

Case 5:16-cm-00010-SP Document 55 Filed 03/03/16 Page 2 of 4 Page ID #:762

The Court has considered the Application of the American Civil Liberties Union ("ACLU"), ACLU of Southern California, ACLU of Northern California, and ACLU of San Diego and Imperial Counties for leave to file a brief of amici curiae. The court hereby grants the application. The proposed brief attached to the application is deemed filed as of the date of this order. March _______, 2016 Honorable Sheri Pym United States Magistrate Judge Submitted by: Peter Bibring. Attorney for Proposed Amici, ACLU et al.

Case 5:16-cm-00010-SP Document 55 Filed 03/03/16 Page 3 of 4 Page ID #:763

PROOF OF SERVICE

I am employed in the County of Los Angeles, State of California. I am over the age of 18 and not a party to the within action. My business address is ACLU of Southern California, 1313 West 8th Street, Los Angeles, CA 90017.

On March 2, 2016, I caused to be served through mail (USPS) and e-mail the foregoing document described as:

[PROPOSED] ORDER GRANTING LEAVE TO FILE BRIEF OF AMICI CURIAE BY AMERICAN CIVIL LIBERTIES UNION ET AL.

on each person on the attached Service List.

Executed on March 2, 2016, in Los Angeles, California.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I am employed in the office of a member of the bar of this Court at whose direction the service was made.

Diana Gonzalez

Print Name

Signature

Scrvice List

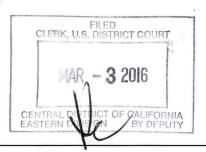
Scrvice Type	Counsel Served	Party
Mail & E-mail	Theodorc J. Boutrous, Jr. Nicola T. Hanna Eric D. Vandevelde Gibson, Dunn & Crutcher LLP 333 South Grand Avenuc Los Angeles, CA 90071-3197 Telephone: (213) 229-7000 Facsimile: (213) 229-7520 Email: tboutrous@gibsondunn.com nhanna@gibsondunn.com evandevelde@gibsondunn.com	Apple, Inc.
	evandeverde@grosondum,com	

Cole wed 17:19 Fax 2139775297 actu-sc Q005/005 Case 5:16-cm-00010-SP Document 55 Filed 03/03/16 Page 4 of 4 Page ID #:764

1	Mail & E-mail	Theodore B. Olson	
- 11		A MCOROL C IN CHOOM	Apple, Inc.
2		Gibson, Dunn & Crutcher LLP	1 appio, inc.
		1050 Connecticut Avenue, N.W.	
3		Washington, DC, 20036-5306	
4		Telephone: (202) 955-8500	
_		Facsimile: (202) 467-0539	
5		Email: tolson@gibsondunn.com	
6	Mail & E-mail	Marc J. Zwillinger	Apple, Inc.
-,		Jefffrey G. Landis	
7		Zwillgen PLLC	
8		1900 M Street N.W., Suite 250	
9		Washington, D.C. 20036	
9		Telephone: (202) 706-5202	
10		Facsimile: (202) 706-5298	
11		Email: marc@zwillgen.com	·
	A December 1	jeff@zwillgen.com	
12	Mail & E-mail	Eileen M. Decker	United States
13		Patricia A. Donahue	of America
1		Tracy L. Wilkison	
14		Allen W. Chiu	
15		1500 United States Courthouse	
		7312 North Spring Street	
16		Los Angeles, California 90012	
17		Telephone: (213) 894-0622/2435	
		Facsimile: (213) 894-8601	
18		Email: Tracy. Wilkison@usdoj.gov	
19	777	Allen.Chiu@usdoj.gov	

Case 5:16-cm-00010-SP Document 56 Filed 03/03/16 Page 1 of 2 Page ID #:765

Name and address: Peter Bibring ACLU Foundation of Southern California 1313 West Eighth Street Los Angeles, CA 90017



UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA

USA

CASE NUMBER:

5:16-cm-00010-SP-1

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 35K GD 203

DEFENDANT(S)

CASE NUMBER:

5:16-cm-00010-SP-1

NOTICE OF APPEARANCE OR WITHDRAWAL OF COUNSEL

INSTRUCTIONS

Appearance of Counsel:

Attorneys may use this form to enter an appearance in a case, or to update the docket of a case to reflect a prior appearance. To do so, complete Sections I, II, and IV of this form, then file and serve the form in the case. (Using an attorney's CM/ECF login and password to file this form will expedite the addition of that attorney to the docket as counsel of record.)

Withdrawal of Counsel:

This form may be used to terminate an attorney's status as counsel of record for a party in three situations: (1) the attorney being terminated has already been relieved by the Court, but the docket does not yet reflect that fact; (2) at least one member of the attorney's firm or agency will continue to represent that party and the withdrawing attorney is not the only member of the Bar of this Court representing that party; or (3) the represented party has been dismissed from the case, but the attorneys are still receiving notices of electronic filing. For any of these situations, complete Sections I, III, and IV of this form, then file and serve the form in the case.

<u>Note</u>: In situations not covered above, attorneys seeking to withdraw from a case must first obtain permission from the Court. In such circumstances, attorneys should complete and file a "Request for Approval of Substitution or Withdrawal of Counsel" (Form G-01) rather than this "Notice of Appearance or Withdrawal of Counsel" (Form G-123). See Form G-01 for further information.

SECTION I - IDENTIFYING INFORMATION

Please complete the following information for the attorney you wish to add or remove (if removing an attorney, provide the information as it <u>currently</u> appears on the docket; if appearing pro hac vice, enter "PHV" in the field for "CA Bar Number"):

Name: Peter Bibring	CA Bar Number: 223981	
Firm or agency: ACLU Foundation of Southern California		
Address: 1313 West Eighth Street, Los Angeles CA 90017		
Telephone Number: 213-977-9500x.295	Fax Number:	213-977-5297
Email: pbibring@aclusocal.org		
Counsel of record for the following party or parties: Amicus	Curiae American	Civil Liberties Union, ACLU of Northern
California, ACLU of Southern California, and ACLU of San	Diego And Imperi	al Counties

SECTION II - TO ADD AN ATTORNEY TO THE DOCKET

Pleas	se select one of the following options:		
	The attorney listed above has already appeared as counsel of record in this case and should have been added to the docket. The date of the attorney's first appearance in this case:		
	The filing of this form constitutes the first appearance in this case of the attorney listed above. Other members of this attorney's firm or agency have previously appeared in the case.		
\times	The filing of this form constitutes the first appearance in this case of the attorney listed above. No other members of this attorney's firm or agency have previously appeared in the case.		
	By order of the court dated in case number (see attached copy), the attorney listed above may appear in this case without applying for admission to practice <i>pro hac vice</i> .		
	This case was transferred to this district by the Judicial Panel on Multidistrict Litigation ("JPML") pursuant to 28 U.S.C. § 1407 from the District of, where it was assigned case number The attorney listed above is counsel of record in this case in the transferee district, and is permitted by the rules of the JPML to continue to represent his or her client in this district without applying for admission to practice <i>pro hac vice</i> and without the appointment of local counsel.		
	On, the attorney listed above was granted permission to appear in this case <i>pro hac vice</i> before the Bankruptcy Court, and L.Bankr.R. 8 authorizes the continuation of that representation in this case before the District Court.		
In ad	dition, if this is a criminal case, please check the applicable box below. The attorney listed above is:		
	☐ USAO ☐ FPDO ☐ CJA Appointment ☒ Pro Bono ☐ Retained		
SEC 7	TION III - TO REMOVE AN ATTORNEY FROM THE DOCKET		
Pleas	e select one of the following options:		
	The attorney named above has already been relieved by the Court as counsel of record in this case and should have been removed from the docket. Date of the order relieving this attorney:		
	Please remove the attorney named above from the docket of this case; at least one member of the firm or agency named above, and at least one member of the Bar of this Court, will continue to serve as counsel of record for the party or parties indicated. (Note: if you are removing yourself from the docket of this case as a result of separating from a firm or agency, you should consult Local Rules 5-4.8.1 and 83-2.4 and Form G-06 ("Notice of Change of Attorney Business or Contact Information"), concerning your obligations to notify the Clerk and parties of changes in your business or contact information.)		
	The represented party has been dismissed from the case, but the attorneys are still receiving notices of electronic filing. Date party was dismissed:		
	The attorney named above was appointed on appeal and the appeal has been adjudicated. Date the mandate was filed:		
<u>SECT</u>	TION IV - SIGNATURE		
I real	uest that the Clerk update the docket as indicated above.		
rrequ	acst that the ciefk update the docker as indicated above.		
Ι	Date: March 2, 2016 Signature:		
	Name: Peter Bibring		

Courtroom: Courtroom 3 or 4

Judge: Hon. Sheri Pym

26

27

TABLE OF CONTENTS 1 2 TABLE OF AUTHORITIES..... 3 INTERESTS OF AMICI CURIAE 4 SUMMARY OF ARGUMENT......1 5 BACKGROUND2 6 ARGUMENT.....4 7 8 The All Writs Act does not authorize the government to compel I. Apple to create and authenticate software that would allow the 9 government to break into Apple's customers' devices.4 10 Apple is "far removed from the underlying controversy" A. 11 because it neither possesses nor controls the information the government seeks.....5 12 13 The assistance the government seeks is unreasonably В. burdensome. 8 14 The government has failed to demonstrate that the C. 15 16 Congress has deliberately withheld the authority sought D. 17 18 II. 19 20 21 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 5	Application of the U.S., 427 F.2d 639 (9th Cir. 1970)14
6 7	Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities (Mountain Bell), 616 F.2d 1122 (9th Cir. 1980)
8 9 10	Application of U.S. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder & Terminating Trap (Bell Telephone), 610 F.2d 1148 (3d Cir. 1979)
11	Arizona v. Hicks, 480 U.S. 321 (1987)
12	Arver v. United States, 245 U.S. 366 (1918)
13	Boyd v. United States, 116 U.S. 616 (1886)17
14	Butler v. Perry, 240 U.S. 328 (1916)
15	Chapman v. United States, 365 U.S. 610 (1961)8
16 17	Clark v. Martinez, 543 U.S. 371 (2005)16
18	Clinton v. Goldsmith, 526 U.S. 529 (1999)
19	Cty. of Sacramento v. Lewis, 523 U.S. 833 (1998)
 20 21 22 23 24 25 26 27 	In re Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011)
28	

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

Case 5:16-cm-00010-SP Document 57 Filed 03/03/16 Page 4 of 29 Page ID #:770

Case	5:16-cm-00010-SP Document 57 Filed 03/03/16 Page 5 of 29 Page ID #:771
1	Other Authorities
2 3	Andrea Peterson, Congressman with Computer Science Degree: Encryption Back-doors Are "Technologically Stupid," Wash. Post (Apr. 30, 2015), http://wapo.st/1RESSn1
4 5 6 7	Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry, Deloitte Univ. Press (2014), https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumertrust MASTER.pdf
8 9	Cal. DOJ, California Data Breach Report (Feb. 2016), https://oag.ca.gov/breachreport2016
10 11	Charlie Savage, <i>U.S. Tries to Make It Easier to Wiretap the Internet</i> , N.Y. Times (Sept. 27, 2010), http://nyti.ms/1TH2kcD
12 13	Charlie Savage, U.S. Weighs Wide Overhaul of Wiretap Laws, N.Y. Times (May 7, 2013), http://nyti.ms/1WLESJo
14 15	Christopher Soghoian, <i>The Technology at the Heart of the Apple–FBI Debate, Explained</i> , Wash. Post, Feb. 29, 2016, http://wapo.st/1T6hk3F
16 17 18	Erin Kelley, Congress Wades into Encryption Debate with Bill to Create Expert Panel, USA Today (Jan. 11, 2016), http://usat.ly/1UK35ij
19 20	Kif Leswing, GOP Debate: What Republicans Got Wrong About Technology, Fortune (Dec. 16, 2015), http://for.tn/1Q4C73Z15
21 22	Malena Carollo, Survey: Consumers Reject Companies That Don't Protect Privacy, Christian Sci. Monitor (Jan. 29, 2016), http://www.csmonitor.com/World/Passcode/2016/0129/Survey- Consumers-reject-companies-that-don-t-protect-privacy
23 24 25	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
26 27 28	Nicole Perlroth & David E. Sanger, <i>Obama Won't Seek Access to Encrypted User Data</i> , N.Y. Times (Oct. 10, 2015), http://nyti.ms/1G6YAvL
20	

Case	:16-cm-00010-SP Document 57 Filed 03/03/16 Page 6 of 29 Page ID #:772
1 2	President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://l.usa.gov/21wkz9y
3 4	Rebecca Rifkin, <i>Hacking Tops List of Crimes Americans Worry About Most</i> , Gallup (Oct. 27, 2104),
5	http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx
6 7	Susan Page, Ex-NSA Chief Backs Apple on iPhone 'Back Doors,' USA Today (Feb. 24, 2016), http://usat.ly/1LAPJjq16
8	T.C. Sottek, Hillary Clinton on Encryption: 'Maybe the Back Door Isn't the Right Door,' The Verge (Dec. 19, 2015),
10	http://www.theverge.com/2015/12/19/10628208/hillary-clinton-back-door-debate
11	Rules
12 13	Fed. R. Crim. P. 41
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

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

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

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

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

BACKGROUND

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

Case \$:16-cm-00010-SP Document 57 Filed 03/03/16 Page 9 of 29 Page ID #:775

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

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

ARGUMENT

I. The All Writs Act does not authorize the government to compel Apple to create and authenticate software that would allow the government to break into Apple's customers' devices.

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

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

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

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

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

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

A. Apple is "far removed from the underlying controversy" because it neither possesses nor controls the information the government seeks.

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

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

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

¹ See also In re Application of U.S. for an Order Directing a Provider of Commc'n Servs. to Provide Technical Assistance to Agents of the U.S. Drug Enforcement Admin., No. 15-1242 M, 2015 WL 5233551, at *5 (D.P.R. Aug. 27, 2015) (similar for the contents of electronic communications over mobile-phone network); In re Application of U.S. for an Order Directing X to Provide Access to Videotapes (Access to Videotapes), No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (directing apartment complex owner "merely to provide access" to videotapes in owner's possession); United States v. Hall, 583 F. Supp. 717, 718–19 (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).

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

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

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

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

B. The assistance the government seeks is unreasonably burdensome.

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

³ The fact that Apple licenses its mobile operating system does not confer on Apple ownership of or control over all iPhones or, most relevantly, the private data stored on them. Real property analogies are instructive. The Supreme Court has long recognized that a tenant, lessee, or licensee does not cede his control over or privacy interest in rented property, even when the owner retains implied or express permission to enter the property for a specific purpose. *See, e.g., Chapman v. United States*, 365 U.S. 610 (1961); *United States v. Henderson*, 241 F.3d 638, 647 (9th Cir. 2001). Furthermore, now that consumer products increasingly contain 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
 2
 3

45

6

7 8 9

1011

1213

1415

17

16

18 19

2021

22

2324

2526

27

28

courts have repeatedly underscored the minimal effort required to comply with the requests they have granted.⁴

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

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

⁴ See, e.g., Bell Telephone, 610 F.2d at 1152, 1153, 1155 ("Tracing calls on [electronic switching system (ESS) equipment] is relatively simple" and "the central offices that served the telephones receiving the traced calls used ESS equipment," therefore "these traces would cause a minimal disruption of normal operations."); Mountain Bell, 616 F.2d at 1132 ("The Order was extremely narrow in scope, restricting the operation to ESS facilities, excluding the use of manual tracing, prohibiting any tracing technique which required active monitoring by company personnel, and requiring that operations be conducted 'with a minimum of interference to the telephone service." (emphasis added)); Hall, 583 F. Supp. at 721 (noting bank was already "in the business . . . of issuing credit" and "routinely, indeed monthly, compile[d] a list of all the purchases and the amounts of those purchases"); United States v. X, 601 F. Supp. at 1043 ("[D]irecting the out-of-state 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.").

Case \$:16-cm-00010-SP Document 57 Filed 03/03/16 Page 16 of 29 Page ID #:782

2.7

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

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

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

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

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

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

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

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

⁷ See *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry* 5–6, Deloitte Univ. Press (2014), https://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/11/DUP_970-Building-consumertrust_MASTER.pdf; Malena Carollo, *Survey: Consumers Reject Companies That Don't Protect Privacy*, Christian Sci. Monitor (Jan. 29, 2016), http://www.csmonitor.com/World/Passcode/2016/0129/Survey-Consumers-reject-companies-that-don-t-protect-privacy.

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

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

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

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

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

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

D. Congress has deliberately withheld the authority sought here.

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

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

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

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

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

6

10 11

12 13

14 15

16 17

18

19 20

21

23

22

25

24

26 27

28

basis of the security risks related to backdoors, the Obama administration reportedly shelved its effort to seek legislation mandating their creation.¹⁰

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

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

In recent sessions of Congress, the FBI has campaigned for Congress to expand CALEA's reach to cover companies like Apple. 11 But the FBI's proposals

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

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

¹¹ 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.

have met stiff resistance from Congress, technology experts, and a number of former national security officials.¹²

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

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

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

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

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

¹² See Andrea Peterson, Congressman with Computer Science Degree: Encryption Back-doors Are "Technologically Stupid," Wash. Post (Apr. 30, 2015), http://wapo.st/1RESSn1; Susan Page, Ex-NSA Chief Backs Apple on iPhone 'Back Doors,' USA Today (Feb. 24, 2016), http://usat.ly/1LAPJjq; 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.

1
 2
 3

45

6

7 8

1011

9

1213

1415

1617

18

19 20

2122

2324

25

26 27

28

Supreme Court has "emphasized time and again that '[t]he touchstone of due process is protection of the individual against arbitrary action of government." (alteration in original) (quoting *Wolff v. McDonnell*, 418 U.S. 539, 558 (1974))).

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

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

6

7

8 9

10 11

12 13

14

15

16

17

18 19

20

21

22

23 24

25 26

27

28

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

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

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

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

1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | § 1 | §

6 7

8 9

10

1112

13

15

14

17

16

18

19

2021

22

2324

2526

2728

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

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

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

Case \$ 16-cm-00010-SP Document 57 Filed 03/03/16 Page 26 of 29 Page ID #:792

In the history, traditions, and norms of compelled investigative assistance, 1 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 not the objective character of certain conduct is consistent with our traditions, 4 precedents, and historical understanding of the Constitution and its meaning"). 5 And for good reason. On the government's apparent understanding of its authority under the Act, for example, it is not clear what would prevent law enforcement from obtaining an order compelling: an individual to spy on her neighbor; an 8 9 employee of the ACLU to retrieve information on another employee's personal device; a cybersecurity firm to remotely hack into a customer's network to obtain 10 evidence; or even the friend of a Black Lives Matter organizer to seek out 11 information and report on that person's plans for a peaceful protest. 12 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 interpret the Act to avoid them.

CONCLUSION

For these reasons, the Court should deny the government's request.

March 2, 2016

Respectfully Submitted,

Peter Bibring

ACLU OF SOUTHERN

CALIFORNIA

pbibring@aclusocal.org 1313 West Eighth Street Los Angeles, CA 90017

27 28

17

18

19

20

21

22

23

24

25

Case 5:16-cm-00010-SP	Document 57	Filed 03/03/16	Page 27 of 29 Page ID #:793
1		Tel	ephone: (213) 977-9500
2		Ale	ex Abdo
3			na Bhandari
4			za Sweren-Becker* ett Max Kaufman
5		aab	odo@aclu.org
6			TERICAN CIVIL LIBERTIES NION FOUNDATION
7			Broad Street, 18th Floor
8			w York, NY 10004 ephone: (212) 549-2500
9		161	ephone. (212) 349-2300
10			da Lye (SBN 215584)
		_	e@aclunc.org LU OF NORTHERN
11		CA	ALIFORNIA
12			Drumm Street, 2nd Floor
13			n Francisco, CA 94111 ephone: (415) 621-2493
14		~	:11 (GD) (2002 5)
15			vid Loy (SBN 229235) ridloy@aclusandiego.org
16			LU OF SAN DIEGO AND
17			PERIAL COUNTIES
18			n Diego, CA 92138 ephone: (619) 232-2121
19			
20			pplication for admission to the bar ding
21		-	_
22		Att	orneys for <i>amici curiae</i>
23			
24			
25			
26			
27			
28			

2

3 4

5

6

7 8

9

11

10

12 13

14

15

16

17

18 19

20 21

22 23

24 25

26 27

28

PROOF OF SERVICE

I am employed in the County of Los Angeles, State of California. I am over the age of 18 and not a party to the within action. My business address is ACLU of Southern California, 1313 West 8th Street, Los Angeles, CA 90017.

On March 2, 2016, I caused to be served through mail (USPS) and e-mail the foregoing document described as:

BRIEF OF AMICI CURIAE

AMERICAN CIVIL LIBERTIES UNION, ACLU OF NORTHERN CALIFORNIA, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF SAN DIEGO AND IMPERIAL COUNTIES, IN SUPPORT OF APPLE, INC.

on each person on the attached Service List.

Executed on March 2, 2016, in Los Angeles, California.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I am employed in the office of a member of the bar of this Court at whose direction the service was made.

Diana Gonzalez

Print Name

Signature

Service List

Service Type	Counsel Served	Party	
Mail & E-mail	I & E-mail Theodore J. Boutrous, Jr. Nicola T. Hanna		
	Eric D. Vandevelde		
	Gibson, Dunn & Crutcher LLP		
	333 South Grand Avenue		
	Los Angeles, CA 90071-3197		
	Telephone: (213) 229-7000		
	Facsimile: (213) 229-7520		
	Email: tboutrous@gibsondunn.com		
	nhanna@gibsondunn.com		
	evandevelde@gibsondunn.com		

Case 5:16-cm-00010-SP Document 57 Filed 03/03/16 Page 29 of 29 Page ID #:795

1	Mail & E-mail	Theodore B. Olson	Apple, Inc.
		Gibson, Dunn & Crutcher LLP	rippie, me.
2		1050 Connecticut Avenue, N.W.	
3		Washington, DC, 20036-5306	
		Telephone: (202) 955-8500	
4		Facsimile: (202) 467-0539	
5		Email: tolson@gibsondunn.com	
	Mail & E-mail	Marc J. Zwillinger	Apple, Inc.
6		Jefffrey G. Landis	appre, me.
7		Zwillgen PLLC	
		1900 M Street N.W., Suite 250	
8		Washington, D.C. 20036	
9		Telephone: (202) 706-5202	
10		Facsimile: (202) 706-5298	
10		Email: marc@zwillgen.com	
11		jeff@zwillgen.com	
12	Mail & E-mail	Eileen M. Decker	United States
12		Patricia A. Donahue	of America
13		Tracy L. Wilkison	
14		Allen W. Chiu	
14		1500 United States Courthouse	
15		7312 North Spring Street	
16		Los Angeles, California 90012	
10		Telephone: (213) 894-0622/2435	
17		Facsimile: (213) 894-8601	
18		Email: Tracy. Wilkison@usdoj.gov	
		Allen.Chiu@usdoj.gov	
19			