20 SEARCH WARRANT ON A BLACK ) **AMERICAN CIVIL LIBERTIES**  
21 LEXUS IS300, CALIFORNIA ) **UNION, ACLU OF NORTHERN**  
22 LICENSE PLATE 35KGD203. ) **CALIFORNIA, ACLU OF**  
23 ) **SOUTHERN CALIFORNIA, AND**  
24 ) **ACLU OF SAN DIEGO AND**  
25 ) **IMPERIAL COUNTIES, IN**  
26 ) **SUPPORT OF APPLE, INC.**  
27 )  
28 )

---

Hearing Date: March 22, 2016  
Time: 1:00 pm  
Courtroom: Courtroom 3 or 4  
Judge: Hon. Sheri Pym

1 **TABLE OF CONTENTS**

2 TABLE OF AUTHORITIES .....ii

3 INTERESTS OF AMICI CURIAE ..... 1

4 SUMMARY OF ARGUMENT ..... 1

5 BACKGROUND ..... 2

6 ARGUMENT.....4

7

8 I. The All Writs Act does not authorize the government to compel

9 Apple to create and authenticate software that would allow the

10 government to break into Apple’s customers’ devices. .... 4

11 A. Apple is “far removed from the underlying controversy”

12 because it neither possesses nor controls the information

13 the government seeks..... 5

14 B. The assistance the government seeks is unreasonably

15 burdensome. .... 8

16 C. The government has failed to demonstrate that the

17 assistance it seeks is absolutely necessary..... 13

18 D. Congress has deliberately withheld the authority sought

19 here..... 13

20 II. The order the government seeks violates the Fifth Amendment. .... 16

21 CONCLUSION.....20

22

23

24

25

26

27

28

1 **TABLE OF AUTHORITIES**

2 **Cases**

3 *Application of the U.S. for Relief*, 427 F.2d 639 (9th Cir. 1970) ..... 14

4 *Application of the U.S.*, 427 F.2d 639 (9th Cir. 1970) ..... 14

5

6 *Application of U.S. for an Order Authorizing an In-Progress Trace of*  
7 *Wire Commc’ns over Tel. Facilities (Mountain Bell)*, 616 F.2d 1122  
(9th Cir. 1980).....6, 9, 13

8 *Application of U.S. for Order Authorizing Installation of Pen Register*  
9 *or Touch-Tone Decoder & Terminating Trap (Bell Telephone)*, 610  
10 F.2d 1148 (3d Cir. 1979) .....6, 9

11 *Arizona v. Hicks*, 480 U.S. 321 (1987)..... 17

12 *Arver v. United States*, 245 U.S. 366 (1918) ..... 18

13 *Boyd v. United States*, 116 U.S. 616 (1886)..... 17

14 *Butler v. Perry*, 240 U.S. 328 (1916) ..... 18

15 *Chapman v. United States*, 365 U.S. 610 (1961) ..... 8

16 *Clark v. Martinez*, 543 U.S. 371 (2005) ..... 16

17 *Clinton v. Goldsmith*, 526 U.S. 529 (1999)..... 7

18 *Cty. of Sacramento v. Lewis*, 523 U.S. 833 (1998) ..... 16, 20

19

20 *In re Application of the U.S. for an Order Authorizing Disclosure of*  
21 *Location Information of a Specified Wireless Tel.*, 849 F. Supp. 2d  
22 526 (D. Md. 2011) ..... 13

23 *In re Application of the U.S. for an Order Authorizing the Use of a*  
24 *Pen Register*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) .....4, 14

25 *In re Application of U.S. for an Order Directing a Provider of*  
26 *Commc’n Servs. to Provide Technical Assistance to Agents of the*  
27 *U.S. Drug Enforcement Admin.*, No. 15-1242 M, 2015 WL 5233551  
(D.P.R. Aug. 27, 2015) .....6

28

1	<i>In re Application of U.S. for an Order Directing X to Provide Access</i>	
2	<i>to Videotapes (Access to Videotapes)</i> , No. 03-89, 2003 WL	
3	22053105 (D. Md. Aug. 22, 2003) .....	6, 9
4	<i>In re Order Requiring Apple, Inc. to Assist in the Execution of a</i>	
5	<i>Search Warrant Issued by this Court (In re Order Requiring Apple)</i> ,	
6	No. 1:15-mc-01902-JO (E.D.N.Y. Feb. 29, 2016) .....	passim
7	<i>New Motor Vehicle Bd. v. Orrin W. Fox Co.</i> , 439 U.S. 96 (1978) .....	19
8	<i>Pa. Bureau of Corr. v. U.S. Marshals Serv.</i> , 474 U.S. 34 (1985) .....	4
9	<i>Palko v. Connecticut</i> , 302 U.S. 319 (1937) .....	17
10	<i>Plum Creek Lumber Co. v. Hutton</i> , 608 F.2d 1283 (9th Cir. 1979) .....	12, 14
11	<i>Stanford v. Texas</i> , 379 U.S. 476 (1965) .....	17, 19
12	<i>The Company v. United States</i> , 349 F.3d 1132 (9th Cir. 2003) .....	12
13	<i>United States v. Doe</i> , 537 F. Supp. 838 (E.D.N.Y. 1982) .....	6
14	<i>United States v. Hall</i> , 583 F. Supp. 717 (E.D. Va. 1984) .....	6, 9, 13
15	<i>United States v. Henderson</i> , 241 F.3d 638 (9th Cir. 2001) .....	8
16	<i>United States v. N.Y. Tel. Co.</i> , 434 U.S. 159 (1977) .....	passim
17	<i>United States v. Salerno</i> , 481 U.S. 739 (1987) .....	17
18	<i>United States v. X</i> , 601 F. Supp. 1039 (D. Md. 1984) .....	6, 9
19	<i>Wolff v. McDonnell</i> , 418 U.S. 539 (1974) .....	17
20	<b>Statutes</b>	
21		
22	28 U.S.C. § 1651 .....	2, 4
23	47 U.S.C. § 1001 .....	15
24	47 U.S.C. § 1002 .....	15
25		
26		
27		
28		

1 **Other Authorities**

2 Andrea Peterson, *Congressman with Computer Science Degree:*  
3 *Encryption Back-doors Are “Technologically Stupid,”* Wash. Post  
4 (Apr. 30, 2015), <http://wapo.st/1RESSn1> ..... 16

5 *Building Consumer Trust: Protecting Personal Data in the Consumer*  
6 *Product Industry*, Deloitte Univ. Press (2014),  
7 [https://d2mtr37y39tpbu.cloudfront.net/wp-](https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumer-trust_MASTER.pdf)  
8 [content/uploads/2014/11/DUP\\_970-Building-consumer-](https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumer-trust_MASTER.pdf)  
9 [trust\\_MASTER.pdf](https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumer-trust_MASTER.pdf)..... 11

10 Cal. DOJ, California Data Breach Report (Feb. 2016),  
11 <https://oag.ca.gov/breachreport2016> ..... 11

12 Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*,  
13 N.Y. Times (Sept. 27, 2010), <http://nyti.ms/1TH2kcD> ..... 15

14 Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y.  
15 Times (May 7, 2013), <http://nyti.ms/1WLESJo> ..... 15

16 Christopher Soghoian, *The Technology at the Heart of the Apple–FBI*  
17 *Debate, Explained*, Wash. Post, Feb. 29, 2016,  
18 <http://wapo.st/1T6hk3F>..... 10

19 Erin Kelley, *Congress Wades into Encryption Debate with Bill to*  
20 *Create Expert Panel*, USA Today (Jan. 11, 2016),  
21 <http://usat.ly/1UK35ij> ..... 14

22 Kif Leswing, *GOP Debate: What Republicans Got Wrong About*  
23 *Technology*, Fortune (Dec. 16, 2015), <http://for.tn/1Q4C73Z> ..... 15

24 Malena Carollo, *Survey: Consumers Reject Companies That Don’t*  
25 *Protect Privacy*, Christian Sci. Monitor (Jan. 29, 2016),  
26 [http://www.csmonitor.com/World/Passcode/2016/0129/Survey-](http://www.csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-that-don-t-protect-privacy)  
27 [Consumers-reject-companies-that-don-t-protect-privacy](http://www.csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-that-don-t-protect-privacy)..... 11

28 Mike McConnell, Michael Chertoff & William Lynn, Opinion, *Why*  
*the Fear Over Ubiquitous Data Encryption Is Overblown*, Wash.  
Post (July 28, 2015), <http://wapo.st/1ShCPic> ..... 16

Nicole Perlroth & David E. Sanger, *Obama Won’t Seek Access to*  
*Encrypted User Data*, N.Y. Times (Oct. 10, 2015),  
<http://nyti.ms/1G6YAvL>..... 15

1	President Barack Obama, Remarks by the President at the	
2	Cybersecurity and Consumer Protection Summit (Feb. 13, 2015),	
	<a href="http://1.usa.gov/21wkz9y">http://1.usa.gov/21wkz9y</a> .....	11
3	Rebecca Rifkin, <i>Hacking Tops List of Crimes Americans Worry About</i>	
4	<i>Most</i> , Gallup (Oct. 27, 2104),	
5	<a href="http://www.gallup.com/poll/178856/hacking-tops-list-crimes-american-worry.aspx">http://www.gallup.com/poll/178856/hacking-tops-list-crimes-</a>	
6	<a href="http://www.gallup.com/poll/178856/hacking-tops-list-crimes-american-worry.aspx">american-worry.aspx</a> .....	11
7	Susan Page, <i>Ex-NSA Chief Backs Apple on iPhone ‘Back Doors,’</i>	
8	USA Today (Feb. 24, 2016), <a href="http://usat.ly/1LAPJjq">http://usat.ly/1LAPJjq</a> .....	16
9	T.C. Sottek, <i>Hillary Clinton on Encryption: ‘Maybe the Back Door</i>	
10	<i>Isn’t the Right Door,’</i> The Verge (Dec. 19, 2015),	
11	<a href="http://www.theverge.com/2015/12/19/10628208/hillary-clinton-back-door-debate">http://www.theverge.com/2015/12/19/10628208/hillary-clinton-</a>	
12	<a href="http://www.theverge.com/2015/12/19/10628208/hillary-clinton-back-door-debate">back-door-debate</a> .....	15
13	<b>Rules</b>	
14	Fed. R. Crim. P. 41 .....	7

14  
15  
16  
17  
18  
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

## **INTERESTS OF AMICI CURIAE**

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation’s civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans’ right to privacy. The American Civil Liberties Union of Southern California, American Civil Liberties Union of Northern California, and American Civil Liberties Union of San Diego and Imperial Counties are the geographic affiliates in California of the ACLU.

## **SUMMARY OF ARGUMENT**

This case concerns an unprecedented law-enforcement effort to conscript an American technology company into creating software designed to weaken the security of its own devices—an effort that, if successful, would set precedent implicating the security and privacy of hundreds of millions of Americans. Neither the All Writs Act nor the Constitution authorizes the government to make the demand it has made here. While the government can in some circumstances require private parties to support law-enforcement investigations—for example, by requiring them to produce relevant evidence or give truthful testimony—the government does not hold the general power to enlist private third parties as its investigative agents to seek out information they do not possess or control. In other words, law enforcement may not commandeer innocent third parties into becoming its undercover agents, its spies, or its hackers.

The government’s demand is unlawful under the All Writs Act because that Act does not permit the government to require innocent third parties to turn over information not already in their possession or control, because the assistance the government seeks is unreasonably burdensome and unnecessary, and because

1 Congress has deliberately withheld from the government the authority to require  
2 technology companies to circumvent the security protections in their devices.  
3 Indeed, in a related case, Magistrate Judge Orenstein recently arrived at all of these  
4 conclusions in a meticulous and carefully reasoned opinion that should guide this  
5 Court’s consideration. *In re Order Requiring Apple, Inc. to Assist in the Execution*  
6 *of a Search Warrant Issued by this Court (In re Order Requiring Apple)*, No. 1:15-  
7 mc-01902-JO, slip op. at 50 (E.D.N.Y. Feb. 29, 2016).

8 Separately, the order the government seeks would violate the Constitution.  
9 The Fifth Amendment imposes a limit on the nature of the assistance that law  
10 enforcement may compel, and the assistance sought here plainly exceeds that limit.  
11 At the very least, the fact that the government’s interpretation of the All Writs Act  
12 would raise serious constitutional questions supplies an additional reason to reject  
13 the government’s sweeping construction of the Act.

14 The government has defended its application as limited to this case and this  
15 case alone, but the legal precedent it seeks cannot be so contained. If the  
16 government prevails, then this case will be the first of many requiring companies  
17 to degrade the security and to undermine the trust in their products so essential to  
18 privacy in the digital age. For the many users who rely on digital devices to secure  
19 their information and communications, including members of vulnerable  
20 populations who rely on mobile devices to access the Internet, this burden would  
21 be severe.

22 For these reasons, this Court should deny the government’s request.

## 23 **BACKGROUND**

24 In an application filed on February 16, 2016, the government asked this  
25 Court to issue an order pursuant to the All Writs Act, 28 U.S.C. § 1651,  
26 compelling Apple to create cryptographically “signed” software to be installed on  
27  
28



1 an iPhone 5C that the FBI obtained during its investigation into the December  
2 2015 shootings in San Bernardino, California. The FBI specified that the software  
3 would: (1) bypass or disable the phone’s auto-erase function, if enabled; (2) allow  
4 the FBI to test passcodes on the device electronically (rather than through manual  
5 typing); and (3) circumvent the passcode rate-limiter on the device, which delays  
6 successive failed passcode attempts. Application at 7–8, *In the Matter of the*  
7 *Search of an Apple iPhone Seized During the Execution of a Search Warrant on a*  
8 *Black Lexus IS300, California License Plate 35KGD203*, No. 15-0415M (C.D.  
9 Cal. Feb. 16, 2016) (hereinafter “Application”). This Court granted the  
10 government’s request the same day, subject to Apple’s opportunity to object. Order  
11 at 3, *In re the Search of an Apple iPhone Seized During the Execution of a Search*  
12 *Warrant on a Black Lexus IS300, California License Plate 35KGD203*, ED No. 15-  
13 0415M (C.D. Cal. Feb. 16, 2016) (hereinafter “Order”).

14           Apple manufactured the iPhone at issue, but it does not possess or control  
15 the device or the personal data stored on it. *See* Application at 3. Moreover, Apple  
16 does not possess the software that the FBI seeks. Indeed, Apple has stated that, to  
17 comply with the government’s proposed order, Apple’s security engineers would  
18 have to write software specifically designed to disable the security measures those  
19 engineers built into the phone. *See* Motion to Vacate at 12, *In re the Search of an*  
20 *Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus*  
21 *IS300, California License Plate 35KGD203*, No. CM-16-10 (SP) (C.D. Cal. Feb.  
22 25, 2016) (hereinafter “Motion to Vacate”).  
23  
24  
25  
26  
27  
28

## ARGUMENT

1  
2 **I. The All Writs Act does not authorize the government to compel Apple**  
3 **to create and authenticate software that would allow the government to**  
4 **break into Apple’s customers’ devices.**

5 The order the government seeks would be unprecedented. The government is  
6 not seeking evidence in Apple’s possession or control, as would be consistent with  
7 precedent under the All Writs Act. Rather, it seeks to compel Apple to create and  
8 authenticate software that would allow the government to break into an  
9 individual’s iPhone, setting a precedent that would undermine the security and  
10 privacy of all who use Apple’s devices. No court has ever interpreted the All Writs  
11 Act to grant the government such authority, and this court should not be the first.  
12 Instead, it should embrace the careful reasoning of Magistrate Judge Orenstein’s  
13 opinion rejecting the same theory the government advances here. *See In re Order*  
14 *Requiring Apple*, slip op. at 15.

15 The All Writs Act, first enacted in 1789, is a gap-filling statute, not a source  
16 of authority itself. The Act permits federal courts to “issue all writs necessary or  
17 appropriate in aid of their respective jurisdictions and agreeable to the usages and  
18 principles of law.” 28 U.S.C. § 1651. In other words, it allows courts to issue  
19 orders effectuating *other* orders or powers that have some independent basis in  
20 law. *See United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977); *Pa. Bureau of*  
21 *Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 42 n.7 (1985) (courts may resort to the  
22 All Writs Act “to fill statutory interstices”); *In re Order Requiring Apple*, slip op.  
23 at 15 (“The limits of such gap-filling authority are easily discerned.”). The Act is  
24 not “a mechanism for the judiciary to give [the government] the investigative tools  
25 that Congress has not.” *In re Application of the U.S. for an Order Authorizing the*  
26 *Use of a Pen Register*, 396 F. Supp. 2d 294, 325 (E.D.N.Y. 2005).

27 In its narrow role as gap-filler, the Act confers only limited authority, as the  
28 Supreme Court has made clear. *See N.Y. Tel. Co.*, 434 U.S. at 172 (“[T]he power of

1 federal courts to impose duties upon third parties [under the All Writs Act] is not  
2 without limits.”). In *New York Telephone*, the government sought to compel a  
3 private telephone company to facilitate the installation of a “pen register” to obtain  
4 calling records passing through the company’s facilities. *Id.* at 164, 175–78. The  
5 Court approved the requested order, but only after considering four factors.

6 First, the Court looked to the connection between the investigation and the  
7 telephone company, concluding that the company was “not so far removed from  
8 the underlying controversy.” *Id.* at 174. Second, the Court analyzed the company’s  
9 burden of compliance, concluding that the company lacked a “substantial interest  
10 in not providing assistance.” *Id.* On this point, the Court explained that: (a) the  
11 company was a “highly regulated public utility with a duty to serve the public,” (b)  
12 it regularly used pen registers itself, for its own business purposes, and (c) its  
13 compliance required “minimal effort” and would occasion “no disruption to [the  
14 company’s] operations.” *Id.* at 174–75. Third, the Court considered whether the  
15 assistance was necessary, noting there was “no conceivable way” to effectuate the  
16 underlying order to install a pen register without the company’s assistance. *Id.* at  
17 175. And, fourth, the Court found that the order was “consistent with”  
18 congressional action and intent, because Congress had clearly intended to permit  
19 the use of pen registers in criminal investigations. *Id.* at 176.

20 None of these factors supports the order the government seeks here.

21 **A. Apple is “far removed from the underlying controversy” because**  
22 **it neither possesses nor controls the information the government**  
23 **seeks.**

24 Apple may not be compelled under the All Writs Act to assist the  
25 government here because it does not possess or control the information the  
26 government seeks. When the Act is used to supplement a court’s warrant authority,  
27 as the government seeks to do in this case, its application is limited to  
28

1 circumstances in which the third party either possesses or controls the information  
2 to which the warrant grants access.

3 This rule is plain from prior case law. In *New York Telephone*, for example,  
4 the telephone dialing information the government sought to collect was in the  
5 possession of the telephone company; it passed over phone lines that the company  
6 owned and controlled. *See id.* at 174–75. Likewise, the Ninth Circuit upheld an  
7 order requiring a telephone company to “perform an in-progress trace of telephone  
8 calls”—but only “by means of electronic facilities within its exclusive control.” *See*  
9 *Application of U.S. for an Order Authorizing an In-Progress Trace of Wire*  
10 *Commc’ns over Tel. Facilities (Mountain Bell)*, 616 F.2d 1122, 1123 (9th Cir.  
11 1980) (emphasis added). In so holding, the court emphasized the narrowness of its  
12 ruling, stating that “our decision today should not be read to authorize the  
13 wholesale imposition upon private, third parties of duties pursuant to search  
14 warrants.” *Id.* at 1132. Many other decisions have applied the Act in a similarly  
15 limited fashion. *See, e.g., Application of U.S. for Order Authorizing Installation of*  
16 *Pen Register or Touch-Tone Decoder & Terminating Trap (Bell Telephone)*, 610  
17 F.2d 1148, 1155 (3d Cir. 1979) (tracing of phone calls on the company’s lines).<sup>1</sup>  
18

---

19  
20 <sup>1</sup> *See also In re Application of U.S. for an Order Directing a Provider of*  
21 *Commc’n Servs. to Provide Technical Assistance to Agents of the U.S. Drug*  
22 *Enforcement Admin.*, No. 15-1242 M, 2015 WL 5233551, at \*5 (D.P.R. Aug. 27,  
23 2015) (similar for the contents of electronic communications over mobile-phone  
24 network); *In re Application of U.S. for an Order Directing X to Provide Access to*  
25 *Videotapes (Access to Videotapes)*, No. 03-89, 2003 WL 22053105, at \*3 (D. Md.  
26 Aug. 22, 2003) (directing apartment complex owner “merely to provide access” to  
27 videotapes in owner’s possession); *United States v. Hall*, 583 F. Supp. 717, 718–19  
28 (E.D. Va. 1984) (compelling credit card issuer to provide records in company’s  
possession); *United States v. X*, 601 F. Supp. 1039, 1042–43 (D. Md. 1984)  
(similar as to telephone billing records); *United States v. Doe*, 537 F. Supp. 838,  
840 (E.D.N.Y. 1982) (similar as to subscriber’s toll records).

1 In fact, the government does not cite a single case in which a court relied on  
2 the Act to compel a third party to assist in the execution of a warrant where the  
3 party did not possess or control the information sought. *See* Motion to Compel at  
4 8–10, 12, 16 (discussing cases involving landlords or credit card companies turning  
5 over materials in their possession, trap-and-trace or cellphone-monitoring cases  
6 involving information traveling through a medium controlled by the party, or the  
7 compelled production of a handwriting exemplar by the very individual whose  
8 handwriting was at issue); *see also In re Order Requiring Apple*, slip op. at 36 n.32  
9 (noting that each recipient of an assistance order in the cases relied upon by the  
10 government “was in possession of evidence of the crime under investigation”).<sup>2</sup>

11 This limitation on the Act—to information in the possession or control of  
12 third parties—is, in reality, a limit inherent in the warrant authority itself. Because  
13 the Act permits courts solely to effectuate (and not to broaden) some independent  
14 authority, the scope of that independent authority constrains the use of the Act.  
15 *Clinton v. Goldsmith*, 526 U.S. 529, 535–36 (1999). Here, the underlying order is a  
16 traditional search warrant, which confers on law enforcement the power to search  
17 and seize property, Fed. R. Crim. P. 41(b), not to force a third party to transform  
18 what has been seized. For example, a warrant that authorizes the government to  
19 seize records in a foreign language cannot be used as a basis for an order under the  
20 Act compelling a third party to translate the records into English. And a warrant  
21 that authorizes the government to seize a block of clay cannot be used to compel a

---

22 <sup>2</sup> The government does cite a set of recently disclosed cases in which it obtained  
23 orders under the Act compelling Apple to use an existing technical tool to extract  
24 data stored on iPhones running older versions of the iPhone’s operating system.  
25 *See* Tr. of Oral Argument at 24, *In re Order Requiring Apple*, No. 1:15-mc-O  
26 1902-JO (E.D.N.Y. Oct. 26, 2015). Those orders appear to have been uncontested  
27 until recently, when Magistrate Judge Orenstein questioned the legality of the  
28 practice, *see* Application at 12 n.5, invited adversarial briefing, and ultimately  
ruled against the government. *See In re Order Requiring Apple*, slip op.

1 sculptor to mold a figurine. In this case, the warrant authorized the government to  
2 seize and search a private mobile device. That the information on the device may  
3 be undecipherable does not entitle the government to rely on the warrant as a basis  
4 to compel a third party to transform that information.<sup>3</sup>

5 **B. The assistance the government seeks is unreasonably burdensome.**

6 Apple may not be compelled under the All Writs Act to assist the  
7 government here because the assistance would be unreasonably burdensome. The  
8 government is attempting to force Apple to design and build new software that  
9 would subvert several of the core security features that Apple has built into its  
10 phones and operating systems and on which its customers rely for the security of  
11 their personal information. No court has ever issued an even remotely comparable  
12 order under the All Writs Act. To the contrary, courts have compelled assistance  
13 under the Act only where the party lacked a “substantial interest in not providing  
14 assistance.” *N.Y. Tel. Co.*, 434 U.S. at 174. In *New York Telephone*, for example,  
15 the Supreme Court emphasized that the order sought would require “minimal  
16 effort” from the company, was not “offensive” to the company, and would not  
17 “disrupt[]” the company’s “operations.” *Id.* at 174–75. And in many cases since,  
18

---

19  
20 <sup>3</sup> The fact that Apple licenses its mobile operating system does not confer on  
21 Apple ownership of or control over all iPhones or, most relevantly, the private data  
22 stored on them. Real property analogies are instructive. The Supreme Court has  
23 long recognized that a tenant, lessee, or licensee does not cede his control over or  
24 privacy interest in rented property, even when the owner retains implied or express  
25 permission to enter the property for a specific purpose. *See, e.g., Chapman v.*  
26 *United States*, 365 U.S. 610 (1961); *United States v. Henderson*, 241 F.3d 638, 647  
27 (9th Cir. 2001). Furthermore, now that consumer products increasingly contain  
28 licensed software, the government’s theory that a license confers ownership would  
trigger “a virtually limitless expansion of the government’s legal authority to  
surreptitiously intrude on personal privacy.” *See In re Order Requiring Apple*, slip  
op. at 32 n.26.

1 courts have repeatedly underscored the minimal effort required to comply with the  
2 requests they have granted.<sup>4</sup>

3 The burden imposed here, by contrast, would be unprecedented—not just in  
4 its effect on Apple, but in its consequences for Apple’s millions of customers.

5 It would require Apple to develop, build, and test a technical capability that,  
6 for security and privacy reasons, it does not want to build. This goes far beyond the  
7 “meager” burden permitted by *New York Telephone*, which emphasized that the  
8 assistance ordered was not “in any way burdensome,” and that pen registers were  
9 by no means “offensive” to the company, given that it “regularly employ[ed]”  
10 them in the course of its ordinary business. *Id.* at 172, 174–75. Apple does not  
11 possess, let alone “regularly employ,” the software the government seeks. And  
12 even the government, in a related case involving Apple, appears to have  
13 recognized that compelling the creation of new software and new technical  
14 capabilities is a novel use of the Act. In that case, the government sought to compel  
15

---

16 <sup>4</sup> See, e.g., *Bell Telephone*, 610 F.2d at 1152, 1153, 1155 (“Tracing calls on  
17 [electronic switching system (ESS) equipment] is relatively simple” and “the  
18 central offices that served the telephones receiving the traced calls used ESS  
19 equipment,” therefore “these traces would cause a minimal disruption of normal  
20 operations.”); *Mountain Bell*, 616 F.2d at 1132 (“The Order was extremely narrow  
21 in scope, restricting the operation to ESS facilities, excluding the use of manual  
22 tracing, *prohibiting any tracing technique which required active monitoring* by  
23 company personnel, and requiring that operations be conducted ‘with a minimum  
24 of interference to the telephone service.’” (emphasis added)); *Hall*, 583 F. Supp. at  
25 721 (noting bank was already “in the business . . . of issuing credit” and “routinely,  
26 indeed monthly, compile[d] a list of all the purchases and the amounts of those  
27 purchases”); *United States v. X*, 601 F. Supp. at 1043 (“[D]irecting the out-of-state  
28 telephone company to provide the Government with telephone toll records of the  
subscriber [which] will not be ‘unduly burdensome,’ as such records are seemingly  
readily available and are maintained in the ordinary course of business.”); *Access  
to Videotapes*, 2003 WL 22053105, at \*3 (“[T]he only cooperation required by the  
apartment complex is merely to provide access to surveillance tapes already in  
existence, rather than any substantive assistance, and nothing more.”).

1 Apple to use a technical capability it already possessed (which could be used to  
2 extract data from older, less-secure iPhones), and expressly distinguished the order  
3 it sought on that basis. *See* Government’s Reply at 25, *In re Order Requiring*  
4 *Apple*, No. 1:15-mc-01902-JO (E.D.N.Y. Oct. 22, 2015) (stating that “the order in  
5 this case would not require Apple to make any changes to its software or hardware,  
6 and it would not require Apple to introduce any new ability to access data on its  
7 phones. It would simply require Apple to use its existing capability to bypass the  
8 passcode”).

9         Moreover, the burden imposed by the government’s request extends far  
10 beyond Apple itself. If granted, the request would establish a precedent that would  
11 undermine the security of hundreds of millions of iPhones and other devices, relied  
12 upon by countless individuals to protect sensitive and private information. If the  
13 government’s interpretation of the law holds, not only could it force Apple to  
14 create the cryptographically signed software it seeks here, but it could force Apple  
15 to deliver similar signed software using Apple’s automatic-update infrastructure.  
16 *See also* Mot. to Vacate at 26 (noting prospect of “forcing a software company to  
17 insert malicious code in its autoupdate process”). This would be devastating for  
18 cybersecurity, because it would cause individuals to legitimately fear and distrust  
19 the software update mechanisms built into their products. *See* Christopher  
20 Soghoian, *The Technology at the Heart of the Apple–FBI Debate, Explained*,  
21 Wash. Post, Feb. 29, 2016, <http://wapo.st/1T6hk3F>.

22         Simply put, what the government seeks here is an authority that would  
23 undermine American and global trust in software security updates, with  
24 catastrophic consequences for digital security and privacy.  
25

26         These burdens are particularly acute given the ever-growing threat of  
27 cyberattack. President Obama has identified cyber threats as “one of the most  
28 serious economic national security challenges that we face as a nation.” President



1 Barack Obama, Remarks by the President at the Cybersecurity and Consumer  
2 Protection Summit (Feb. 13, 2015), <http://1.usa.gov/21wkz9y>. And Americans now  
3 worry more about hacking crimes than any other.<sup>5</sup> That fear is justified: Three in  
4 five Californians (more than 49 million individuals) were affected by a security  
5 breach in just the past four years.<sup>6</sup> The public now understandably decides which  
6 technology to use based on its security.<sup>7</sup> As President Obama has recognized,  
7 “attacks are getting more and more sophisticated every day. So we’ve got to be just  
8 as fast and flexible and nimble in constantly evolving our defenses.” *Id.* Apple’s  
9 ability to deliver trusted, prompt updates to its consumers plays a vital role in  
10 protecting hundreds of millions of people from sophisticated cyberattacks.

11 In the face of the growing threat posed by cyberattacks and corresponding  
12 consumer concern over privacy, requiring Apple to build a deliberately weakened  
13 version of its mobile operating system would be particularly onerous. Apple has  
14 invested significant resources into making its devices as secure as possible. As a  
15 result, information security is now one of the primary features that Apple’s  
16 products deliver. No court has ever issued an All Writs Act order requiring a  
17 company to subvert the core of its product. As the Ninth Circuit held in a related  
18

---

19 <sup>5</sup> Rebecca Rifkin, *Hacking Tops List of Crimes Americans Worry About Most*,  
20 Gallup (Oct. 27, 2104), [http://www.gallup.com/poll/178856/hacking-tops-list-](http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx)  
21 [crimes-americans-worry.aspx](http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx).

22 <sup>6</sup> Cal. DOJ, California Data Breach Report (Feb. 2016), <https://oag.ca.gov/breachreport2016>.

23 <sup>7</sup> See *Building Consumer Trust: Protecting Personal Data in the Consumer*  
24 *Product Industry* 5–6, Deloitte Univ. Press (2014), [https://d2mtr37y39tpbu.](https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumer-trust_MASTER.pdf)  
25 [cloudfront.net/wp-content/uploads/2014/11/DUP\\_970-Building-consumer-](https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumer-trust_MASTER.pdf)  
26 [trust\\_MASTER.pdf](https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumer-trust_MASTER.pdf); Malena Carollo, *Survey: Consumers Reject Companies That*  
27 *Don’t Protect Privacy*, Christian Sci. Monitor (Jan. 29, 2016), [http://www.](http://www.csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-that-don-t-protect-privacy)  
28 [csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-](http://www.csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-that-don-t-protect-privacy)  
[that-don-t-protect-privacy](http://www.csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-that-don-t-protect-privacy).

1 context in *The Company v. United States*, 349 F.3d 1132 (9th Cir. 2003), Title III  
2 of the Wiretap Act—which expressly authorizes third-party assistance—could not  
3 be interpreted to compel the assistance of a company where doing so would cause  
4 a “complete disruption” of a service it offered. *Id.* at 1145.

5       Relatedly, other courts have considered the security risks to third parties that  
6 would be created by compliance with orders under the All Writs Act. In *Plum*  
7 *Creek Lumber Co. v. Hutton*, 608 F.2d 1283 (9th Cir. 1979), the Ninth Circuit  
8 addressed the Occupational Safety and Health Administration’s attempt to require  
9 workers at a lumber factory to wear noise-level and air-quality monitoring devices.  
10 The Ninth Circuit refused to compel employees to wear the devices, in significant  
11 part because the monitors posed a safety risk to the company’s employees. *Id.* at  
12 1286, 1289. The government cites *Plum Creek* for the proposition that the All  
13 Writs Act permits the government to compel “nonburdensome technical  
14 assistance,” but in that case and *The Company*, the Ninth Circuit also recognized  
15 that the Act does not permit the government to compel assistance that substantially  
16 interferes or is incompatible with a business’s operation, or places undue burdens  
17 on third parties.

18       That Apple’s employees might have the technical know-how to create the  
19 software the government seeks is not material. There was no question that the  
20 company in *Plum Creek* had the ability to provide the assistance the government  
21 demanded (and failed to obtain). Apple is being asked to break the security  
22 protections it has spent considerable resources developing, that are an integral part  
23 of its products, and that serve as essential safeguards for millions of iPhone users.  
24 That assistance would be unreasonably burdensome.

1           **C.     The government has failed to demonstrate that the assistance it**  
2           **seeks is absolutely necessary.**

3           The government has not demonstrated that the order it seeks is “necessary”  
4 within the meaning of the All Writs Act. In *New York Telephone*, the Supreme  
5 Court authorized the third-party assistance sought in part because there was “no  
6 conceivable way” to effectuate the underlying surveillance order without such  
7 assistance. 434 U.S. at 175. Subsequent courts have interpreted *New York*  
8 *Telephone* to require absolute necessity before compelling third-party assistance  
9 under the Act. *See, e.g., Mountain Bell*, 616 F.2d at 1129 (“[T]he refusal by [the  
10 company] to cooperate would have completely frustrated any attempt to  
11 accomplish the tracing operation.”); *United States v. Hall*, 583 F. Supp. 717, 721  
12 (E.D. Va. 1984) (“[T]he Supreme Court has said that the assistance of the third  
13 party must be absolutely necessary.”).

14           The government has failed to make that showing here. In particular, the  
15 government has not shown it has exhausted other means of accessing the data on  
16 the iPhone at issue. *See In re Order Requiring Apple*, slip op. at 45–48.

17           **D.     Congress has deliberately withheld the authority sought here.**

18           Congress has deliberately withheld the authority the government seeks here,  
19 and it would therefore be inappropriate to supply it through the Act. The Act is not  
20 a substitute for authority that Congress has chosen not to confer. In *New York*  
21 *Telephone*, for example, the Supreme Court relied heavily on the fact that  
22 Congress had plainly intended to authorize the government to install precisely the  
23 kind of tracking device the government sought to install. *See* 434 U.S. at 176  
24 (“Congress clearly intended to permit the use of pen registers by federal law  
25 enforcement . . . .”); *see also In re Application of the U.S. for an Order Authorizing*  
26 *Disclosure of Location Information of a Specified Wireless Tel.*, 849 F. Supp. 2d  
27 526, 579 (D. Md. 2011) (“[T]he Supreme Court acknowledged and deferred to  
28

1 congressional approval of a pen register as a permissible law enforcement tool.”).  
2 And in other cases, courts have similarly looked to congressional intent in  
3 determining the reach of the Act. *See Plum Creek*, 608 F.2d at 1290 (“This circuit  
4 has never held that the district court has such wide-ranging inherent powers that it  
5 can impose a duty on a private party when Congress has failed to impose one.”);  
6 *Application of the U.S. for Relief*, 427 F.2d 639, 644 (9th Cir. 1970) (denying the  
7 government’s request for assistance under the All Writs Act because of the  
8 legislative history and comprehensiveness of the underlying statutory scheme); *In*  
9 *re Application of the U.S. for an Order Authorizing the Use of a Pen Register*, 396  
10 F. Supp. 2d at 325 (The All Writs Act is not “a mechanism for the judiciary to give  
11 [the government] the investigative tools that Congress has not.”).<sup>8</sup>

12         In this case, Congress has quite deliberately refused to authorize law  
13 enforcement to force manufacturers of mobile devices to unlock those devices.  
14 During the last few years, there has been a robust legislative debate—instigated by  
15 the government itself—about whether technology companies such as Apple should  
16 be required to build “backdoors” into the security features now commonly included  
17 in computers, mobile devices, and communications software. These backdoors  
18 would enable law enforcement to access data that might otherwise, in some  
19 circumstances, be inaccessible. Though the debate has been wide-ranging,  
20 Congress has, thus far, not acceded to the government’s demands.<sup>9</sup> In fact, on the  
21

---

22         <sup>8</sup> *See also Application of the U.S.*, 427 F.2d 639, 644 (9th Cir. 1970) (holding  
23 that because there was no statutory authorization, a federal district court could not  
24 compel a telephone company to provide technical cooperation in intercepting a  
25 wire communication) (later superseded by amendments to Title III, 18 U.S.C.  
§§ 2511, 2518 & 2520, providing express authority for assistance in certain  
circumstances).

26         <sup>9</sup> *See Erin Kelley, Congress Wades into Encryption Debate with Bill to Create*  
27 *Expert Panel*, USA Today (Jan. 11, 2016), <http://usat.ly/1UK35ij>; T.C. Sottek,  
28 *Hillary Clinton on Encryption: ‘Maybe the Back Door Isn’t the Right Door,’* The

1 basis of the security risks related to backdoors, the Obama administration  
2 reportedly shelved its effort to seek legislation mandating their creation.<sup>10</sup>

3 Congress has thus far refused, in other words, to give law enforcement what  
4 it has asked for here: the ability to compel companies to actively bypass the  
5 security built into their products.

6 In a closely related context, Congress has even more explicitly withheld  
7 similar authority. The Communications Assistance for Law Enforcement Act  
8 (“CALEA”), passed in 1994, requires “telecommunications carriers” to ensure  
9 their equipment, facilities, and services are capable of intercepting individuals’  
10 communications in real time. But when Congress enacted CALEA, it expressly  
11 exempted “information services” of the kind that Apple provides. *See* 47 U.S.C.  
12 §§ 1002(b)(2), 1001(6)(B)(iii). In other words, CALEA exempts companies like  
13 Apple from the requirement that they build interception features into their  
14 communications services and products. *See In re Order Requiring Apple*, slip op.  
15 at 20 (concluding that CALEA represented a “legislative decision” not to require  
16 information services to affirmatively assist law enforcement).

17  
18 In recent sessions of Congress, the FBI has campaigned for Congress to  
19 expand CALEA’s reach to cover companies like Apple.<sup>11</sup> But the FBI’s proposals

---

20  
21 Verge (Dec. 19, 2015), <http://www.theverge.com/2015/12/19/10628208/hillary-clinton-back-door-debate>; Kif Leswing, *GOP Debate: What Republicans Got Wrong About Technology*, Fortune (Dec. 16, 2015), <http://for.tn/1Q4C73Z>.

22  
23 <sup>10</sup> Nicole Perlroth & David E. Sanger, *Obama Won’t Seek Access to Encrypted User Data*, N.Y. Times (Oct. 10, 2015), <http://nyti.ms/1G6YAaL>.

24  
25 <sup>11</sup> *See* Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. Times (Sept. 27, 2010), <http://nyti.ms/1TH2kcD>; Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. Times (May 7, 2013), <http://nyti.ms/1WLESJo>.

1 have met stiff resistance from Congress, technology experts, and a number of  
2 former national security officials.<sup>12</sup>

3 In short, Congress has had ample opportunity, in multiple contexts, to  
4 compel companies such as Apple to build surveillance mechanisms into their  
5 products to facilitate government access, but Congress has declined to do so.  
6 Because Congress has deliberately withheld the authority the government asks for  
7 here, the All Writs Act may not be used to confer it.

8 **II. The order the government seeks violates the Fifth Amendment.**

9  
10 The compelled assistance the government seeks from Apple is unlawful for  
11 the separate and independent reason that it violates the Fifth Amendment. At the  
12 very least, interpreting the All Writs Act in the way the government proposes  
13 raises serious constitutional questions that this Court has a duty to avoid. *See Clark*  
14 *v. Martinez*, 543 U.S. 371, 380–81 (2005).

15 There is a constitutional limit to the assistance that law enforcement may  
16 compel of third parties. It is true, of course, that law enforcement can compel  
17 assistance in some circumstances—it can, for example, compel citizens to give  
18 testimony, to produce relevant documents in their possession, to permit entry for  
19 the seizure of evidence, and the like. Indeed, the government has requested, and  
20 Apple has provided, that sort of assistance in this case.

21 But there is an outer bound to what law enforcement may require of innocent  
22 third parties. *Cf. Cty. of Sacramento v. Lewis*, 523 U.S. 833, 845 (1998) (The  
23

---

24 <sup>12</sup> *See* Andrea Peterson, *Congressman with Computer Science Degree:*  
25 *Encryption Back-doors Are “Technologically Stupid,”* Wash. Post (Apr. 30, 2015),  
26 <http://wapo.st/1RESSn1>; Susan Page, *Ex-NSA Chief Backs Apple on iPhone ‘Back*  
27 *Doors,’* USA Today (Feb. 24, 2016), <http://usat.ly/1LAPJjq>; Mike McConnell,  
28 Michael Chertoff & William Lynn, *Opinion, Why the Fear Over Ubiquitous Data*  
*Encryption Is Overblown*, Wash. Post (July 28, 2015), <http://wapo.st/1ShCPic>.

1 Supreme Court has “emphasized time and again that “[t]he touchstone of due  
2 process is protection of the individual against arbitrary action of government.”  
3 (alteration in original) (quoting *Wolff v. McDonnell*, 418 U.S. 539, 558 (1974))).

4 This principle is evident in the Supreme Court’s Fifth Amendment cases,  
5 which recognize that the government may not exercise authority inconsistent with  
6 “the concept of ordered liberty.” *United States v. Salerno*, 481 U.S. 739, 746  
7 (1987) (quoting *Palko v. Connecticut*, 302 U.S. 319, 325–26 (1937)). And it flows,  
8 in significant part, from the incompatibility of excessive law-enforcement authority  
9 with free democracy. “[T]he resistance of the colonies to the oppressions” of  
10 Britain were animated in large part by the over-zealous use of so-called “writs of  
11 assistance,” which “had given customs officials blanket authority to search where  
12 they pleased.” *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). James Otis  
13 denounced them as “the worst instrument of arbitrary power, the most destructive  
14 of English liberty and the fundamental principles of law” because they placed “the  
15 liberty of every man in the hands of every petty officer.” *Boyd v. United States*,  
16 116 U.S. 616, 625 (1886). The Framers’ “revulsion” against these excesses  
17 reflected the view that a free society must circumscribe the government’s power to  
18 search for evidence of crimes, including by eliminating “blanket authority to  
19 search” and by constraining the government’s power to sweep up innocent third  
20 parties. *Stanford*, 379 U.S. at 481–82; *see also Arizona v. Hicks*, 480 U.S. 321, 329  
21 (1987) (“But there is nothing new in the realization that the Constitution  
22 sometimes insulates the criminality of a few in order to protect the privacy of us  
23 all.”).

24 Yet what the government proposes here is to transform the All Writs Act  
25 into a source of “blanket authority” as intrusive as any writ of assistance. *Stanford*,  
26 379 U.S. at 481; *see also In re Order Requiring Apple*, slip op. at 44 (noting that  
27 the government’s view of the All Writs Act contains no “principled limit on how  
28

1 far a court may go in requiring a person or company to violate the most deeply-  
2 rooted values”). The government seeks to compel an innocent third party into  
3 becoming an agent of the state, to conscript a private entity into a criminal  
4 investigation, and to require it to develop information for the government that is  
5 neither in its possession nor control. This is a tactic foreign to free democracies.  
6 And it presents an unparalleled danger of eroding the public trust—both of  
7 government and between citizens—necessary to ordered liberty.<sup>13</sup>

8         The Supreme Court has not explicitly addressed the constitutional  
9 constraints on the government’s ability to compel an innocent third party to  
10 participate in a criminal investigation. But it has crafted a judicial limit on the All  
11 Writs Act that is best explained as recognition that the conscription of third parties  
12 by the police raises troubling constitutional questions. In *New York Telephone*, it  
13 said that courts may not rely on the Act to impose “unreasonable burdens.” *N.Y.*  
14 *Tel. Co.*, 434 U.S. at 172. That phrase does not appear anywhere in the Act,  
15 however, and appears to reflect, instead, the intuitive notion that law enforcement’s  
16 authority to enlist third parties in official investigations abuts more fundamental  
17 constitutional freedoms.

18         Where precisely the line lies between permissible and impermissible  
19 conscription in law-enforcement investigations is a question perhaps unanswerable  
20 in the abstract. And it would undoubtedly be a more complicated one were  
21 Congress itself to clearly and expressly require the sort of assistance the  
22

---

23         <sup>13</sup> The few exceptions prove the rule. Consistent with due process’s focus on  
24 history and practice, the government’s power to conscript has been recognized  
25 only in narrow contexts in which the power is so tied to modern statehood that it  
26 effectively predates the Constitution. *See, e.g., Arver v. United States*, 245 U.S.  
27 366, 378 (1918) (power to compel military service inherent in “very conception of  
28 just government”); *Butler v. Perry*, 240 U.S. 328, 331 (1916) (compelled work on  
public roads).



1 government seeks in a manner that could be fairly understood as regulatory, rather  
2 than investigative, in nature. *See, e.g., New Motor Vehicle Bd. v. Orrin W. Fox Co.*,  
3 439 U.S. 96, 106–07 (1978) (“At least since the demise of the concept of  
4 ‘substantive due process’ in the area of economic regulation, this Court has  
5 recognized that legislative bodies have broad scope to experiment with economic  
6 problems.” (alteration and quotation marks omitted)).

7         But wherever the line is, the government’s demand in this case plainly  
8 crosses it. Many factors set the request here apart from any law enforcement has  
9 made before. First, the demand here, and the precedent it would set, implicates the  
10 rights of countless Americans, not just those of Apple. The government’s demand  
11 would inevitably weaken the security of all of Apple’s users—everyday Americans  
12 attempting to secure their private data and their communications. Second, it would  
13 require Apple to design and create software in service of a governmental  
14 investigation, even though Apple does not possess or control the information the  
15 government seeks. Third, Congress has not enacted a statute requiring technology  
16 companies to be able to actively bypass the security built into their products. *See*  
17 *supra* Part I.A–B. Finally, it would require Apple to provide this novel assistance  
18 in aid of a criminal investigation to which it has little connection, despite its  
19 vehement objection to doing so. *Stanford*, 379 U.S. at 485 (First, Fourth, and Fifth  
20 “amendments are indeed closely related, safeguarding not only privacy and  
21 protection against self-incrimination but ‘conscience and human dignity and  
22 freedom of expression as well.’”).

23         The effect of the government’s demands would be to conscript a private  
24 party with little connection to the government’s criminal investigation into  
25 breaking the security of its own products and, thereby, weakening the security of  
26 all its users.

1 In the history, traditions, and norms of compelled investigative assistance,  
2 such a demand is plainly unprecedented. *See Lewis*, 523 U.S. at 857 (Kennedy, J.,  
3 concurring) (explaining that the substantive due process inquiry “ask[s] whether or  
4 not the objective character of certain conduct is consistent with our traditions,  
5 precedents, and historical understanding of the Constitution and its meaning”).  
6 And for good reason. On the government’s apparent understanding of its authority  
7 under the Act, for example, it is not clear what would prevent law enforcement  
8 from obtaining an order compelling: an individual to spy on her neighbor; an  
9 employee of the ACLU to retrieve information on another employee’s personal  
10 device; a cybersecurity firm to remotely hack into a customer’s network to obtain  
11 evidence; or even the friend of a Black Lives Matter organizer to seek out  
12 information and report on that person’s plans for a peaceful protest.

13 The government’s theory threatens a radical transformation of the  
14 relationship between the government and the governed. But the Court need not  
15 address the profound constitutional questions provoked by that threat. It is enough  
16 that the government’s theory raises them to trigger the Court’s obligation to  
17 interpret the Act to avoid them.

## 18 CONCLUSION

19 For these reasons, the Court should deny the government’s request.  
20

21  
22 March 2, 2016

Respectfully Submitted,

23  
24 By: \_\_\_\_\_  
25 Peter Bibring  
26 ACLU OF SOUTHERN  
27 CALIFORNIA  
28 pbibring@aclusocal.org  
1313 West Eighth Street  
Los Angeles, CA 90017

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

Telephone: (213) 977-9500

Alex Abdo  
Esha Bhandari  
Eliza Sweren-Becker\*  
Brett Max Kaufman  
aabdo@aclu.org  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
125 Broad Street, 18th Floor  
New York, NY 10004  
Telephone: (212) 549-2500

Linda Lye (SBN 215584)  
llye@aclunc.org  
ACLU OF NORTHERN  
CALIFORNIA  
39 Drumm Street, 2nd Floor  
San Francisco, CA 94111  
Telephone: (415) 621-2493

David Loy (SBN 229235)  
davidloy@aclusandiego.org  
ACLU OF SAN DIEGO AND  
IMPERIAL COUNTIES  
San Diego, CA 92138  
Telephone: (619) 232-2121

\*Application for admission to the bar  
pending

Attorneys for *amici curiae*