

1 Michael M. Maddigan (Bar No. 163450)
2 HOGAN LOVELLS US LLP
3 1999 Avenue of the Stars, Suite 1400
4 Los Angeles, California 90067
5 Telephone: (310) 785-4600
6 Facsimile: (310) 785-4601
7 michael.maddigan@hoganlovells.com



8 Neal Kumar Katyal (*pro hac vice* application
9 forthcoming)
10 HOGAN LOVELLS US LLP
11 555 Thirteenth Street, N.W.
12 Washington, D.C. 20004
13 Telephone: (202) 637-5600
14 Facsimile: (202) 637-5910
15 neal.katyal@hoganlovells.com

16 Attorneys for *Amici Curiae*

17 UNITED STATES DISTRICT COURT
18 CENTRAL DISTRICT OF CALIFORNIA
19 EASTERN DIVISION

20 **BY FAX**

21 IN THE MATTER OF THE SEARCH
22 OF AN APPLE IPHONE SEIZED
23 DURING THE EXECUTION OF A
24 SEARCH WARRANT ON A BLACK
25 LEXUS IS300, CALIFORNIA
26 LICENSE PLATE 35KGD20

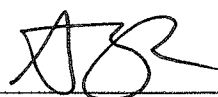
27 ED No. CM 16-10 (SP)
28 ~~PROPOSED~~ ORDER ON
APPLICATION OF
AMAZON.COM, BOX, CISCO
SYSTEMS, DROPBOX,
EVERNOTE, FACEBOOK,
GOOGLE, MICROSOFT,
MOZILLA, NEST, PINTEREST,
SLACK, SNAPCHAT, WHATSAPP,
AND YAHOO TO FILE A BRIEF
AMICUS CURIAE IN SUPPORT OF
APPLE, INC.

Date: March 22, 2016
Time: 1:00 p.m.
Place: Courtroom 3 or 4
Judge: Honorable Sheri Pym

LOGGED

2016 MAR - 3 PM 3:21
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

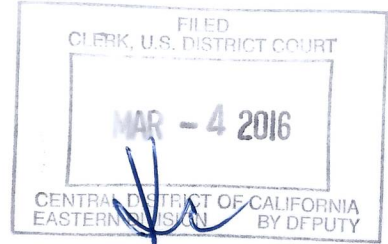
1 The Court has read and considered the application of Amazon.com, Box,
2 Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest,
3 Pinterest, Slack, Snapchat, WhatsApp, and Yahoo to participate in this case as
4 *amici curiae*. The Court finds good cause to grant the application. Accordingly, **IT**
5 **IS HEREBY ORDERED** that Amazon.com, Box, Cisco Systems, Dropbox,
6 Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat,
7 WhatsApp, and Yahoo may participate as *amici curiae*, and that the proposed brief
8 submitted with the application is deemed filed.

9
10 

11 _____
12 Honorable Sheri Pym
13 United States Magistrate Judge

14 Dated: March 4, 2016.
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Michael M. Maddigan (Bar No. 163450)
2 HOGAN LOVELLS US LLP
3 1999 Avenue of the Stars, Suite 1400
4 Los Angeles, California 90067
5 Telephone: (310) 785-4600
6 Facsimile: (310) 785-4601
7 michael.maddigan@hoganlovells.com



8 Neal Kumar Katyal (*pro hac vice* application forthcoming)
9 HOGAN LOVELLS US LLP
10 555 Thirteenth Street, N.W.
11 Washington, D.C. 20004
12 Telephone: (202) 637-5600
13 Facsimile: (202) 637-5910
14 neal.katyal@hoganlovells.com

15 Attorneys for *Amici Curiae*

16 UNITED STATES DISTRICT COURT
17 CENTRAL DISTRICT OF CALIFORNIA
18 EASTERN DIVISION

BY FAX

19 IN THE MATTER OF THE SEARCH
20 OF AN APPLE IPHONE SEIZED
21 DURING THE EXECUTION OF A
22 SEARCH WARRANT ON A BLACK
23 LEXUS IS300, CALIFORNIA
24 LICENSE PLATE 35KGD20

ED No. CM 16-10 (SP)

**BRIEF OF AMICI CURIAE
AMAZON.COM, BOX, CISCO
SYSTEMS, DROPBOX,
EVERNOTE, FACEBOOK,
GOOGLE, MICROSOFT,
MOZILLA, NEST, PINTEREST,
SLACK, SNAPCHAT, WHATSAPP,
AND YAHOO IN SUPPORT OF
APPLE, INC.**

Hearing:

Date: March 22, 2016
Time: 1:00 p.m.
Place: Courtroom 3 or 4
Judge: Hon. Sheri Pym

LOGGED

2016 MAR -3 PM 3:21
CLERK, U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page

TABLE OF AUTHORITIES..... ii

STATEMENT OF INTEREST 1

ARGUMENT..... 5

 I. THE GOVERNMENT’S INTERPRETATION OF THE ALL WRITS ACT IS UNPRECEDENTED AND UNNECESSARY..... 5

 A. The All Writs Act Is A Limited, “Residual” Source Of Federal Court Authority..... 5

 B. The Government Seeks A Dramatic Extension Of *New York Telephone* To Cover Ever-Evolving Technologies..... 6

 C. The Government’s Interpretation Of The All Writs Act Ignores Congress’s Comprehensive Regulation Of Investigative Methods..... 10

 II. THE LAW DOES NOT ALLOW FEDERAL AGENTS TO CONSCRIPT COMPANIES INTO DEFEATING THEIR OWN SECURITY SAFEGUARDS AND PRODUCT DESIGNS..... 15

 A. The Government Seeks Here Far More Than The Nonburdensome Technical Assistance Allowed By The All Writs Act 15

 B. The Government’s Position, If It Prevails, Will Undermine The Security Of Americans’ Most Sensitive Data 18

 III. THE CANON OF CONSTITUTIONAL AVOIDANCE COUNSELS AGAINST THE GOVERNMENT’S EXPANSIVE INTERPRETATION OF THE ALL WRITS ACT..... 21

CONCLUSION..... 24

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

TABLE OF AUTHORITIES

Page

CASES:

Adams v. United States ex rel. McCann,
317 U.S. 269 (1942) 5

Bernstein v. Dep’t of Justice,
176 F.3d 1132 (9th Cir. 1999)..... 22

Brown v. Entertainment Merchants Ass’n,
131 S. Ct. 2729 (2011) 22

Diamond v. Chakrabarty,
447 U.S. 303 (1980) 12

FTC v. Wyndham Worldwide Corp.,
799 F.3d 236 (3d Cir. 2015) 18

Harris v. Nelson,
394 U.S. 286 (1969) 5

*In re Application of U.S. for an Order Authorizing an In-Progress
Trace of Wire Commc’ns Over Tel. Facilities*,
616 F.2d 1122 (9th Cir. 1980)..... 7, 15

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

*In re Application of U.S. for an Order Directing X to Provide Access
to Videotapes*,
No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003) 8, 16

*In re Order Requiring Apple, Inc. to Assist in the Execution of a
Search Warrant Issued by This Court*,
No. 15-MC-1902 (E.D.N.Y. Feb. 29, 2016) *passim*

INS v. St. Cyr,
533 U.S. 289 (2001) 21

1 *Junger v. Daley*,
 2 209 F.3d 481 (6th Cir. 2000) 22

3 *NAACP v. Button*,
 4 371 U.S. 415 (1963) 24

5 *NLRB v. Catholic Bishop of Chicago*,
 6 440 U.S. 490 (1979) 24

7 *Pennsylvania Bureau of Corr. v. United States Marshals Serv.*,
 8 474 U.S. 34 (1985) 5, 6, 10, 12

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

10 *Riley v. California*,
 11 134 S. Ct. 2473 (2014) 8, 9

12 *Riley v. Nat’l Fed’n of the Blind of N.C., Inc.*,
 13 487 U.S. 781 (1988) 23

14 *Sorrell v. IMS Health Inc.*,
 15 131 S. Ct. 2653 (2011) 22

16 *United States v. Hall*,
 17 583 F. Supp. 717 (E.D. Va. 1984) 8, 16

18 *United States v. Jones*,
 19 132 S. Ct. 945 (2012) 9

20 *United States v. New York Tel. Co.*,
 434 U.S. 159 (1977) *passim*

21 *United States v. X*,
 22 601 F. Supp. 1039 (D. Md. 1984) 8

23 *Universal City Studios, Inc. v. Corley*,
 24 273 F.3d 429 (2d Cir. 2001) 22

25 **STATUTES:**

26 18 U.S.C. §§ 2511-2522 10

27 18 U.S.C. §§ 2701-2712 4

28

1 18 U.S.C. § 2703..... 11

2 28 U.S.C. § 1651..... *passim*

3 47 U.S.C. §§ 1001-1010 11

4 47 U.S.C. § 1002(b)(2) 11

5 47 U.S.C. § 1002(b)(3) 11

6 50 U.S.C. § 1805..... 10

7 50 U.S.C. § 1874..... 14

8 USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015)..... 10

9 **CONSTITUTIONAL PROVISIONS:**

10

11 U.S. Const. amend. I..... 21, 22, 23, 24

12 U.S. Const. amend. IV 8, 9

13 **OTHER AUTHORITIES:**

14

15 Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by*

16 *Requiring Government Access to All Data And Communications*

17 *(Jul. 6, 2015)*..... 20

18 Devlin Barrett et al., *Apple and Others Encrypt Phones, Fueling*

19 *Government Standoff*, *The Wall St. J.*, Nov. 18, 2014 18

20 Katie Benner & Matt Apuzzo, *Narrow Focus May Aid F.B.I. in Apple*

21 *Case*, *N.Y. Times*, Feb. 22, 2016 13

22 Cory Bennett & Katie Bo Williams, *Week Ahead: Encryption Fight*

23 *Heats Up*, *The Hill*, Feb. 22, 2016 12

24 Box, *Privacy Policy*, <http://goo.gl/QR1u1> 14

25 James B. Comey, Dir., FBI, *Joint Statement with Deputy Attorney*

26 *General Sally Quillian Yates Before the Senate Judiciary*

27 *Committee* (July 8, 2015) 19

28 The Chertoff Group, *The Ground Truth About Encryption and the*

Consequences of Extraordinary Access, <http://goo.gl/Z9xPpj>..... 20

1 Dropbox, *2015 Transparency Report*, <https://goo.gl/HhEUQm> 5

2 Dropbox, *Privacy Policy*, <http://goo.gl/QR1u1> 14

3 Evernote, *Privacy Policy*, <https://goo.gl/yKbzbq> 14

4 Evernote, *Transparency Report for 2015*, <https://goo.gl/MIpwJW> 4

5 Facebook, *Data Policy*, <http://goo.gl/VxoRFQ> 14

6 Facebook, *Information for Law Enforcement*, <https://goo.gl/SdfH4r> 4

7 Facebook, *United States Law Enforcement Requests for Data*,
 8 <https://goo.gl/YwTyOQ> 4

9 Google, *Privacy & Terms*, <https://goo.gl/NICNc> 13

10 Google, *Transparency Report*, <https://goo.gl/RkS5f8> 4

11 Julia Harte & Julia Edwards, *Apple Lawyer, FBI Director Face Off in*
 12 *Congress on iPhone Encryption*, REUTERS, Mar. 2, 2016 13

13 Amy Hess, Exec. Assistant Dir., Science & Technology Branch, FBI,
 14 *Statement Before the House Oversight and Government Reform*
 15 *Committee, Subcommittee on Information Technology* (Apr. 29,
 16 2015) 19

17 Erin Kelly, *Bill Would Stop Feds from Mandating ‘Backdoor’ to Data*,
 18 USA Today, Apr. 2, 2015 20

19 Mike Masnick, Techdirt, *FBI Claims It Has No Record of Why It*
 20 *Deleted Its Recommendation to Encrypt Phones* (Feb. 29, 2016) 19

21 Microsoft, *Law Enforcement Requests Report*, <https://goo.gl/3KHQUB> 4

22 Microsoft, *Privacy Statement*, <http://goo.gl/mGf4qs> 14

23 Mozilla, *Privacy Policy*, <http://goo.gl/LX4rRi> 14

24 Ellen Nakashima, *Google, Facebook and Other Powerful Tech Firms*
 25 *Filing Briefs to Support Apple*, Wash. Post, Feb. 28, 2016 20

26 Office of the Nat’l Counterintelligence Exec., *Foreign Spies Stealing*
 27 *US Economic Secrets in Cyberspace* (Oct. 2011) 18

28

1 Nicole Perloth & David E. Sanger, *Obama Won't Seek Access to*
 2 *Encrypted User Data*, N.Y. Times, Oct. 10, 2015 11

3 Pinterest, *Quarterly Transparency Report Archive*,
 4 <https://goo.gl/S89TmN> 4

5 President's Review Group on Intelligence & Communications
 6 Technologies, *Liberty and Security in a Changing World*
 (Dec. 12, 2013) 20

7 David Rowan, *WhatsApp: The Inside Story*, Wired UK, Feb. 19, 2014 17

8 Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*,
 9 N.Y. Times, Sept. 27, 2010 11

10 Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*,
 11 N.Y. Times, May 7, 2013 11

12 Snapchat, *Law Enforcement Guide*, <https://goo.gl/H2jSGQ> 4

13 Snapchat, *Privacy Policy*, <http://goo.gl/EvfTe2> 13

14 Snapchat, *Transparency Report*, <https://goo.gl/pZbxnC> 4

15 Snapchat, *When are Snaps and Chats Deleted?*, <https://goo.gl/adHPnO> 17

16 Dustin Volz et al., *Key U.S. Lawmaker Suggests Openness to*
 17 *Encryption Legislation after Apple Order*, Reuters, Feb. 18, 2016 12

18 Dustin Volz, *U.S. Lawmakers Seek to Bar States from Mandating*
 19 *Encryption Weaknesses*, Reuters, Feb. 10, 2016 12

20 The White House, *Administration Strategy on Mitigating the Theft of*
 21 *U.S. Trade Secrets* (Feb. 2013) 18

22 The White House, Office of the Press Sec'y, *Fact Sheet: Cybersecurity*
 23 *National Action Plan* (Feb. 9, 2016) 19

24 WhatsApp, *Privacy Notice*, <http://goo.gl/0GQ7LI> 14

25 Yahoo, *Government Data Requests*, <https://goo.gl/dnwcFv> 4

26 Yahoo, *Privacy Center*, <http://goo.gl/Ng6xjn> 14

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

STATEMENT OF INTEREST

Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo respectfully submit this brief as *amici curiae* in support of Apple, Inc.

Amazon.com is one of the world’s largest and best known online retailers and cloud service providers. Amazon seeks to be the Earth’s most customer-centric company, where customers can discover anything they might want to buy online at the lowest possible prices. Amazon’s cloud computing business, Amazon Web Services, is trusted by more than a million active customers around the world—including the fastest growing startups, largest enterprises, and leading government agencies—to power their IT infrastructure, make them more agile, and lower costs.

Box is a cloud-based enterprise content management platform that makes it easier for people to securely collaborate and get work done faster. Today, more than 41 million users and 54,000 businesses—including 55% of the Fortune 500—trust Box to manage content in the cloud.

Cisco Systems is the worldwide leader in providing infrastructure for the internet. It also offers various services, managed from data centers operated by Cisco, which allow its customers to use, among other things, remote data centers, wireless internet services, internet security services and collaboration tools, which drive efficiency in their business.

Dropbox provides file storage, synchronization, and collaboration services. With over 400 million users and 150,000 businesses on Dropbox Business, people around the world use Dropbox to work the way they want, on any device, wherever they go. Dropbox’s products are built on trust; when people put their files in Dropbox, they can trust they’re secure and their data is their own.

Evernote provides a platform that allows individuals and teams to bring their life’s work together in one digital workspace. More than 150 million people and

1 over 20,000 businesses trust Evernote to help them collect their best ideas, write
2 meaningful words, and move important projects forward.

3 **Facebook** is one of the world's leading providers of online networking
4 services. Facebook provides a free Internet-based social media service that enables
5 more than 1.5 billion people to connect with their friends and family, to discover
6 what is going on in the world around them, and to share and publish the opinions,
7 ideas, photos, and activities that matter to them and the people they care about.

8 **Google** is a diversified technology company whose mission is to organize the
9 world's information and make it universally accessible and useful. Google offers a
10 variety of web-based products and services—including Search, Gmail, Maps,
11 YouTube, and Blogger—that are used by people throughout the United States and
12 around the world.

13 **Microsoft** is a leader in the technology industry. Since its founding in 1975,
14 it has developed a wide range of software, services, and hardware products,
15 including the flagship Windows operating system, the Office suite of productivity
16 applications, the Surface tablet computer, and the Xbox gaming system.

17 **Mozilla** is a global, mission-driven organization that works with a worldwide
18 community to create open source products like its web browser Firefox. Its mission
19 is guided by the Mozilla Manifesto, a set of principles that recognizes, among other
20 things, that individuals' security and privacy on the Internet are fundamental and
21 must not be treated as optional. In furtherance of that, Mozilla has also adopted
22 data-privacy principles that emphasize transparency, user control, limited data
23 collection, and multi-layered security control and practices.

24 **Nest** builds hardware, software, and services for the connected home. The
25 Nest Learning Thermostat, Nest Protect smoke and carbon monoxide alarm, and
26 Nest Cam security camera can all be controlled from customers' phones. Nest
27 algorithms use data about a customer's preferences to adapt and optimize device
28 behavior.

1 **Pinterest** is an online catalog of ideas. Every month, over 100 million
2 people around the world use Pinterest to find and save ideas for cooking, parenting,
3 style, and more.

4 **Slack** is a messaging platform for teams. It brings together all team
5 communications and organizes them into one place; uses real-time messaging to
6 improve productivity and reduce internal e-mail; and eliminates inefficiencies by
7 providing easy-to-use archiving and search.

8 **Snapchat** is a camera application that empowers users to tell their stories and
9 talk with their friends.

10 **WhatsApp**, a subsidiary of Facebook, is a fast, simple, and reliable mobile
11 messaging application available on a variety of mobile platforms. Over a billion
12 users rely on WhatsApp to easily and securely exchange messages, calls, photos,
13 and videos with friends, family, and others.

14 **Yahoo** is a guide focused on informing, connecting, and entertaining its more
15 than one billion users around the world. Yahoo's wholly-owned subsidiary,
16 Tumblr, Inc.—with an audience of over 500 million people per month—provides a
17 platform for users to connect, to explore new ideas and creative expressions, and
18 form communities. Yahoo's commitment to security compels it to both
19 thoughtfully respond to requests from law enforcement and build products that
20 make a more secure user experience and overall digital ecosystem, including
21 ongoing work on an intuitive end-to-end encryption solution for Yahoo Mail users.

22 *Amici* often compete vigorously with Apple—and with each other. But *amici*
23 here speak with one voice because of the singular importance of this case to them
24 and their customers who trust *amici* to safeguard their data and most sensitive
25 communications from attackers. *Amici* share the government's and the public's
26 grief and outrage at the heinous act of terrorism that took place in San Bernardino,
27 California, in December 2015, and they fully support the lawful investigation of
28 that crime. But *amici* are also united in their view that the government's order to

1 Apple exceeds the bounds of existing law and, when applied more broadly, will
2 harm Americans' security in the long run.

3 To be clear: *Amici* feel no sympathy for terrorists. Technology companies
4 like *amici* have obligations under the Stored Communications Act, 18 U.S.C.
5 §§ 2701-2712, and other laws to produce customer data to law enforcement with
6 proper legal process, and *amici* take their obligations seriously. Many *amici* have
7 full-time teams of employees—with someone on duty or on call around-the-clock—
8 dedicated to responding to law enforcement requests for customer data. Indeed, in
9 just the first six months of 2015, *amici* collectively responded to tens of thousands
10 of U.S. government data requests in criminal cases.¹ Many *amici* also publish law-
11 enforcement guidelines that explain their products, what customer data can be
12 requested through legal process, and how to best serve process on the company.²
13 *Amici*, in short, have no interest in shielding those who break the law. But *amici*
14 reject the government's unsupported assertion that the law allows it to commandeer
15 a company's own engineers to undermine their products' data security features.

16 The Court should vacate its order compelling Apple to engineer security
17 flaws into its own software and deny the government's motion to compel.

18
19
20
21
22
23 ¹ See Dropbox, *2015 Transparency Report*, <https://goo.gl/HhEUQm>; Evernote,
24 *Transparency Report for 2015*, <https://goo.gl/MlpwJW>; Facebook, *United States*
25 *Law Enforcement Requests for Data*, <https://goo.gl/YwTyOQ>; Google,
26 *Transparency Report*, <https://goo.gl/RkS5f8>; Microsoft, *Law Enforcement Requests*
27 *Report*, <https://goo.gl/3KHQUB>; Pinterest, *Quarterly Transparency Report*
28 *Archive*, <https://goo.gl/S89TmN>; Snapchat, *Transparency Report*,
<https://goo.gl/pZbxnC>; Yahoo, *Government Data Requests*, <https://goo.gl/dnwcFv>.

² See, e.g., Facebook, *Information for Law Enforcement Authorities*,
<https://goo.gl/SdfH4r>; Snapchat, *Law Enforcement Guide*, <https://goo.gl/H2jSGQ>.

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

ARGUMENT

I. THE GOVERNMENT’S INTERPRETATION OF THE ALL WRITS ACT IS UNPRECEDENTED AND UNNECESSARY.

A. The All Writs Act Is A Limited, “Residual” Source Of Federal Court Authority.

The All Writs Act, 28 U.S.C. § 1651, was originally enacted as part of the Judiciary Act of 1789, ch. 20, 1 Stat. 73. That was fifty years before the telegraph was invented and almost a century before Alexander Graham Bell made the first telephone call. Amended just twice, in non-substantive ways, the All Writs Act currently provides: “The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a).

As its terms indicate, the All Writs Act was not designed to confer sweeping new powers. Rather, it gave federal courts a “residual source of authority to issue writs that are not otherwise covered by statute.” *Pennsylvania Bureau of Corr. v. United States Marshals Serv.*, 474 U.S. 34, 43 (1985). The first Congress recognized that “historic aids” might be necessary for federal courts to exercise and protect their newfound jurisdiction. *Adams v. United States ex rel. McCann*, 317 U.S. 269, 273 (1942). The Act supplies those aids, but they are not unfettered; they must be employed according to established “usages and principles of law.” See *Harris v. Nelson*, 394 U.S. 286, 300 (1969) (explaining that “the purpose and function of the All Writs Act [is] to supply the courts with the instruments needed to perform their duty, . . . provided only that such instruments are ‘agreeable’ to the usages and principles of law”).

Now, 200 years later, the government endeavors to reinterpret the All Writs Act as an open-ended source of new powers. It asks this Court to endorse an unprecedented expansion of the Act that would allow law enforcement to force private technology companies to circumvent security features that protect their

1 customers' most sensitive information from hackers and criminals. Such
2 conscription looks nothing like the "historic aids" that the 1789 Judiciary Act
3 contemplated. Moreover, where the new authority the government seeks would not
4 "fill[] the interstices of federal judicial power," *Pennsylvania Bureau of Corr.*, 474
5 U.S. at 41, but would confer on the judiciary a power that the legislature has
6 withheld, it contradicts "the usages and principles of law." For that very reason,
7 another court recently rejected an even less sweeping request under the All Writs
8 Act. *See* Mem. & Order, *In re Order Requiring Apple, Inc. to Assist in the*
9 *Execution of a Search Warrant Issued by This Court*, No. 15-MC-1902 (slip op.)
10 (E.D.N.Y. Feb. 29, 2016). The court held that the "usages and principles" clause
11 prohibits the government from using the All Writs Act "to achieve a legislative goal
12 that Congress has considered and rejected." *Id.* at 26; *see infra* Part I.C. As a
13 textual matter, then, the circumscribed authority provided in the All Writs Act
14 cannot—and does not—support the government's broad reinterpretation.

15
16 **B. The Government Seeks A Dramatic Extension Of New York
Telephone To Cover Ever-Evolving Technologies.**

17 Nor has the government justified its boundless reading of the statute under
18 Supreme Court precedent. In keeping with its "residual" status, the All Writs Act
19 has not been extensively analyzed by courts. In this case, both Apple and the
20 government draw heavily from the Supreme Court's 1977 decision in *United States*
21 *v. New York Telephone Co.*, 434 U.S. 159. They have extracted three (or so) factors
22 from *New York Telephone* to guide their analysis. *See* Dkt. No. 1, at 10 (Feb. 19,
23 2016) (Mot. to Compel); Dkt. No. 16, at 20 (Feb. 25, 2016) (Mot. to Vacate). But
24 the emphasis on a rigid multifactor test obscures the bigger point. Those factors
25 were not ends unto themselves; they were markers to gauge whether the
26 government had pushed a "residual" power too far.

27 In the decision on appeal in *New York Telephone*, the court of appeals was
28 concerned that an order to the telephone company would "pose a severe threat to

1 the autonomy of third parties who for whatever reason prefer not to render such
2 assistance.” 434 U.S. at 171. The Supreme Court concluded that the lower court
3 had no reason to worry, because “the power of federal courts to impose duties upon
4 third parties is not without limits.” *Id.* at 172. In particular, orders requested under
5 the All Writs Act cannot impose an “unreasonable burden[.]” *Id.* The key question
6 in *New York Telephone* was whether a specific order was “appropriate” and not
7 “unreasonable.” *Id.* at 172, 174. And that question could not be divorced from the
8 context in which it arose: *New York Telephone* involved the installation of a pen
9 register, “a mechanical device that records the numbers dialed on a telephone.” *Id.*
10 at 161 n.1. The Supreme Court thought it “clear that Congress did not view pen
11 registers as posing a threat to privacy of the same dimension as the interception of
12 oral communications,” which was governed by statutory procedures. *Id.* at 168. It
13 was equally clear to the Supreme Court that “the use of pen registers [wa]s by no
14 means offensive” to the public utility subject to the order. *Id.* at 174.

15 It is dangerous to extend that limited endorsement of judicial power over
16 third parties to situations the Supreme Court never could have envisioned—and all
17 the more troubling where the Court itself declined to opine on “the diverse contexts
18 in which [third party duties] may arise.” *Id.* at 176 n.24. As the Ninth Circuit has
19 explained, *New York Telephone*’s only “gloss” on the All Writs Act was its
20 conclusion that a third party could be ordered “to provide nonburdensome technical
21 assistance to law enforcement officers.” *Plum Creek Lumber Co. v. Hutton*, 608
22 F.2d 1283, 1289 (9th Cir. 1979). But the Supreme Court stopped there. It did not
23 give courts “plenary power” or “a roving commission” to order third parties to
24 assist law enforcement wherever law enforcement deems it expedient. *Id.* Other
25 applications of the Act have thus hewed carefully to the “nonburdensome technical
26 assistance” required in *New York Telephone*. See, e.g., *In re Application of United*
27 *States for an Order Authorizing an In-Progress Trace of Wire Commc’ns Over Tel.*
28 *Facilities*, 616 F.2d 1122, 1129, 1132 (9th Cir. 1980) (*Wire Commc’ns*) (ordering

1 telephone company to install devices “virtually identical” to a pen register, which
 2 required no “active monitoring by company personnel”); *United States v. X*, 601 F.
 3 Supp. 1039, 1043 (D. Md. 1984) (ordering telephone company to provide existing
 4 toll records for two subscribers); *United States v. Hall*, 583 F. Supp. 717, 722 (E.D.
 5 Va. 1984) (ordering bank to produce existing credit card records for a particular
 6 account); *In re Application of United States for an Order Directing X to Provide*
 7 *Access to Videotapes*, No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22,
 8 2003) (*Videotapes*) (ordering apartment complex “to provide access to surveillance
 9 tapes already in existence”).

10 The request here is far different. This Court should therefore exercise
 11 caution in how it applies a decision from an era in which concepts like “cell
 12 phones” and “the Internet” were unheard of. Extending *New York Telephone’s*
 13 holding as the government requests here would unmoor it from its motivating
 14 rationale. And the Supreme Court has cautioned lower courts against woodenly
 15 applying prior decisions without assessing intervening technological change, in the
 16 comparable context of the Fourth Amendment.³

17 In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court explained
 18 that cell phones had altered the reasonableness of a full search incident to arrest.
 19 The Court observed that modern cell phones “are based on technology nearly
 20 inconceivable just a few decades ago,” when the only relevant search-incident-to-
 21 arrest precedents had been decided. *Id.* at 2484. In part because of the quantitative
 22 and qualitative differences in available information, it concluded that the reasoning
 23 in those precedents did not have “much force with respect to digital content on cell
 24 phones.” *Id.* Americans live their lives on their phones now. They store their

25
 26 ³ Although this case does not formally involve the Fourth Amendment
 27 (because the government has a warrant), the principles that inform the Fourth
 28 Amendment analysis are instructive here. Both doctrines, after all, assess the
 reasonableness of government intrusions onto private property, and Congress
 passed the Fourth Amendment and the 1789 Judiciary Act just four days apart.

1 emails, their conversations, their appointments, their photos, sometimes even their
2 medical information, all in a device they carry in their pockets. Cell phones are the
3 way we organize and remember the things that are important to us; they are, in a
4 very real way, an extension of our memories. And as a result, to access someone's
5 cell phone is to access their innermost thoughts and their most private affairs.
6 Those concerns are why the Supreme Court in *Riley* found the difference between
7 searches of cell phones and other searches incident to arrest so stark that "any
8 extension of [the Court's prior] reasoning to digital data has to rest on its own
9 bottom." *Id.* at 2489.

10 A majority of the Supreme Court in *United States v. Jones*, 132 S. Ct. 945
11 (2012), made a similar point. Writing for four Justices, Justice Alito remarked that
12 "technology can change" an individual's expectations of privacy and thus alter the
13 calculus that courts must perform. *Id.* at 962 (Alito, J., concurring in the judgment).
14 And Justice Sotomayor, writing for herself, emphasized that technology can disrupt
15 the calculus so much that "it may be necessary to reconsider" basic Fourth
16 Amendment premises. *Id.* at 957 (Sotomayor, J., concurring). Again, the critical
17 lesson was that, when transplanting dated precedents into modern technological
18 scenarios, courts should never lose sight of the overarching reasonableness inquiry
19 that underlies all government access to private information.

20 The same concerns apply here. Whatever principles this Court extracts from
21 the 1977 *New York Telephone* decision about the 1789 All Writs Act, one thing is
22 clear: Applying the All Writs Act here would extend the Act in unprecedented
23 ways, not routinely apply it. The stakes are much higher now—the security
24 interests greater, the government's request broader, the companies' objections
25 sharper, the technological and social problems thornier—than when the Supreme
26 Court assessed the installation of a pen register. As the Supreme Court has
27 cautioned, any extension of the All Writs Act to such complex modern scenarios
28 must "rest on its own bottom." *Riley*, 134 S. Ct. at 2489. The government's

1 proposed extension, which would move beyond companies' existing products to
 2 subvert security features millions of Americans rely on to keep their digital
 3 information secure, *see infra* Part II, fails that test. A 200-year-old source of
 4 residual power that must be exercised consistently with "the usages and principles
 5 of law," 28 U.S.C. § 1651(a), cannot be transformed into a perpetual invitation to
 6 reshape private parties' behavior in policy-laden ways.

7
 8 **C. The Government's Interpretation Of The All Writs Act Ignores
 Congress's Comprehensive Regulation Of Investigative Methods.**

9 It is well established that the All Writs Act is unavailable "[w]here a statute
 10 specifically addresses the particular issue at hand." *Pennsylvania Bureau of Corr.*,
 11 474 U.S. at 43; *see* Mot. to Vacate 15-19. That doctrinal preference for legislative
 12 action is also good policy: In light of rapidly evolving technology and its
 13 tremendous social benefits, Congress is better suited to confront the issues here.
 14 And indeed, Congress has already grappled with these issues on many occasions—
 15 leading to a comprehensive legislative scheme for regulating investigative methods.
 16 "The absence from that comprehensive scheme of any requirement that Apple
 17 provide the assistance sought here implies a legislative decision to prohibit the
 18 imposition of such a duty." *In re Order*, No. 15-MC-1902, at 20.

19 In 1968, when Congress turned its attention to surveillance techniques, it
 20 initially focused on law enforcement methods. It enacted the Wiretap Act, which
 21 lays out specific procedures by which law enforcement can request, and courts can
 22 supervise, the interception of communications (originally wire and oral, and later
 23 electronic as well). *See* 18 U.S.C. §§ 2511-2522. In the Foreign Intelligence
 24 Surveillance Act of 1978 (FISA), Congress then prescribed specific procedures for
 25 the surveillance of foreign intelligence information, and required that certain
 26 persons furnish technical assistance to law enforcement. *See* 50 U.S.C. § 1805. It
 27 continues to update and amend FISA, including just last year in the USA Freedom
 28 Act of 2015. *See* Pub. L. No. 114-23, 129 Stat. 268. In 1986, in the Stored

1 Communications Act, Congress also outlined the conditions under which law
2 enforcement can compel an internet service provider to disclose certain subscriber
3 content. *See* 18 U.S.C. § 2703.

4 Particularly relevant here, Congress next decided to regulate
5 telecommunications carriers and manufacturers of telecommunications equipment.
6 In 1994, it enacted the Communications Assistance for Law Enforcement Act,
7 commonly known as CALEA, to enhance law enforcement's ability to conduct
8 surveillance. CALEA requires telecommunications carriers and manufacturers to
9 design their services and equipment in a manner that ensures law enforcement can
10 execute court-ordered wiretaps. *See* 47 U.S.C. §§ 1001-1010. It specifically
11 exempts information service providers from that command. *Id.* § 1002(b)(2).
12 Moreover, it specifies that in most instances telecommunications carriers "shall not
13 be responsible for decrypting, or ensuring the government's ability to decrypt,"
14 communications. *Id.* § 1002(b)(3).

15 Since CALEA was enacted, there have been a number of proposals to extend
16 it to electronic communication service providers like Apple. Yet Congress has
17 never seen fit to give law enforcement the power it now seeks from this Court. In
18 2010, for example, the Obama administration prepared a legislative proposal to
19 extend CALEA to all services that enable communications, but never submitted the
20 proposal to Congress. *See* Charlie Savage, *U.S. Tries to Make It Easier to Wiretap*
21 *the Internet*, N.Y. Times, Sept. 27, 2010. In 2013, it advocated a modified plan that
22 would have imposed fines rather than mandates; that proposal was never formally
23 submitted, either. *See* Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap*
24 *Laws*, N.Y. Times, May 7, 2013. In fact, the Obama administration has since
25 dropped the call for new legislation altogether. *See* Nicole Perlroth & David E.
26 Sanger, *Obama Won't Seek Access to Encrypted User Data*, N.Y. Times, Oct. 10,
27 2015.

28

1 Even absent formal proposals from the Executive Branch, Congress has
2 given these issues considerable attention. Legislation aimed at expanding law
3 enforcement's investigative capabilities has been discussed in reaction to this very
4 case. See Dustin Volz et al., *Key U.S. Lawmaker Suggests Openness to Encryption*
5 *Legislation After Apple Order*, Reuters, Feb. 19, 2016; Cory Bennett & Katie Bo
6 Williams, *Week Ahead: Encryption Fight Heats Up*, The Hill, Feb. 22, 2016. And
7 legislation has been proposed to block state governments from requiring companies
8 to create encryption backdoors. See Dustin Volz, *U.S. Lawmakers Seek to Bar*
9 *States from Mandating Encryption Weaknesses*, Reuters, Feb. 10, 2016. That
10 debate illustrates exactly how the democratic process should work.

11 The government ignores that process here and instead seeks powers from the
12 judiciary that the legislature has repeatedly withheld. That is not the function of the
13 courts, or of the gap-filling All Writs Act. See *Pennsylvania Bureau of Corr.*, 474
14 U.S. at 41. The government's reading of the Act would "thoroughly undermine[]
15 both the legislature's own prerogative to reject a legislative proposal effectively and
16 efficiently (without the need to affirmatively ban the proposed authority) and the
17 more general protection against tyranny that the Founders believed required the
18 careful separation of governmental powers." *In re Order*, No. 15-MC-1902, at 27.
19 Those separation-of-powers concerns are especially acute where, as here, the issues
20 at hand are "a matter of high policy for resolution within the legislative process
21 after the kind of investigation, examination, and study that legislative bodies can
22 provide." *Diamond v. Chakrabarty*, 447 U.S. 303, 317 (1980). "That process
23 involves the balancing of competing values and interests, which in our democratic
24 system is the business of elected representatives." *Id.* It should not be truncated by
25 ad hoc judicial decisions.

26 Make no mistake: If the government prevails in this case, it will seek many
27 such decisions. The government's motion reassures this Court and the public that
28 the request here is a one-time-only hack. See Mot. to Compel 14-15. But there are

1 already strong indications that law enforcement will ask for broad authority under
 2 the All Writs Act on facts far different from the terrorism investigation at hand. For
 3 example, FBI Director James Comey just days ago told the House Judiciary
 4 Committee that this Court’s decision will be “potentially precedential” in other
 5 cases involving similar technology. *See* Julia Harte & Julia Edwards, *Apple*
 6 *Lawyer, FBI Director Face Off in Congress on iPhone Encryption*, Reuters, Mar. 2,
 7 2016. Manhattan District Attorney Cyrus Vance, Jr., likewise told journalists that
 8 he “[a]bsolutely” would seek access to all locked phones linked to criminal
 9 proceedings if the government’s theory were to prevail here. *See* Katie Benner &
 10 Matt Apuzzo, *Narrow Focus May Aid F.B.I. in Apple Case*, N.Y. Times, Feb. 22,
 11 2016. That is exactly why this Court should reject any case-specific arguments the
 12 government makes here. Investigative tools meant for extraordinary cases may
 13 become standard in ordinary ones. *See New York Tel.*, 434 U.S. at 179 (Stevens, J.,
 14 dissenting in part) (warning that the “accretion [of arbitrary police powers] is no
 15 less dangerous and unprecedented because the first step appears to be only
 16 minimally intrusive”). As one court has already observed, “[n]othing in the
 17 government’s arguments suggests any principled limit on how far a court may go.”
 18 *In re Order*, No. 15-MC-1902, at 44.

19 For technology companies like *amici*, the difference between judicial action
 20 and legislative action is not merely philosophical and constitutional. It is critical
 21 from a practical standpoint that regulatory changes come, if at all, through the
 22 legislative process—and not through decisions from individual judges across the
 23 country applying the All Writs Act. *Amici* pride themselves on transparency with
 24 the public, particularly with respect to sensitive issues such as disclosing users’
 25 data. They publish privacy reports or privacy policies online, and take revisions to
 26 those policies very seriously.⁴ And many of them publicly report information about

27
 28 ⁴ *See* Google, *Privacy & Terms*, <https://goo.gl/NICNc>; Snapchat, *Privacy Policy*, <http://goo.gl/EvfTe2>; Facebook, *Data Policy*, <http://goo.gl/VxoRFQ>;

1 the government requests they receive, to the extent permitted by law. *See* 50 U.S.C.
 2 § 1874 (regulating public reporting by persons subject to FISA orders). Some of
 3 *amici* even fought in court to secure that right.

4 A boundless All Writs Act could cripple these efforts. Under the ad hoc
 5 approach the government advocates, the assistance it can request is limited only by
 6 its imagination and the case-by-case reasonableness calls made by magistrate
 7 judges across the country. By contrast, when operating within the framework of
 8 existing statutes, *amici* can apply the law openly and evenhandedly. Under current
 9 law, companies can describe the types of process they receive—warrants,
 10 subpoenas, national security letters, and so on—and explain how they respond.
 11 And *amici*'s experiences with law enforcement under existing statutes confirm the
 12 wisdom of a statutorily circumscribed approach. Not only can they better account
 13 for users' privacy and security interests (and better communicate with users about
 14 those interests), but they can also better assist law enforcement through efficient,
 15 consistent, established procedures. After all, technology companies like *amici*
 16 respond to tens of thousands of law enforcement requests in criminal cases each
 17 year. Indeed, even this case was cooperative at the outset. *See* Dkt. No. 16-32, at
 18 2-3 (Feb. 25, 2016) (Decl. of Lisa Olle) (reciting Apple's immediate compliance
 19 with several FBI requests).

20 All the virtues of statutory predictability fall away if the government can
 21 invoke the All Writs Act as expansively as it seeks to do here. The American
 22 people as *voters* are cut out of this important debate, because their elected
 23 representatives have no opportunity to weigh complex policy choices. And the
 24 American people as *consumers* are cut out of the debate, because they cannot select

25
 26 Microsoft, *Privacy Statement*, <http://goo.gl/mGf4qs>; Yahoo, *Privacy Center*,
 27 <http://goo.gl/Ng6xjn>; Box, *Privacy Policy*, <http://goo.gl/G5JXDT>; Mozilla, *Privacy*
 28 *Policy*, <http://goo.gl/LX4rRi>; Dropbox, *Privacy Policy*, <http://goo.gl/QQR1u1>;
 WhatsApp, *Privacy Notice*, <http://goo.gl/0GQ7LI>; Evernote, *Privacy Policy*,
<https://goo.gl/yKbzbq>.

1 products based on company policies or security features if the government may
 2 override those policies and features without notice. These repercussions underscore
 3 why the Court should decline to extend *New York Telephone* from the installation
 4 of pen registers in the 1970s to the creation of security-defeating technology in
 5 2016.

6
 7 **II. THE LAW DOES NOT ALLOW FEDERAL AGENTS TO**
 8 **CONSCRIPT COMPANIES INTO DEFEATING THEIR OWN**
 9 **SECURITY SAFEGUARDS AND PRODUCT DESIGNS.**

10 **A. The Government Seeks Here Far More Than The Nonburdensome**
 11 **Technical Assistance Allowed By The All Writs Act.**

12 The government argues that the All Writs Act grants the Court the power to
 13 compel any technical assistance from a company that does not require “inordinate
 14 effort.” *Mot. to Compel* 13. But most of the government’s cited cases actually
 15 stand for a much narrower proposition: that a court can require companies to assist
 16 the government with nonburdensome technical assistance—that is, with tools
 17 companies already have available. That is an altogether different power from the
 18 one the government seeks here, a power to commandeer private engineers working
 19 for private companies to write computer code that would disable the security
 20 protections their employers have designed into their products.

21 In *New York Telephone*, for instance, the phone company already used pen
 22 registers for billing purposes and to trace harassing telephone calls to customers.
 23 434 U.S. at 174-175. The telephone company in *Wire Communications* similarly
 24 admitted that it used trap-and-trace devices like the one the government had
 25 requested “in response to obscene or annoying calls, or following telephone
 26 threats.” 616 F.2d at 1126. And in *In re Application of U.S. for an Order Directing*
 27 *a Provider of Communication Services to Provide Technical Assistance to Agents*
 28 *of the U.S. Drug Enforcement Administration*, No. 15-1242, 2015 WL 5233551, at
 *2, *5 (D.P.R. Aug. 27, 2015), the court merely required the phone company to use
 the tools it employed for court-ordered wiretaps to assist with consensual

1 monitoring of a particular phone. In each of the phone cases, the companies could
2 comply with the court's order by employing pre-existing procedures.

3 That pattern repeats itself outside of the telephone cases. In *United States v.*
4 *Hall*, the credit card company "routinely" compiled the billing records the
5 government had requested. 583 F. Supp. at 721. And the federal agents in
6 *Videotapes*, would review the tapes the court compelled "by using apartment
7 complex equipment that is currently in operation and routinely used by complex
8 employees." 2003 WL 22053105, at *1.⁵ In each case, law enforcement worked
9 within companies' existing capabilities.

10 The assistance that the government seeks here is thus different not just in
11 degree, but also in kind. The government is not asking companies to do what they
12 do in the normal course of business; the government is asking companies to change
13 how they do business. To honor an order like the Court issued here, companies
14 must divert engineering talent to fundamentally alter their products. *See Mot. to*
15 *Compel* 13. Their engineers will have to design, create, test, validate, and deploy
16 entirely new software to undermine security features they previously designed,
17 created, tested, validated, and deployed. *See Mot. to Vacate* 13. The government
18 seeks the power to conscript technology companies' engineers to develop products
19 that they do not want to create, and which they would not create absent government
20 compulsion. That is a far cry from the "nonburdensome technical assistance" that
21 the All Writs Act authorizes. *Plum Creek*, 608 F.2d at 1289.

22 Against this, the government emphasizes that it is technically feasible for
23 companies like Apple to comply with its requests. It references, for example,
24 Apple's capability or ability to comply with the government's demands no fewer
25 than six times in its motion to compel. *See Mot. to Compel* 1, 3 n.2, 6, 10, 11, 14.

26
27 ⁵ The apartment complex in *Videotapes* also "di[d] not contest the
28 government's application," further reducing the case's precedential value.
Videotapes, 2003 WL 22053105, at *1.

1 But technical feasibility cannot, and should not, be the standard for reasonableness
2 under the All Writs Act. *Amici*, like Apple, employ top engineering talent. With
3 enough time and resources, *amici*'s engineers could possibly come up with any
4 number of new versions of their companies' products that circumvent or undermine
5 their pre-existing data-security features. But those new versions would not be the
6 same product anymore. Box would not be Box; Gmail would not be Gmail;
7 WhatsApp would not be WhatsApp; and so on.

8 That is the key point. How apps and programs store data is not just—as the
9 government claims—a “public brand marketing strategy.” Mot. to Compel 3. It is
10 at the core of the products' identities. Some companies pride themselves on
11 promptly deleting users' data when it is no longer needed. *See, e.g.*, Snapchat,
12 *When are Snaps and Chats Deleted?*, <https://goo.gl/adHPnO> (“Delete is our
13 default.”); David Rowan, *WhatsApp: The Inside Story*, Wired UK, Feb. 19, 2014
14 (WhatsApp does not store users' messages on its servers). Others have designed
15 their services so that users can store and easily search large volumes of data
16 spanning a long stretch of time. Indeed, how companies store and manage
17 customers' data is one way companies tailor their chat, e-mail, social-media, and
18 data-storage solutions to customers' needs. Change those features and the
19 government has changed the product in a fundamental way. The government
20 therefore does not seek unobjectionable technical assistance; it seeks the ability to
21 compel technology companies to modify their products, on spec, for the FBI in
22 ways that are contrary to their core values.

23 The distinction between the use of existing tools and the creation of new ones
24 against companies' wishes is borne out in the Ninth Circuit's All Writs Act case
25 law. *Plum Creek* emphasized that although the Act allows a court to compel a third
26 party “to provide nonburdensome technical assistance,” it does not permit “forcing
27 an employer to rescind a company policy so that [a government agency] can more
28 efficiently conduct an investigation.” 608 F.2d at 1289-1290. *Amici* have policies

1 against undermining their own security features. The government seeks the power
 2 to force *amici* and other technology companies to rescind those policies, and,
 3 worse, the power to impose a new, contrary policy. That is precisely what *Plum*
 4 *Creek* forbids. *See id.*

5
 6 **B. The Government’s Position, If It Prevails, Will Undermine The
 Security Of Americans’ Most Sensitive Data.**

7 *Amici* do not create security-protecting features just to satisfy their own
 8 ideological predilections. They also do so in response to “consumer demands to
 9 protect private data.” Devlin Barrett et al., *Apple and Others Encrypt Phones,*
 10 *Fueling Government Standoff*, Wall St. J. (Nov. 18, 2014). As storing sensitive
 11 personal and commercial data electronically becomes less of a luxury and more of a
 12 necessity, protecting that data has also become a necessity. That is why in 2013 the
 13 White House rolled out a comprehensive strategy to combat trade-secret theft, with
 14 a particular focus on enhanced cybersecurity. *See* The White House,
 15 *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* 1 (Feb.
 16 2013), <https://goo.gl/S7pXaD>. Strong privacy protections from companies like
 17 *amici* are an important component of that strategy. *See* Office of the Nat’l
 18 Counterintelligence Exec., *Foreign Spies Stealing US Economic Secrets in*
 19 *Cyberspace*, A-4 to A-5 (Oct. 2011), <http://goo.gl/QidbfG> (identifying data
 20 encryption and multi-factor authentication measures as “[b]est [p]ractices” for data
 21 protection).

22 The government’s bid to have technology companies undermine their own
 23 security measures is all the more puzzling because the Executive has been
 24 *encouraging* companies to increase cybersecurity in consumer products. The
 25 Federal Trade Commission, for instance, has claimed the power to sanction
 26 companies that do not adequately secure their customers’ data. *See FTC v.*
 27 *Wyndham Worldwide Corp.*, 799 F.3d 236, 240-242 (3d Cir. 2015). The White
 28 House has touted its work with technology companies, including many of the *amici*,

1 to enhance security on consumer accounts. See The White House, Office of the
2 Press Sec’y, *Fact Sheet: Cybersecurity National Action Plan* (Feb. 9, 2016),
3 <https://goo.gl/2hWPWV> (“By judiciously combining a strong password with
4 additional factors, such as a fingerprint or a single use code delivered in a text
5 message, Americans can make their accounts even more secure.”). And Director
6 Comey has told the Senate Judiciary Committee that “[t]he development and robust
7 adoption of strong encryption is a key tool to secure commerce and trade, safeguard
8 private information, promote free expression and association, and strengthen cyber
9 security.” James B. Comey, Dir., FBI, *Joint Statement with Deputy Attorney
10 General Sally Quillian Yates Before the Senate Judiciary Committee* (July 8, 2015),
11 <https://goo.gl/Pdht0w>; see also Amy Hess, Exec. Assistant Dir., Sci. & Tech.
12 Branch, FBI, *Statement Before the House Oversight and Government Reform
13 Committee, Subcommittee on Information Technology* (Apr. 29, 2015),
14 <https://goo.gl/jzxaLi> (“To be clear, we in the FBI support and encourage the use of
15 secure networks and sophisticated encryption to prevent cyber threats to our critical
16 national infrastructure, our intellectual property, and our data.”).

17 These are not one-off statements. Until recently, the FBI’s webpage listed
18 tips for protecting consumers’ mobile devices like “[p]asscode protect your mobile
19 device” and “[d]epending on the type of phone, the operating system may have
20 encryption available.” Mike Masnick, Techdirt, *FBI Claims It Has No Record of
21 Why It Deleted Its Recommendation to Encrypt Phones* (Feb. 29, 2016),
22 <https://goo.gl/P8ewUL>. Similarly, the President’s Review Group on Intelligence
23 and Communications Technologies recommended in December 2013 that the
24 government “take additional steps to promote security” by “(1) fully supporting and
25 not undermining efforts to create encryption standards; (2) making clear that it will
26 not in any way subvert, undermine, weaken, or make vulnerable generally available
27 commercial encryption; and (3) supporting efforts to encourage the greater use of
28 encryption technology.” President’s Review Grp. on Intelligence & Commc’ns

1 Techs., *Report and Recommendations: Liberty and Security in a Changing World*
2 22 (Dec. 12, 2013), <https://goo.gl/HXghaV>. *Amici's* security features in their
3 products comport with these past recommendations.

4 The government reconciles its conflicting positions by arguing that security
5 is all well and good, just so long as it does not interfere with the execution of a
6 lawful warrant. *See* Mot. to Compel 21. But once a company builds a security-
7 defeating tool, it cannot guarantee that it will be used by law enforcement only and
8 always. *See* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by*
9 *Requiring Government Access to All Data and Communications 2* (July 6, 2015),
10 <https://goo.gl/Jv5tCK> (observing that “exceptional access would create
11 concentrated targets that could attract bad actors”); The Chertoff Group, *The*
12 *Ground Truth About Encryption and the Consequences of Extraordinary Access*,
13 <http://goo.gl/Z9xPpj> (concluding that “an extraordinary access requirement is likely
14 to have a negative impact on technological development, the United States’
15 international standing, and the competitiveness of the U.S. economy”).

16 As one legislator has explained, “if we put in backdoors for the convenience
17 of the government, those backdoors can be exploited by hackers as well.” Erin
18 Kelly, *Bill Would Stop Feds from Mandating ‘Backdoor’ to Data*, USA Today,
19 Apr. 2, 2015 (quoting Representative Thomas Massie). Not just hackers: Other
20 countries, including countries with less-robust due-process guarantees, would
21 demand similar access. *See* Ellen Nakashima, *Google, Facebook and Other*
22 *Powerful Tech Firms Filing Briefs to Support Apple*, Wash. Post, Feb. 28, 2016.
23 And if companies’ security-defeating tools were to fall into the wrong hands, the
24 companies—not the U.S. government—would be the ones left to deal with the
25 fallout of lawsuits, lost customers, and damaged reputations. That very real risk is
26 not merely a “marketing or general policy concern[.]” Mot. to Compel 20. It is a
27 danger that any technology company would be blind to ignore.

28

1 The government may believe that the risk to technology companies is so
2 minimal or that the benefit to its investigations so great that the risks are ones that
3 the companies should bear. But the Ninth Circuit held in *Plum Creek* that the All
4 Writs Act “does not give the district court a roving commission to order a party
5 subject to an investigation to accept additional risks at the bidding of” government
6 agents. 608 F.2d at 1289. The All Writs Act, the Court explained, “does not
7 authorize a court to order a party to bear risks not otherwise demanded by law, or to
8 aid the government in conducting a more efficient investigation.” *Id.* at 1289-1290.
9 Yet that is what the government asks technology companies to do—to use their
10 own personnel to defeat their own products’ security and to assume all the risks that
11 the tool the government commanded them to make will fall into the wrong hands.
12 That is simply too great a risk to impose on third parties under the limited, residual
13 authority furnished by the All Writs Act.

14 **III. THE CANON OF CONSTITUTIONAL AVOIDANCE COUNSELS**
15 **AGAINST THE GOVERNMENT’S EXPANSIVE INTERPRETATION**
16 **OF THE ALL WRITS ACT.**

17 The canon of constitutional avoidance provides yet another reason to reject
18 the government’s expansive interpretation of the All Writs Act. Under that canon,
19 where “an otherwise acceptable construction of a statute would raise serious
20 constitutional problems, and where an alternative interpretation of the statute is
21 ‘fairly possible,’ [a court is] obligated to construe the statute to avoid such
22 problems.” *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citation omitted). The
23 government’s interpretation of the All Writs Act presents grave constitutional
24 problems under the First Amendment: Computer code is protected speech, and the
25 government asks this Court, under the authority of the All Writs Act, to compel
26 Apple to write code. It also raises serious due process and separation-of-powers
27 questions. *See In re Order*, No. 15-MC-1902, at 27-30; Mot. to Vacate 18-19, 34.
28 This Court should reject the government’s constitutionally problematic reading of
the vague terms of the All Writs Act.

1 Writing computer code can be a creative, complex, and expressive task, and
 2 it is a form of protected speech under the First Amendment. In the Second Circuit’s
 3 unequivocal words, “software programs qualify as ‘speech’ for First Amendment
 4 purposes.” *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 448 n.22 (2d Cir.
 5 2001); *id.* at 449 (“[W]e join the other courts that have concluded that computer
 6 code, and computer programs constructed from code can merit First Amendment
 7 protection.”). The Sixth Circuit has similarly determined that “computer source
 8 code” is “protected by the First Amendment,” because it “is an expressive means
 9 for the exchange of information and ideas about computer programming.” *Junger*
 10 *v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000). A panel of the Ninth Circuit has
 11 likewise held that “encryption software, in its source code form and as employed by
 12 those in the field of cryptography, must be viewed as expressive for First
 13 Amendment purposes.” *Bernstein v. Dep’t of Justice*, 176 F.3d 1132, 1141 (9th
 14 Cir. 1999) (footnote omitted).⁶

15 Recent Supreme Court case law strengthens those holdings. In *Sorrell v. IMS*
 16 *Health Inc.*, 131 S. Ct. 2653, 2667 (2011), the Supreme Court reaffirmed the broad
 17 principle that “information is speech,” and computer code is, at a minimum, a type
 18 of information. In *Brown v. Entertainment Merchants Ass’n*, 131 S. Ct. 2729
 19 (2011), the Court held that digital video games are entitled to First Amendment
 20 protection. It explained: “whatever the challenges of applying the Constitution to
 21 ever-advancing technology, the basic principles of freedom of speech and the press,
 22 like the First Amendment’s command, do not vary when a new and different
 23 medium for communication appears.” *Id.* at 2733 (citation and internal quotation
 24 marks omitted). Computer code may be a “new and different medium for
 25 communication,” but it is not, as a consequence, any less deserving of protection.
 26

27 ⁶ The Ninth Circuit granted rehearing en banc in *Bernstein*, and withdrew the
 28 panel opinion, 192 F.3d 1308 (9th Cir. 1999), but never actually decided the issue
 en banc because the regulations at issue were changed.

1 The government seeks to force Apple and its engineers to write software—
2 that is, to engage in protected speech—against their will. In the government’s own
3 words, the order would require Apple to “writ[e] software code.” Mot. to Compel
4 13. This Court’s order would also require Apple to cryptographically “sign[]” code
5 as authentic when it is clearly nothing more than government compulsion. Order
6 Compelling Apple, Inc. to Assist Agents in Search at 2, No. 15-MJ-451, Dkt. No.
7 19 (C.D. Cal. Feb. 16, 2016). That is classic compelled speech. And as the
8 Supreme Court has explained, “[t]here is certainly some difference between
9 compelled speech and compelled silence, but in the context of protected speech, the
10 difference is without constitutional significance.” *Riley v. Nat’l Fed’n of the Blind*
11 *of N.C., Inc.*, 487 U.S. 781, 796 (1988). That is because “the First Amendment
12 guarantees ‘freedom of speech,’ a term necessarily comprising the decision of both
13 what to say and what *not* to say.” *Id.* at 796-797. Computer code is “protected
14 speech,” and technology companies therefore have the right to determine for
15 themselves “what *not* to say.” *Id.* The government’s interpretation of the All Writs
16 Act would invest courts with a “roving commission” to invade that right. *Plum*
17 *Creek*, 608 F.2d at 1289.

18 The All Writs Act certainly does not confer that power explicitly; it is not a
19 blank check to the federal courts. Rather, it only authorizes “writs” that are, among
20 other things, “agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a).
21 It is certainly not *clear* that an order compelling a third-party to write source code is
22 the sort of “writ[]” authorized by the Act, or that it is “agreeable to the usages and
23 principles of law”—because it is historically unprecedented, because it encroaches
24 on an area fully regulated by Congress, and because it is in tension with
25 constitutional values. *Id.*

26 In the absence of a clearer statement from Congress, the avoidance canon
27 compels a court to construe the vague All Writs Act in a way that does *not* raise
28 serious First Amendment concerns. As the Supreme Court has explained, when one

1 interpretation of a statute “presents a significant risk that the First Amendment will
2 be infringed,” a court should adopt it only if it is the “affirmative intention of the
3 Congress clearly expressed.” *NLRB v. Catholic Bishop of Chicago*, 440 U.S. 490,
4 502, 506 (1979) (citations omitted); *see also NAACP v. Button*, 371 U.S. 415, 433
5 (1963) (“Because First Amendment freedoms need breathing space to survive,
6 government may regulate in the area only with narrow specificity.”). Congress
7 certainly did not express the clear and affirmative intention to authorize orders
8 compelling speech.

9 In short, the government’s reading of the All Writs Act raises serious First
10 Amendment problems, because it would allow a court to compel protected speech.
11 And because the All Writs Act does not clearly and specifically authorize such an
12 order, this Court should decline to grant it.


13 **CONCLUSION**

14 For the foregoing reasons, the Court should vacate its order compelling
15 Apple to assist the government and deny the government’s motion to compel
16 assistance.

17 Dated: March 3, 2016

Respectfully submitted,

HOGAN LOVELLS US LLP

20 By: 
21 Michael M. Maddigan
22 Neal Kumar Katyal (*pro hac vice*
23 application forthcoming)
24 Attorneys for *Amici Curiae*