

ORIGINAL

1 JEROME C. ROTH (State Bar No. 159483)
 jerome.roth@mto.com
 2 ROSEMARIE T. RING (State Bar No. 220769)
 rose.ring@mto.com
 3 JONATHAN H. BLAVIN (State Bar No. 230269)
 jonathan.blavin@mto.com
 4 JOSHUA PATASHNIK (State Bar No. 295120)
 josh.patashnik@mto.com
 5 MUNGER, TOLLES & OLSON LLP
 560 Mission Street
 6 Twenty-Seventh Floor
 San Francisco, California 94105-2907
 7 Telephone: (415) 512-4000
 Facsimile: (415) 512-4077
 8



9 ARIEL C. GREEN (State Bar No. 304780)
 ariel.green@mto.com
 10 MUNGER, TOLLES & OLSON LLP
 355 South Grand Avenue
 11 Thirty-Fifth Floor
 Los Angeles, California 90071-1560
 12 Telephone: (213) 683-9100
 Facsimile: (213) 687-7302
 13

Attorneys for *Amici Curiae*

14
 15 UNITED STATES DISTRICT COURT
 16 CENTRAL DISTRICT OF CALIFORNIA
 17 EASTERN DIVISION

LOGGED

14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

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

Case No. ED No. CM 10-16-SP
**[PROPOSED] ORDER GRANTING
 MOTION OF AIRBNB, INC.;**
ATLISSIAN PTY. LTD.;
AUTOMATTIC INC.;
CLOUDFLARE, INC.; EBAY INC.;

Judge: Hon. Sheri Pym

1 On March 3, 2016, Airbnb, Inc., Atlassian Pty. Ltd., Automattic Inc.,
2 CloudFlare, Inc., eBay Inc., GitHub, Inc., Kickstarter, PBC, LinkedIn Corporation,
3 Mapbox Inc., A Medium Corporation, Meetup, Inc., Reddit, Inc., Square, Inc.,
4 Squarespace, Inc., Twilio Inc., Twitter, Inc., and Wickr Inc. filed a motion for leave
5 to file a brief as *Amici Curiae* in connection with Respondent Apple Inc.'s Motion
6 to Vacate Order Compelling Apple Inc. to Assist Agents in Search, which is
7 scheduled for hearing on March 22, 2016.

8 Having considered the motion, and finding that good cause has been shown,
9 the Court **GRANTS** the motion of Airbnb, Inc., Atlassian Pty. Ltd., Automattic Inc.,
10 CloudFlare, Inc., eBay Inc., GitHub, Inc., Kickstarter, PBC, LinkedIn Corporation,
11 Mapbox Inc., A Medium Corporation, Meetup, Inc., Reddit, Inc., Square, Inc.,
12 Squarespace, Inc., Twilio Inc., Twitter, Inc., and Wickr Inc. to file a brief as *Amici*
13 *Curiae*. The brief of *Amici Curiae*, submitted concurrently with the Motion, hereby
14 is ordered and deemed filed.

15
16 **IT IS SO ORDERED.**

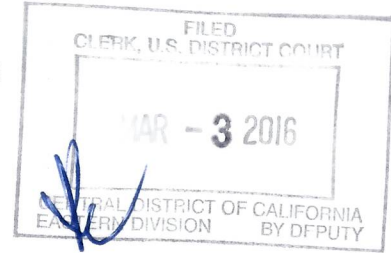
17 DATED: March 3, 2016

18
19
20 

21 _____
22 Honorable Sheri Pym
23 United States Magistrate Judge
24
25
26
27
28

ORIGINAL

1 JEROME C. ROTH (State Bar No. 159483)
 jerome.roth@mto.com
 2 ROSEMARIE T. RING (State Bar No. 220769)
 rose.ring@mto.com
 3 JONATHAN H. BLAVIN (State Bar No. 230269)
 jonathan.blavin@mto.com
 4 JOSHUA PATASHNIK (State Bar No. 295120)
 josh.patashnik@mto.com
 5 MUNGER, TOLLES & OLSON LLP
 560 Mission Street
 6 Twenty-Seventh Floor
 San Francisco, California 94105-2907
 7 Telephone: (415) 512-4000
 Facsimile: (415) 512-4077
 8



9 ARIEL C. GREEN (State Bar No. 304780)
 ariel.green@mto.com
 10 MUNGER, TOLLES & OLSON LLP
 355 South Grand Avenue
 11 Thirty-Fifth Floor
 Los Angeles, California 90071-1560
 12 Telephone: (213) 683-9100
 Facsimile: (213) 687-7302
 13

Attorneys for *Amici Curiae*

14
 15 UNITED STATES DISTRICT COURT
 16 CENTRAL DISTRICT OF CALIFORNIA
 17 EASTERN DIVISION
 18

19 IN THE MATTER OF THE SEARCH
 OF AN APPLE IPHONE SEIZED
 20 DURING THE EXECUTION OF A
 SEARCH WARRANT ON A BLACK
 21 LEXUS IS300, CALIFORNIA
 LICENSE PLATE 35KGD203
 22
 23
 24
 25
 26
 27
 28

Case No. ED CM 16-10-SP

BRIEF OF *AMICI CURIAE*
AIRBNB, INC.; ATLISSIAN PTY.
LTD.; AUTOMATTIC INC.;
CLOUDFLARE, INC.; EBAY INC.;
GITHUB, INC.; KICKSTARTER,
PBC; LINKEDIN CORPORATION;
MAPBOX INC.; A MEDIUM
CORPORATION; MEETUP, INC.;
REDDIT, INC.; SQUARE, INC.;
SQUARESPACE, INC.; TWILIO
INC.; TWITTER, INC.; AND
WICKR INC.

Judge: Hon. Sheri Pym

LOGGED

2016 MAR -3 AM 11:55
 CLERK U.S. DISTRICT COURT
 CENTRAL DIST. OF CALIF.
 RIVERSIDE

TABLE OF CONTENTS

	Page
I. INTEREST OF <i>AMICI CURIAE</i>	1
II. SUMMARY OF ARGUMENT	3
III. ALLOWING THE GOVERNMENT TO FORCE COMPANIES TO UNDERMINE THEIR OWN PROMISED SECURITY MEASURES WILL ERODE THE CORE VALUES OF PRIVACY, SECURITY, AND TRANSPARENCY.....	5
A. In The Current Era of Rapid Technological Change, the Core Values of Privacy, Security, and Transparency Are More Vital than Ever	6
B. <i>Amici</i> Are Committed to Advancing These Core Values by Employing Security Technologies to Protect User Data, Acting Transparently, and Providing Users Control over Their Data.....	7
C. <i>Amici</i> Recognize and Respect the Government’s Important Work Protecting Our National Security.....	8
D. The Government’s Request Has No Legal Limits and Will Undermine Existing, Transparent Statutory Schemes that Reflect a Balancing of Competing Policy Considerations	9
E. Forcing Technology Companies to Break Their Own Security Measures Will Undermine User Confidence that Their Data Is Secure and Being Handled Transparently.....	12
IV. THE GOVERNMENT LACKS THE AUTHORITY UNDER THE ALL WRITS ACT TO FORCE A PRIVATE PARTY TO RE-WRITE ITS SOFTWARE CODE AND SERVE AS AN INVESTIGATIVE ARM OF LAW ENFORCEMENT	14
A. The All Writs Act Is a Gap-Filling Measure, Not a Broad Independent Grant of Substantive Power to Federal Courts	15
B. Congress Has Enacted Several Statutes that Together Provide a Comprehensive Regulatory Regime Allowing the Government in Certain Circumstances to Obtain Assistance from Third Parties in the Course of Investigations, Displacing the All Writs Act	16
1. Congress’s Decision to Prohibit Limits on Encryption and to Exclude Information Service Providers in CALEA Evidences Its Intent to Deny the Relief Sought by the Government	17
2. Congress Has Placed Significant Limits on Law Enforcement’s Ability to Compel Technical Assistance from Third Parties.....	19

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

C. Courts Have Rejected Similar Efforts Under the All Writs Act to Compel Forms of Assistance that Are Not Contemplated by Statute.....20

D. The Cases upon Which the Government Relies Do Not Support Forcing a Private Party to Create New Technology to Assist the Government’s Investigation.....23

V. CONCLUSION25

TABLE OF AUTHORITIES

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

Page

FEDERAL CASES

ACLU v. Clapper,
785 F.3d 787 (2d Cir. 2015)..... 11, 12

In re Apple, Inc.,
___ F. Supp. 3d ___, 2016 WL 783565 (E.D.N.Y. Feb. 29, 2016) 19, 22, 25

In re Apple, Inc.,
2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015) 19, 22, 25

In re Application of U.S.,
396 F. Supp. 2d 294 (E.D.N.Y. 2005)..... 21, 22

In re Application of U.S.,
849 F. Supp. 2d 526 (D. Md. 2011) 22, 24

*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)..... 25

*In re Application of U.S. for an Order Authorizing the Roving
Interception of Oral Commc’ns*,
349 F.3d 1132 (9th Cir. 2003)..... 20

*In re Application of U.S. for an Order Directing a Provider of
Commc’ns Servs. to Provide Tech. Assistance*,
___ F. Supp. 3d ___, 2015 WL 5233551 (D.P.R. Aug. 27, 2015)..... 25

*In re Application of U.S. for an Order Directing X to Provide Access to
Videotapes*,
2003 WL 22053105 (D. Md. Aug. 22, 2003)..... 23

Carlisle v. United States,
517 U.S. 416 (1996) 16

City of Ontario v. Quon,
560 U.S. 746 (2010) 7, 9

Harris v. Nelson,
394 U.S. 286 (1969) 15

1 *Jackson v. Vasquez*,
 2 1 F.3d 885 (9th Cir. 1993) 15

3 *McClung v. Silliman*,
 4 19 U.S. (6 Wheat.) 598 (1821) 15

5 *McIntire v. Wood*,
 6 11 U.S. (7 Cranch) 504 (1813) 15

7 *Pa. Bureau of Corr. v. U.S. Marshals Serv.*,
 8 474 U.S. 34 (1985) 15, 16

9 *Plum Creek Lumber Co. v. Hutton*,
 608 F.2d 1283 (9th Cir. 1979) 20, 21, 23

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

12 *Syngenta Crop Protection, Inc. v. Henson*,
 13 537 U.S. 28 (2002) 16

14 *U.S. Alkali Export Ass'n v. United States*,
 15 325 U.S. 196 (1945) 16

16 *United States v. Cotterman*,
 17 709 F.3d 952 (9th Cir. 2013) 7, 10

18 *United States v. Doe*,
 19 537 F. Supp. 838 (E.D.N.Y. 1982) 23

20 *United States v. Hall*,
 583 F. Supp. 717 (E.D. Va. 1984) 23

21 *United States v. Jones*,
 22 132 S. Ct. 945 (2012) 11

23 *United States v. Mosko*,
 24 654 F. Supp. 402 (D. Colo. 1987) 25

25 *United States v. New York Telephone Co.*,
 26 434 U.S. 159 (1977) 24, 25

27 *In re XXX, Inc.*,
 28 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014) 25

1	FEDERAL STATUTES	
2	Communications Assistance for Law Enforcement Act (CALEA),	
3	47 U.S.C. § 1001, <i>et seq.</i>	<i>passim</i>
4	Foreign Intelligence Surveillance Act (FISA),	
5	50 U.S.C. § 1801, <i>et seq.</i>	4, 19, 20
6	Judiciary Act of 1789,	
7	1 Stat. 73	5, 15
8	Stored Communications Act (SCA),	
9	18 U.S.C. § 2701, <i>et seq.</i>	4, 19
10	Wiretap Act,	
11	codified at 18 U.S.C. § 2510, <i>et seq.</i>	4, 19, 20
12	18 U.S.C. § 2518.....	19, 20
13	18 U.S.C. § 2703.....	19
14	18 U.S.C. § 3124.....	19
15	28 U.S.C. § 1651.....	15
16	28 U.S.C. § 2241.....	16
17	28 U.S.C. § 2243.....	16
18	47 U.S.C. § 1002.....	17, 18, 19, 20
19	50 U.S.C. § 1802.....	19, 20
20	50 U.S.C. § 1805.....	20
21	50 U.S.C. § 1822.....	19, 20
22	50 U.S.C. § 1824.....	20
23	50 U.S.C. § 1842.....	19, 20
24	50 U.S.C. § 1861.....	19
25	50 U.S.C. § 1881a.....	20
26	50 U.S.C. § 1881b.....	20
27		
28		

1 **FEDERAL RULES**

2 Fed. R. Crim. P. 29 16

3 **FEDERAL LEGISLATIVE MATERIALS**

4 H.R. Rep. No. 103-827(I) (1994) 17, 18

5 S. Rep. No. 99-541 (1986)..... 20

6

7 **OTHER AUTHORITIES**

8 Berkman Ctr. for Internet & Soc’y, *Don’t Panic: Making Progress on*

9 *the “Going Dark” Debate*, Appendix A to Landau (2016),

10 [https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf)

11 [Making_Progress_on_Going_Dark_Debate.pdf](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf)..... 13

12 Bruce Schneier, *Security or Surveillance?* (2016),

13 [https://www.schneier.com/essays/archives/2016/02/security_vs_sur](https://www.schneier.com/essays/archives/2016/02/security_vs_surveill.html)

14 [veill.html](https://www.schneier.com/essays/archives/2016/02/security_vs_surveill.html)..... 13

15 eBay Privacy Policy, [http://pages.ebay.com/help/policies/privacy-](http://pages.ebay.com/help/policies/privacy-policy.html)

16 [policy.html](http://pages.ebay.com/help/policies/privacy-policy.html) 8

17 Encryption Tightrope: Balancing Americans’ Security and Privacy,

18 YOUTUBE (March 1, 2016),

19 [https://www.youtube.com/watch?v=g1GgnbN9oNw&feature=youtu](https://www.youtube.com/watch?v=g1GgnbN9oNw&feature=youtu.be&t=3656)

20 [.be&t=3656](https://www.youtube.com/watch?v=g1GgnbN9oNw&feature=youtu.be&t=3656) 10

21 Executive Office of the President, *Consumer Data Privacy in a*

22 *Networked World: A Framework for Protecting Privacy and*

23 *Promoting Innovation in the Global Digital Economy*,

24 <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf> 6

25 Katie Benner & Matt Apuzzo, *Narrow Focus May Aid FBI in Apple*

26 *Case*, N.Y. Times (Feb. 22, 2016)..... 10

27 LinkedIn Privacy Policy, www.linkedin.com/legal/privacy-policy 8

28 LinkedIn Transparency Report,

<https://www.linkedin.com/legal/transparency#government-requests> 8

Kickstarter Transparency Report,

[https://www.kickstarter.com/blog/kickstarter-transparency-report-](https://www.kickstarter.com/blog/kickstarter-transparency-report-2014)

[2014](https://www.kickstarter.com/blog/kickstarter-transparency-report-2014) 8

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

Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 859 (2004)..... 9

Pew Research Center, *Americans’ Attitudes About Privacy, Security and Surveillance* (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/> 13

Rep. Peter T. King, *Remembering the Lessons of 9/11*, 41 J. LEGIS. 173, 178 (2014-2015) 19

Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. Rev. 245, 263 (2002)..... 12

Steven Levy, *Battle of the Clipper Chip*, N.Y. Times (June 12, 1994) 17

Twilio Transparency Report, <https://www.twilio.com/legal/transparency>..... 8

Twitter Privacy Policy, <https://twitter.com/privacy> 8

Twitter Transparency Report for the United States, <https://transparency.twitter.com/country/us> 9

1 **I. INTEREST OF *AMICI CURIAE***

2 *Amici curiae* are providers of platforms and tools for communicating,
3 publishing, connecting, transacting, and securing traffic over the Internet: Airbnb, Inc.
4 (“Airbnb”), Atlassian Pty. Ltd. (“Atlassian”), Automattic Inc. (“Automattic”),
5 CloudFlare, Inc. (“CloudFlare”), eBay Inc. (“eBay”), GitHub, Inc. (“GitHub”),
6 Kickstarter, PBC (“Kickstarter”), LinkedIn Corporation (“LinkedIn”), Mapbox Inc.
7 (“Mapbox”), A Medium Corporation (“Medium”), Meetup, Inc. (“Meetup”), Reddit,
8 Inc. (“Reddit”), Square, Inc. (“Square”), Squarespace, Inc. (“Squarespace”), Twilio
9 Inc. (“Twilio”), Twitter, Inc. (“Twitter”), and Wickr Inc. (“Wickr”). The number of
10 users of their platforms and tools is over one billion.

11 Airbnb provides an Internet platform through which persons desiring to book
12 accommodations, and persons listing unique accommodations available for rental,
13 can locate each other and enter into direct agreements with each other to reserve and
14 book travel accommodations on a short and long-term basis.

15 Atlassian’s products help teams organize, discuss, and complete their work in a
16 coordinated, efficient and modern fashion. Organizations use Atlassian’s project
17 tracking, content creation and sharing and real-time communication and service
18 management products to work better together and deliver quality results on time.

19 Automattic is the company behind WordPress.com, the online publishing
20 platform that serves more than 15.8 billion pages a month, as well as a host of other
21 popular online services, such as WooCommerce, Jetpack, and Simplenote.

22 CloudFlare offers some of the most advanced web security, distributed denial
23 of service attack mitigation, and content delivery solutions available. CloudFlare is
24 a community of over 2 million websites handling as much as 5 percent of global
25 web and blocking more than 8.3 billion potentially malicious requests every day.

26 eBay is a global commerce leader. With more than 160 million active buyers
27 and more than 800 million live listings globally, eBay enables sellers worldwide to
28 organize and offer their inventory for sale and buyers to find and buy virtually

1 anything, anytime, anywhere.

2 GitHub is a web-based hosting and collaboration platform where people
3 discover, share and contribute to software.

4 Kickstarter is a worldwide community of people dedicated to bringing
5 creative projects to life—a place where people come together to make new things
6 like films, food trucks, board games, and innovative technology.

7 LinkedIn is an Internet company that hosts the world’s largest professional
8 network, with over 400 million members worldwide and over 122 million members
9 in the United States. LinkedIn’s mission is to connect the world’s professionals to
10 enable them to be more productive and successful.

11 Mapbox provides highly customizable maps and mapping software for web,
12 mobile, and embedded applications. Based in Washington, D.C., Mapbox powers
13 the maps behind some of the most visited sites on the web.

14 Medium, based in San Francisco, is an online publishing platform that allows
15 anyone to easily read, write, and share stories and ideas that matter to them. Tens of
16 millions of users have spent more than 3.5 millennia reading together on Medium.

17 Meetup is the world’s largest network of local community groups, enabling
18 people to connect with others online and engage in activities offline.

19 Reddit operates the reddit.com platform, which is a collection of thousands of
20 online communities attracting over 230 million monthly unique visitors that create,
21 read, join, discuss and vote on conversations across a myriad of topics.

22 Square creates tools and services to make commerce easy, from empowering
23 sellers with the tools needed to take their first credit card payment, to providing
24 software for every part of starting, running, and growing a business.

25 Squarespace provides web publishing and development platforms, including
26 Squarespace.com, for creating high quality websites easily and affordably.

27 Twilio is a cloud communications platform that makes communications easy
28 and powerful. With Twilio’s platform, businesses can make communications relevant

1 and contextual by embedding real-time communication and authentication capabilities
2 directly into their software applications.

3 Twitter is a global platform for public self-expression and conversation that
4 gives users the power to create and share ideas, information, and rich media content
5 with each other, instantly. Twitter has more than 300 million monthly active users
6 who share hundreds of millions of Tweets per day.

7 Wickr is a secure communications platform which provides end-to-end
8 encryption and industry-leading security to businesses and individuals around the
9 world to safeguard high-value proprietary and personal data and communications.

10 As providers of several of the most popular communication, networking,
11 ecommerce, publishing, and commercial transaction platforms on the Internet
12 accessed via websites and/or applications on mobile devices, *Amici* have a strong
13 interest in this case, the continued security and privacy of their users' data, and in
14 transparency to users regarding how that data is protected. Several *Amici* also
15 regularly assist in law-enforcement investigations and have a strong interest in
16 ensuring that government requests for user data are made within the bounds of
17 applicable laws, including those that balance the interests of privacy, security, and
18 transparency with law enforcement needs.

19 **II. SUMMARY OF ARGUMENT**

20 The government in this case has invoked a centuries-old statute, the All Writs
21 Act (the "Act"), to force Apple, Inc. ("Apple") to develop software to undermine its
22 own carefully constructed security measures, which were designed to protect its
23 customers' data from hacking, misuse, and theft. This extraordinary and
24 unprecedented effort to compel a private company to become the government's
25 investigative arm not only has no legal basis under the All Writs Act or any other
26 law, but threatens the core principles of privacy, security, and transparency that
27 underlie the fabric of the Internet.

28 In today's era of rapid technological change, these bedrock principles are more

1 vital than ever. The increasing ubiquity of the Internet in all aspects of life has
2 ushered in a new generation of innovative products and services for consumers and
3 businesses. In the midst of this digital revolution—and the ever-present and
4 increasing dangers posed by hackers, identity thieves, and other wrongdoers—
5 ensuring that users’ data is handled in a safe, secure, and transparent manner that
6 protects privacy is of utmost importance.

7 At the same time, *Amici* recognize and respect the government’s important
8 work in law enforcement and national security. Indeed, although *Amici* oppose any
9 forced “backdoors” providing the government access to their systems, they do and
10 will continue to comply with proper and reasonable requests for data pursuant to
11 legal processes enacted by legislatures and consistent with the Constitution. But the
12 government’s efforts in this case—to force a private company to affirmatively
13 develop software that does not currently exist in order to break its own security
14 systems—would erode the privacy and protection of user data, and transparency as
15 to how such data may be used or shared.

16 The government’s demand here, at its core, is unbound by any legal limits. It
17 would set a dangerous precedent, in which the government could sidestep established
18 legal procedures authorized by thorough, nuanced statutes to obtain users’ data in
19 ways not contemplated by lawmakers. These laws include the federal Wiretap Act
20 (“Title III”) (codified at 18 U.S.C. §§ 2510, *et seq.*), the Stored Communications Act
21 (“SCA”) (codified at 18 U.S.C. §§ 2701, *et seq.*), the Communications Assistance for
22 Law Enforcement Act (“CALEA”) (codified at 47 U.S.C. §§ 1001, *et seq.*), and the
23 Foreign Intelligence Surveillance Act (“FISA”) (codified at 50 U.S.C. §§ 1801, *et*
24 *seq.*). Together these statutes provide a comprehensive regulatory scheme enabling
25 law-enforcement agencies to secure the assistance of third parties in accessing
26 communications and data in connection with their investigative functions in the
27 manner and subject to the limitations that Congress has deemed appropriate.

28 In enacting such laws, Congress balanced law enforcement and national

1 security needs with the important interests of protecting users' privacy and security.
2 Congress also considered the impact that regulating or mandating certain levels of
3 law-enforcement assistance may have on innovation, creativity and growth by the
4 technology industry. By circumventing the procedures adopted by Congress, and
5 thereby overturning the careful weighing of policy considerations they reflect, the
6 government is seeking to enlist the judiciary in re-writing laws without engaging in
7 an essential public debate. While *Amici* are sensitive to the emotionally charged
8 atmosphere that can surround investigations such as this one, a meaningful discourse
9 on this topic is critical for all members of our society as we strive to meet the
10 challenge of finding the proper balance between privacy and liberty interests and the
11 dangers posed by criminal and national-security threats.

12 The All Writs Act does not authorize the government to make an end-run
13 around this important public debate and our nation's legislative processes. The Act
14 is a gap-filling procedural measure, not a broad independent grant of substantive
15 power to federal courts. Its purpose, dating back to the Judiciary Act of 1789, is to
16 allow courts to issue writs necessary to effectuate their *existing* powers, not to give
17 courts new powers. For that reason, the Supreme Court repeatedly has recognized
18 that where another statute speaks to the issue at hand, the All Writs Act is displaced
19 and the applicable statutory scheme governs. The government may not use the Act
20 here to circumvent the limitations imposed by the existing, comprehensive statutory
21 scheme to arrogate to itself powers that Congress has chosen not to provide it.

22 For these reasons and those discussed below, *Amici* respectfully urge the Court
23 to deny the government's Motion to Compel and to grant Apple's Motion to Vacate.

24 **III. ALLOWING THE GOVERNMENT TO FORCE COMPANIES TO**
25 **UNDERMINE THEIR OWN PROMISED SECURITY MEASURES**
26 **WILL ERODE THE CORE VALUES OF PRIVACY, SECURITY, AND**
27 **TRANSPARENCY**

28 The government's efforts in this case to force a private company to become
its investigative arm and to take affirmative steps to undermine the company's own

1 promised security measures—essential to the protection of its users’ data—are not
2 only legally unprecedented and unfounded (as discussed below), but they will also
3 erode the critically important principles of privacy, security, and transparency,
4 causing tangible harm to users, Apple and the industry, and society more generally.

5 **A. In The Current Era of Rapid Technological Change, the Core Values**
6 **of Privacy, Security, and Transparency Are More Vital than Ever**

7 In an era where technologies and business models are evolving as rapidly as
8 they are now, the bedrock principles of privacy, security, and transparency are more
9 important than ever.

10 An ever growing range of services delivered to devices as diverse as mobile
11 phones, tablets, computers, appliances, and cars have become an increasingly
12 important and integral part of our daily lives, in ways that could never have been
13 envisioned as recently as five or ten years ago. These services provide the ability to
14 communicate with friends, family, colleagues, external advisers and the world at
15 large; to share and read live news from around the world or in-depth works of
16 commentary and expression; and to engage in commerce whether shopping online,
17 starting a business, or planning your next vacation or tonight’s dinner. In sum, today
18 the devices and the software that power them touch every aspect of our lives. For the
19 companies operating in today’s ever-connected digital world, the values of privacy,
20 security, and transparency are essential guiding principles for building trust with their
21 users. Indeed, the President focused on precisely these values in his Consumer
22 Privacy Bill of Rights. *See* Executive Office of the President, *Consumer Data*
23 *Privacy in a Networked World: A Framework for Protecting Privacy and Promoting*
24 *Innovation in the Global Digital Economy 1* (2012) (noting that “[c]onsumers have a
25 right” to “[t]ransparency” about “privacy and security practices” and the “secure and
26 responsible handling of personal data”).

27 The unprecedented scale of digital information used, stored and
28 communicated on the Internet means that “privacy,” which “has been at the heart of

1 our democracy from its inception,” is “needed[] now more than ever.” *Id* at C3.
2 And courts repeatedly have recognized that as technology advances, individuals’
3 expectations of privacy and transparency are *greater*, not lower. *See United States*
4 *v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (en banc) (“Technology has the
5 dual and conflicting capability to decrease privacy and augment the expectation of
6 privacy.”); *see also City of Ontario v. Quon*, 560 U.S. 746, 759 (2010) (“Rapid
7 changes in the dynamics of communication and information transmission are
8 evident not just in the technology itself but in what society accepts as proper
9 behavior.”). As the Ninth Circuit, sitting en banc, recognized in *Cotterman*, the
10 “uniquely sensitive nature of data on electronic devices carries with it a significant
11 expectation of privacy.” 709 F.3d at 966.

12 Similarly, technological advances have created new cybersecurity risks, from
13 hackers, identity thieves, and other criminal elements that threaten users’ personal
14 data, and the country’s information security infrastructure and national interests.
15 Companies’ protection of users’ data has become increasingly vital as more large-
16 scale, sophisticated, and coordinated threats have emerged.

17 **B. *Amici* Are Committed to Advancing These Core Values by**
18 **Employing Security Technologies to Protect User Data, Acting**
19 **Transparently, and Providing Users Control over Their Data**

20 *Amici* are committed to advancing the core values of security, privacy, and
21 transparency in the way they conduct their business and handle their users’ data.
22 They employ advanced security technology to protect users from external threats.
23 The federal government and many states have pushed the private sector to take these
24 steps, including through legislation and enforcement measures. As the FTC has
25 observed, companies that maintain user data are potential targets for hackers and
26 others, and therefore should incorporate security “into the decisionmaking in every
27 department of [their] business.” FED. TRADE COMM’N, START WITH SECURITY:
28 LESSONS LEARNED FROM FTC CASES 2 (2015).

Further, *Amici* go to great lengths to disclose to their users how their data is

1 collected and protected so those users can make informed choices. They publish
2 detailed privacy policies that inform users about security safeguards and the
3 circumstances in which their data may be shared with others. *See, e.g.*, Twitter
4 Privacy Policy, <https://twitter.com/privacy>; LinkedIn Privacy Policy,
5 www.linkedin.com/legal/privacy-policy. *Amici* design their services to give users
6 control over how their data is used, all to advance the important principles of privacy
7 and transparency.

8 Finally, *Amici* inform their users that personal data may be disclosed in certain
9 circumstances, including in response to lawful requests for user data, such as in law
10 enforcement investigations. *See, e.g.*, eBay Privacy Policy,
11 <http://pages.ebay.com/help/policies/privacy-policy.html> (noting that eBay cooperates
12 with law enforcement and government agencies in response to verified requests
13 relating to a criminal investigation or alleged or suspected illegal activity); LinkedIn
14 Privacy Policy, *supra*, ¶ 2.6 (data may be disclosed to “comply with a legal
15 requirement or process, including, but not limited to, civil and criminal subpoenas,
16 court orders or other compulsory disclosures”); Twitter Privacy Policy, *supra*
17 (similar). Several *Amici* also issue annual transparency reports, which disclose to
18 users and the broader public the number and type of government requests for user data
19 that have been made to them pursuant to lawful process.¹

20 **C. *Amici* Recognize and Respect the Government’s Important Work**
21 **Protecting Our National Security**

22 In addition to committing to the values of privacy, security, and transparency,
23 *Amici* routinely assist U.S. law enforcement in investigating crimes and threats to
24 national security. They comply with proper, reasonable requests for data pursuant to

25 ¹ *See, e.g.*, LinkedIn Transparency Report,
26 <https://www.linkedin.com/legal/transparency#government-requests>; Twitter
27 Transparency Report, <https://transparency.twitter.com/country/us>; Kickstarter
28 Transparency Report, <https://www.kickstarter.com/blog/kickstarter-transparency-report-2014>; Twilio Transparency Report,
<https://www.twilio.com/legal/transparency>.

1 valid legal process. As shown by the transparency reports of several *Amici*, they
2 have provided information in response to numerous such requests.²

3 *Amici's* assistance with these investigations is conducted pursuant to clear
4 rules, governed by applicable statutory and regulatory schemes and in accordance
5 with the Constitution. These include the statutory requirements imposed on the
6 government for obtaining a warrant or issuing a subpoena for user data in a
7 company's possession. These established rules ensure transparency, predictability,
8 and oversight. Absent such rules, there would be a serious risk that law enforcement
9 could abuse its powers to obtain users' private information. *See* Orin S. Kerr, *The*
10 *Fourth Amendment and New Technologies: Constitutional Myths and the Case for*
11 *Caution*, 102 Mich. L. Rev. 801, 859 (2004).³

12 **D. The Government's Request Has No Legal Limits and Will**
13 **Undermine Existing, Transparent Statutory Schemes that Reflect a**
14 **Balancing of Competing Policy Considerations**

15 As described in detail below (*see infra* at 14-25), the government's request in
16 this case rests not on any specific statutory authorization, but on the novel theory that
17 federal courts may use the All Writs Act to compel third parties to provide whatever
18 assistance the government deems necessary or convenient in any particular
19 investigation. In other words, the government seeks unbounded authority to compel
20 Apple to design software that does not currently exist and that will circumvent and
21 undermine security measures intended to protect its users' data. This principle could

22 ² *See, e.g.*, Twitter Transparency Report for the United States,
23 <https://transparency.twitter.com/country/us> (in second half of 2015 Twitter received
24 2,673 U.S. government requests for account information and produced information
25 in response to 79%).

26 ³ When technology is rapidly changing, it is even more important that law
27 enforcement operate pursuant to clear rules. That is because case-by-case judicial
28 tests will quickly become obsolete as "the nature of the electronic devices that
ordinary Americans carry on their persons continue to change." *Riley v. California*,
134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring); *see also* Kerr, *supra*, 102 Mich.
L. Rev. at 858-59. As the Supreme Court has observed, "[t]he judiciary risks error by
elaborating too fully" on the "implications of emerging technology before its role in
society has become clear." *Quon*, 560 U.S. at 759.

1 require companies not just to turn over one user's information but to weaken security
2 measures created to protect *all* users. Granting the government such extraordinary
3 authority, without *any* set rules or legal protections, will not only erode user privacy
4 and security and defeat users' interest in transparency, it will undermine an existing
5 legislative framework balancing competing interests and policy considerations.

6 The government's demand, at its core, is unbound by any legal limits. It
7 would set a dangerous precedent, creating a world in which the government could
8 simply force companies to create, design, and redesign their systems to allow law
9 enforcement access to data, instead of requiring the government to use the measures,
10 and meet the requirements, of legislatively enacted statutory schemes. Nor is the
11 fact that the government may claim that it does not plan to regularly exercise its far-
12 reaching authority to commandeer software engineers of any comfort⁴: the creation
13 or design of software in response to even one government order cannot be undone.
14 *See Cotterman*, 709 F.3d at 966 (observing same about "unfettered dragnet effect"
15 of warrantless border searches). Indeed, law enforcement officials already have
16 indicated that if the government prevails in this case, they would seek to access *all*
17 locked iPhones in their possession that are part of ongoing investigations.⁵

18 Likewise, the government's suggestion that steps could be taken to prevent
19

20 ⁴ Of course, it also must be emphasized that for several companies, particularly
21 smaller ones, the burden in complying with such an order could be enormous.
22 Apple itself has indicated that the burden on a company of its size would be
23 substantial; for smaller companies that can only devote a handful of engineers to
24 such a project the burden could be crippling to their ongoing operations.

25 ⁵ *See* Katie Benner & Matt Apuzzo, *Narrow Focus May Aid FBI in Apple Case*, N.Y.
26 Times (Feb. 22, 2016), http://www.nytimes.com/2016/02/23/technology/apple-unlock-iphone-san-bernardino.html?_r=0 (New York City District Attorney Cyrus Vance responding "absolutely right" when asked whether he would seek to unlock nearly 175 iPhones in New York City law enforcement's possession); The Encryption Tightrope: Balancing Americans' Security and Privacy, YOUTUBE (March 1, 2016),
27 <https://www.youtube.com/watch?v=g1GgnbN9oNw&feature=youtu.be&t=3656> (FBI Director Comey responding "sure, potentially" when asked whether this case will
28 "set a precedent" for law enforcement to seek the same assistance in other cases).

1 the disclosure of encryption-breaking software or limiting the circumstances in
2 which it may force a company to build a backdoor, is of no reassurance. As the
3 Second Circuit noted in the context of the NSA’s self-imposed limits in its
4 collection of bulk telephone metadata, the “more metadata the government collects
5 and analyzes,” the “greater the capacity for such metadata to reveal ever more
6 private and previously unascertainable information about individuals.” *ACLU v.*
7 *Clapper*, 785 F.3d 787, 794 (2d Cir. 2015). These kinds of concerns are particularly
8 pronounced for companies like *Amici*, who securely store the personal data of, and
9 handle massive volumes of Internet traffic for, over a billion users collectively.

10 Indeed, in assessing the constitutionality of warrantless GPS monitoring,
11 Justice Sotomayor observed that granting the government “unfettered discretion” to
12 obtain and use “a substantial quantum of intimate information” about citizens may
13 “alter the relationship between citizen and government in a way that is inimical to
14 democratic society.” *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor,
15 J., concurring). Giving law enforcement the unprecedented power to force
16 companies to design software to break their users’ data protections, a power that is
17 not bound by any legal or practical limit, presents precisely the same risk.

18 By contrast, in enacting existing statutory schemes governing law
19 enforcement access to user data and digital communications—including Title III, the
20 SCA, CALEA, and FISA—Congress weighed and balanced law enforcement needs
21 with user security and privacy. *See infra* at 16-20.⁶ By circumventing these
22 processes and procedures, and the balance of policy considerations they reflect, the
23 government seeks to avoid an essential public debate and do a judicial end-around
24 the legislative framework that Congress carefully crafted.

25 Courts and scholars have emphasized that the public discourse afforded by

26 _____
27 ⁶ This is not to say that *Amici* believe that the existing statutory scheme is perfect.
28 But the fact that these laws are flawed in certain areas does not mean that the All
Writs Act authorizes the broad sweeping powers suggested by the government here.

1 legislative rulemaking is essential for our society as we struggle with challenging
2 questions about how far we should go in sacrificing liberty and privacy in protecting
3 our national security. The Second Circuit affirmed the importance of robust debate
4 of these questions last year when it held that the PATRIOT Act did not authorize
5 bulk telephone metadata collection by the NSA. The court observed that while
6 “expansive development of government repositories of formerly private records” and
7 a corresponding “contraction of the privacy expectations of all Americans” could be
8 “required by national security,” “we would expect such a momentous decision to be
9 preceded by substantial debate.” *Clapper*, 785 F.3d at 818. Similarly, Justice
10 Breyer has recognized the critical importance of public debate in resolving questions
11 raised by the interplay between technology, national security, and privacy:

12 Should cell phones be encrypted? Should web technology, making
13 use of an individual’s privacy preferences, automatically negotiate
14 privacy rules with distant web sites as a condition of access? The
15 complex nature of these problems calls for resolution through a form
16 of participatory democracy. Ideally, that participatory process does
17 not involve legislators, administrators, or judges imposing law from
18 above. Rather, it involves law revision that bubbles up from below.

17 Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. Rev. 245, 263 (2002).

18 Likewise here, the government seeks an order that will “impose law from
19 above” without considering the voices of the ordinary citizenry whose lives would
20 be deeply affected by such relief.

21 **E. Forcing Technology Companies to Break Their Own Security**
22 **Measures Will Undermine User Confidence that Their Data Is**
23 **Secure and Being Handled Transparently**

24 If the government is able to compel companies to break their own security
25 measures, the users of those companies will necessarily lose confidence that their
26 data is being handled in a secure, open manner. The very security measures on which
27 they have relied will have been compromised—and security “work arounds” created
28 —by court order. Technological backdoors, whether or not built for specific and
29 supposedly limited purposes, create an opportunity for criminals and hackers to

1 exploit. As security experts have observed, history has shown that no company can
2 “build an access system that only works for people of a certain citizenship, or with a
3 particular morality, or only in the presence of a specified legal document This is
4 not theoretical; again and again, backdoor accesses built for one purpose have been
5 surreptitiously used for another.” Bruce Schneier, *Security or Surveillance?* (2016),
6 https://www.schneier.com/essays/archives/2016/02/security_vs_surveill.html;
7 Berkman Ctr. for Internet & Soc’y, *Don’t Panic: Making Progress on the “Going*
8 *Dark” Debate*, Appendix A to Landau (2016), [https://cyber.law.harvard.edu/](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf)
9 [pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf)
10 (noting, e.g., that “Vodafone built backdoor access into Greece’s cell phone network
11 for the Greek government; it was used against the Greek government in 2004-2005”).
12 Moreover, forcing a company to undermine its own security measures provides a
13 powerful disincentive to invest in security: firms could have no confidence that their
14 carefully designed security systems would not be redesigned by court order.

15 In short, in addition to reducing the security of data and users’ privacy, the
16 government’s demand here will force companies to violate existing representations to
17 their users regarding access to, and the security of, their data, and will undermine
18 their ability to make such assurances in the future. Similarly, the government could
19 require companies to break other aspects of their agreements with users—by
20 collecting more information than disclosed, sharing the data in undisclosed or
21 unintended ways, or even surreptitiously forcing users to download code mandated
22 by the government to weaken the privacy and safety protections promised to users.
23 This would thwart users’ legitimate expectations of privacy and security in their own
24 information.⁷ According to a recent Pew Report, 93% of Americans say that being in
25

26 ⁷ Indeed, the FTC has prosecuted companies it alleges used information in ways
27 contrary to explicit promises in a privacy policy. *E.g.*, Press Release, Fed. Trade
28 Comm’n, Gateway Learning Settles Privacy Charges (Jul. 7. 2004) (“You can change
the rules but not after the game has been played.”).

1 control of who can get information about them is important.⁸ And if the government
2 can force companies to break promises on issues as critical as data security and
3 privacy, it may similarly “undo” other promises made to consumers to protect their
4 privacy or other civil liberties, further eroding trust and confidence in their services.⁹

5 **IV. THE GOVERNMENT LACKS THE AUTHORITY UNDER THE ALL**
6 **WRITS ACT TO FORCE A PRIVATE PARTY TO RE-WRITE ITS**
7 **SOFTWARE CODE AND SERVE AS AN INVESTIGATIVE ARM OF**
8 **LAW ENFORCEMENT**

9 As noted, Congress has enacted a number of statutes—including Title III, the
10 SCA, CALEA, and FISA—that together comprehensively regulate the government’s
11 ability to acquire electronic communications and data, including from third-party
12 companies. In enacting these laws, Congress balanced competing law-enforcement
13 needs with user security and privacy, and ultimately chose *not* to give the
14 government the very authority that it seeks here.

15 The All Writs Act is a procedural gap-filling measure designed to allow
16 federal courts to effectuate powers they already have, not a broad independent grant
17 of substantive power to federal courts. It cannot be used to circumvent the
18 limitations established through the legislative process and the vital public debate
19 accompanying it. And indeed, courts repeatedly have rejected similar efforts by the
20 government to require third parties to provide forms of assistance not contemplated
21 by statute. The Act does not grant the government the power Congress chose not to
22 provide: the ability to require Apple to affirmatively rewrite its software code and
23 undermine its own security systems to unlock a phone.

24 The cases cited by the government in its Motion to Compel do not support its

25 ⁸ Pew Research Center, *Americans’ Attitudes About Privacy, Security and*
26 *Surveillance* (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

27 ⁹ In fact, this potential erosion of consumer trust puts undermines the entire Internet
28 and technology industry, which has been a source of dynamic innovation and job
creation in the U.S. economy. The critical foundation of that economic success has
been the trust and confidence that consumers have placed in the sector.

1 case. They involve either an order (1) to turn over existing documents or data, or
2 (2) to provide nonburdensome technical assistance to the government of a sort that
3 already had been endorsed by Congress (e.g., pen registers and wiretaps) and that
4 the third party already routinely performed outside the investigative context as part
5 of its regular course of business. In none of these cases has a third party been
6 compelled to take affirmative steps to create anything, much less sophisticated
7 software designed to undermine its own security systems.

8 **A. The All Writs Act Is a Gap-Filling Measure, Not a Broad**
9 **Independent Grant of Substantive Power to Federal Courts**

10 The All Writs Act permits federal courts to “issue all writs necessary or
11 appropriate in aid of their respective jurisdictions and agreeable to the usages and
12 principles of law.” 28 U.S.C. § 1651. The first Congress enacted the statute as part
13 of the Judiciary Act of 1789, not to serve as a “grant of plenary power to the federal
14 courts,” *Jackson v. Vasquez*, 1 F.3d 885, 889 (9th Cir. 1993), but rather as a
15 “legislatively approved source of procedural instruments” designed to allow newly
16 created federal courts to issue the writs necessary for them to perform the functions
17 authorized by other laws. *Harris v. Nelson*, 394 U.S. 286, 299 (1969). In keeping
18 with that original understanding, the Supreme Court’s “view of the scope of the all
19 writs provision” consistently has “confined it to filling the interstices of federal
20 judicial power when those gaps threatened to thwart the otherwise proper exercise of
21 federal courts jurisdiction.” *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S.
22 34, 41 (1985) (citing *McClung v. Silliman*, 19 U.S. (6 Wheat.) 598 (1821)).

23 The Supreme Court thus repeatedly has rebuffed efforts by litigants to use the
24 All Writs Act in a manner that would circumvent or supplant other laws. “The All
25 Writs Act is a residual source of authority to issue writs that are not otherwise
26 covered by statute. Where a statute specifically addresses the particular issue at hand,
27 it is that authority, and not the All Writs Act, that is controlling.” *Pa. Bureau of*
28 *Corr.*, 474 U.S. at 43. The Act “does not authorize” federal courts “to issue ad hoc

1 writs whenever compliance with statutory procedures appears inconvenient or less
 2 appropriate.” *Id.* That is true *even where* the relevant statute does not expressly say
 3 that it provides the exclusive means by which a court may order the performance of
 4 the act at issue.

5 In *Pennsylvania Bureau of Corrections*, for instance, the Supreme Court held
 6 that the Act could not support a federal district court’s order to the U.S. Marshals
 7 Service to transport potential witnesses in the custody of state corrections officials to
 8 federal court to testify in a pending § 1983 action. 474 U.S. at 43. Although no
 9 statute affirmatively said that the Marshals Service *did not* have such a duty, the
 10 Court reasoned that the federal habeas statutes, 28 U.S.C. §§ 2241, 2243, spoke to
 11 the issue of transportation of prisoners to court but provided “no basis . . . for a
 12 federal court to order the Marshals to transport state prisoners to the federal
 13 courthouse.” 474 U.S. at 39. The Court concluded that the lack of specific statutory
 14 authority precluded the use of the All Writs Act to achieve that end.

15 Similarly, in *Carlisle v. United States*, 517 U.S. 416 (1996), the Supreme Court
 16 held that the All Writs Act could not support a district court’s entry of a judgment of
 17 acquittal outside the time limit prescribed by Federal Rule of Criminal Procedure 29.
 18 *Id.* at 429. The Court had no difficulty concluding that Rule 29 “provide[d] the
 19 applicable law” and thus precluded the use of the All Writs Act to support entry of the
 20 judgment of acquittal, even though Rule 29 by its terms did not expressly say so. *Id.*¹⁰

21 **B. Congress Has Enacted Several Statutes that Together Provide a**
 22 **Comprehensive Regulatory Regime Allowing the Government in**
 23 **Certain Circumstances to Obtain Assistance from Third Parties in**
 24 **the Course of Investigations, Displacing the All Writs Act**

25 Here, Congress has left no procedural gaps for the All Writs Act to fill.
 26 Congress has enacted a number of statutes that create a comprehensive scheme

26 ¹⁰ See also, e.g., *Syngenta Crop Protection, Inc. v. Henson*, 537 U.S. 28, 32-33
 27 (2002) (“[p]etitioners may not, by resorting to the All Writs Act, avoid complying
 28 with the statutory requirements for removal”); *U.S. Alkali Export Ass’n v. United*
States, 325 U.S. 196, 203 (1945) (writ of certiorari under All Writs Act could not
 serve as substitute for ordinary appeal authorized by statute).

1 regulating the government's ability to acquire electronic communications and data,
2 including from third-party companies. In passing these statutes, Congress considered
3 the relief the government requests in this action, but chose not to grant it. The All
4 Writs Act may not be used to circumvent the requirements and limitations these
5 statutes place on the government's ability to compel assistance in its investigations.

6 **1. Congress's Decision to Prohibit Limits on Encryption and to**
7 **Exclude Information Service Providers in CALEA Evidences**
8 **Its Intent to Deny the Relief Sought by the Government**

9 Of the statutes compelling third party assistance in law enforcement
10 investigations—Title III, the SCA, FISA, and CALEA—only one (CALEA)
11 mandates specific system-design requirements by third parties. These requirements
12 generally obligate telecommunications carriers to design their systems in such a way
13 as to facilitate the government's interception of real-time communications. *See* 47
14 U.S.C. § 1002(a)(1)-(4). Congress considered, and expressly declined to provide,
15 the very authority the government seeks in this action.

16 First, even for telecommunications carriers covered by CALEA—which Apple
17 and *Amici* are not—Congress denied law enforcement the right to dictate what
18 security protocols, equipment, or operating standards should be employed. *See* 47
19 U.S.C. § 1002(b)(1). The House Report noted that this was “the exact opposite of the
20 original versions of the legislation, which would have barred introduction of services
21 or features that could not be tapped.” H.R. Rep. No. 103-827(I), at 19. This covered
22 encryption:

23 Nothing in this paragraph would prohibit a carrier from deploying an
24 encryption service for which *it does not retain the ability to decrypt*
25 *communications for law enforcement access*. The bill does not address
26 the “Clipper Chip”^[11] or Key Escrow Encryption issue. Nothing in the

26 ¹¹ The reference to the “Clipper Chip” was a 1994 proposal by the National Security
27 Agency that involved installing a chip in cell phones that would allow the
28 government to decrypt and intercept communications at will using a key escrow
system. *See* Steven Levy, *Battle of the Clipper Chip*, N.Y. Times (June 12, 1994),
<http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>.

1 bill is intended to limit or otherwise prevent the use of any type of
2 encryption within the United States. Nor does the Committee intend this
3 bill to be in any way a precursor to any kind of ban or limitation on
4 encryption technology. To the contrary, section 2602 protects the right to
5 use encryption.

6 *Id.* at 24 (emphasis added). In other words, even within the highly regulated space of
7 telecommunications carriers covered under CALEA, Congress protected the ability of
8 companies to design their own technological systems. Under CALEA, a telephone
9 company that encrypts its communications has *no* obligation to redesign its system so
10 that law enforcement officers can make sense of intercepted transmissions.

11 Furthermore, as the text of CALEA makes plain (*see* 47 U.S.C.
12 § 1002(b)(2)), in passing the statute Congress specifically chose *not* to impose any
13 of these same system-design requirements on other entities, and in particular,
14 information service providers (*id.* § 1001(6)), which encompass companies like
15 Apple and several *Amici*. *See also* H.R. Rep. No. 103-827(I), at 18 (1994). That
16 choice was deliberate. Congress considered and rejected proposed versions of
17 CALEA that would have imposed such requirements:

18 [P]rivate network systems or information services can be wiretapped
19 pursuant to court order, and their owners must cooperate when presented
20 with a wiretap order, but these services and systems *do not have to be*
21 *designed so as to comply with the capability requirements*. Only
22 telecommunications carriers, as defined in the bill, are required to design
23 and build their switching and transmission systems to comply with the
24 legislated requirements. *Earlier digital telephony proposals covered all*
25 *providers of electronic communications services, which meant every*
26 *business and institution in the country. That broad approach was not*
27 *practical. Nor was it justified to meet any law enforcement need.*

28 *Id.* (emphases added). This decision was motivated not only by practicality but also
the significant privacy concerns at stake. The House Report observed that because
“society’s patterns of using electronic communications technology have changed
dramatically” between the enactments of the SCA in 1986 and that of CALEA in
1994, stored electronic data “reveals a great deal about [individuals’] private lives,

1 all of it compiled in one place.” *Id.* at 17. The fact that, eight years after imposing
2 disclosure requirements on certain information service providers under the SCA, *all*
3 information service providers were excluded from CALEA’s scope is compelling
4 evidence that Congress did not intend to allow the relief sought here. *See In re*
5 *Apple, Inc.*, ___ F. Supp. 3d ___, 2016 WL 783565, at *10-11 (E.D.N.Y. Feb. 29,
6 2016). Indeed, in the years since CALEA was enacted, Congress has considered—
7 and rejected—additional proposals to give the government the authority it now
8 seeks to give itself via the All Writs Act. *See, e.g.*, Rep. Peter T. King,
9 *Remembering the Lessons of 9/11*, 41 J. LEGIS. 173, 178 (2014-2015); *In re Apple,*
10 *Inc.*, 2015 WL 5920207, at *3 (E.D.N.Y. Oct. 9, 2015).

11 The government does not contend that Apple has any obligation under
12 CALEA to redesign its operating system. Indeed, it has not sought the remedies
13 available under the statute, such as an order for non-compliance. Instead, it asks this
14 Court to do exactly what Congress refused to do. But the Act cannot be invoked to
15 grant the government powers Congress intentionally chose not to provide it.

16 **2. Congress Has Placed Significant Limits on Law**
17 **Enforcement’s Ability to Compel Technical Assistance from**
18 **Third Parties**

19 Title III, the SCA, CALEA, and FISA all require certain providers of wire and
20 electronic communications to offer technical assistance to law enforcement in certain
21 circumstances. Such assistance includes interception of real-time communications,
22 installation of pen registers and trap-and-trace devices, disclosure of stored
23 communications, and investigations seeking “foreign intelligence information.” *See*
24 18 U.S.C. §§ 2518(4), 2703(a)-(b), 3124(a)-(b); 47 U.S.C. § 1002(a)(4); 50
25 U.S.C. §§ 1802(a)(4)(A), 1822(a)(4)(a), 1842(d)(2)(B), 1861(c), 1881a(h)(1),
26 1881b(c)(5). Yet, as the government recognizes, none of these intricate statutes
27 grants the powers the government seeks to arrogate to itself here.

28 Congress did *not* intend to give the government a blank check to compel law
enforcement assistance from third parties—the precise consequence of the

1 government's interpretation of the All Writs Act. Indeed, in enacting the SCA,
2 Congress recognized that consumers have a "reasonable expectation" that third party
3 providers "will not become, in effect, a branch of Government law enforcement." S.
4 Rep. No. 99-541, at 29 (1986). Any technical assistance requested pursuant to
5 CALEA, Title III, or FISA must be provided with minimal interference to the services
6 promised to customers. 18 U.S.C. § 2518(4); 47 U.S.C. § 1002(a)(4); 50 U.S.C.
7 §§ 1802(a)(4)(A), 1805(c)(2)(B), 1822(a)(4)(A)(i), 1824(c)(2)(B), 1842(d)(2)(B)(i),
8 1881a(h)(1)(A), 1881b(c)(5)(B). For example, the Ninth Circuit has held that an
9 eavesdropping request that, effectively, prohibited a vehicle monitoring system
10 company from supplying "any of the various services it had promised its customer"
11 violated 18 U.S.C. § 2518(4). *In re Application of U.S. for an Order Authorizing the*
12 *Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1145-46 (9th Cir. 2003).

13 The government's effort to force Apple to redesign its operating system to
14 facilitate surveillance runs afoul of these principles, which require a consideration
15 not merely of the technical burden on the company, but also on users. The
16 government's request would set a precedent that could be used in future cases to
17 require *Amici* or others to provide technical assistance in a manner that undermines
18 the very products they offer. At the very least, once Apple has written code to
19 comply with the order, the government may seek orders to compel it to use such
20 code over and over again. Congress has chosen not to give the government that
21 authority, and the All Writs Act cannot be used to circumvent that limitation.

22 **C. Courts Have Rejected Similar Efforts Under the All Writs Act to**
23 **Compel Forms of Assistance that Are Not Contemplated by Statute**

24 In keeping with the Act's role as a gap-filling measure rather than a broad
25 substantive grant of power, courts repeatedly have rejected efforts by the
26 government to require third parties to provide forms of novel technical assistance
27 not contemplated by statute. Under this authority, the All Writs Act cannot support
28 the government's request for an order to a company to rewrite its software code to

1 suit the government's preferences absent any statutory basis for that request.

2 The Ninth Circuit's decision in *Plum Creek Lumber Co. v. Hutton*, 608 F.2d
3 1283 (9th Cir. 1979), illustrates the point. In *Plum Creek*, the Occupational Safety
4 and Health Administration (OSHA) was trying to compel a lumber company's
5 affirmative assistance in investigating whether environmental standards were being
6 met by the company, and sought an order under the All Writs Act requiring the
7 company to force its employees to wear certain environmental testing devices while
8 on the job. *Id.* at 1285. Evidence showed that the devices were the most efficient
9 method of measuring air quality and noise level, and while OSHA "could not
10 guarantee that the testing devices would not cause any accidents," the risk of any
11 harm resulting from their being worn was "minimal." *Id.* at 1286. The district court
12 and Ninth Circuit nonetheless rejected OSHA's effort, and in particular concluded
13 that the All Writs Act did not support the issuance of such an order. *Id.* at 1289-90.

14 The Ninth Circuit reasoned that the All Writs Act "permits the district court,
15 in aid of a valid warrant, to order a third party to provide nonburdensome technical
16 assistance to law enforcement officers. It does not give the district court a roving
17 commission to order a party subject to an investigation to accept additional risks at
18 the bidding of OSHA inspectors." *Id.* at 1289. Even if the testing devices were the
19 most efficient monitoring method, "in the absence of law specifying their use," the
20 All Writs Act could not be used to "order Plum Creek to bear the added risks the
21 devices would bring." *Id.* *Plum Creek* forecloses the government's request that this
22 Court "usurp the legislative function," *id.* at 1290, and use a procedural gap-filling
23 statute to require Apple to re-write its own software code and create potentially
24 catastrophic risks to the security of users' Apple devices.

25 *Plum Creek's* holding finds support in more recent case law in which district
26 courts have refused to allow the government to use the All Writs Act to require third
27 parties to provide novel forms of assistance not contemplated by statute. In *In re*
28 *Application of U.S.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005), the court held that the

1 All Writs Act could not support an order requiring a wireless provider to
2 prospectively monitor and disclose to the government a suspect's location based on
3 cell-tower data. The court concluded that this would be an "entirely unprecedented"
4 use of the All Writs Act, and observed that Congress had spoken to the issue in Title
5 III and the SCA, yet had not required companies to provide the type of assistance
6 the government sought. *Id.* at 326. The court refused to "read into the All Writs Act
7 an empowerment of the judiciary to grant the executive branch authority to use
8 investigative techniques either explicitly denied it by the legislative branch, or at a
9 minimum omitted from a far-reaching and detailed statutory scheme." *Id.*

10 Likewise, in *In re Application of U.S.*, 849 F. Supp. 2d 526 (D. Md. 2011), the
11 court rejected a similar effort by the government to use the All Writs Act to require a
12 wireless provider to turn over real-time cell-tower location data pertaining to a
13 particular suspect. The court concluded that existing statutory authority (namely the
14 SCA) did not provide for this type of assistance, *id.* at 574-75, and that the Act could
15 not be used to circumvent that detailed statutory scheme, *id.* at 582.

16 Indeed, in *In re Apple*, in a thorough analysis of the specific issue presented
17 here, the district court declined to approve the government's request for an order
18 commanding Apple to help unlock an iPhone. The court noted that Congress had
19 opted not to give the government the specific authority it sought (2015 WL
20 5920207, at *1-3, 5), that it was "entirely possible, if not likely" that Apple had a
21 "substantial interest" in not providing the assistance sought (*id.* at *5), and that the
22 All Writs Act case law did not support the government's approach (*id.* at *7). The
23 court reaffirmed and expanded upon these conclusions in a recent order, noting that
24 the Act could not be used to compel Apple's assistance because the "legislative
25 scheme" designed by Congress was "so comprehensive as to imply a prohibition
26 against imposing requirements on private entities" that Congress had not
27 "affirmatively prescribe[d]." *Apple*, 2016 WL 783565, at *9. This Court should
28 adopt similar reasoning.

1 **D. The Cases upon Which the Government Relies Do Not Support**
2 **Forcing a Private Party to Create New Technology to Assist the**
3 **Government's Investigation**

4 The cases cited by the government in its Motion to Compel, as well as other
5 cases in which courts have relied upon the All Writs Act to order private parties to
6 assist government investigations, have not required a third party to take affirmative
7 steps to create anything, much less to reengineer sophisticated software. These
8 cases do not support what the government seeks to do here.

9 *First*, courts have used the All Writs Act to order third parties to turn over
10 existing documents or data to the government to aid an investigation, in the same way
11 as third parties routinely are required by subpoena to turn over documents or data
12 discoverable in civil litigation. *See, e.g., United States v. Hall*, 583 F. Supp. 717, 722
13 (E.D. Va. 1984) (ordering a credit card company to produce credit card records kept
14 in the ordinary course of business); *In re Application of U.S. for an Order Directing*
15 *X to Provide Access to Videotapes*, 2003 WL 22053105, at *3 (D. Md. Aug. 22,
16 2003) (directing apartment complex operator “merely to provide access to
17 surveillance tapes already in existence, rather than any substantive assistance, and
18 nothing more”); *United States v. Doe*, 537 F. Supp. 838, 839-40 (E.D.N.Y. 1982)
19 (directing telephone company to provide stored records of phone numbers dialed by
20 suspect). These courts have emphasized the absence of any conceivable “adverse
21 [e]ffect” on the third party associated with producing the records at issue. *Hall*, 583
22 F. Supp. at 719, 721 (noting that the “interest of the third party, Citibank, is not going
23 to be affected by its compliance with this order, unless one argues that persons will
24 not apply for Master Cards because those credit card records may be used by federal
25 investigatory agencies”); *Videotapes*, 2003 WL 22053105, at *3 (noting that “[n]o
26 costs will be incurred” in turning over videotapes, which “are readily available”).

27 *Second*, courts have occasionally used the All Writs Act to order third parties
28 to “provide nonburdensome technical assistance to law enforcement officers.” *Plum*
Creek, 608 F.2d at 1289. These cases—all of which involve telephone companies,

1 not hardware manufacturers, software developers, or other technology firms—do
2 not support the government’s attempt to invoke the All Writs Act in this case. In
3 these cases, the assistance sought by the government was minor, amounting to no
4 more than helping carry out a scaled-down version of a surveillance function already
5 approved by Congress and that the company itself already performed in the regular
6 course of its business. In none of the cases did the assistance sought entail any
7 conceivable burden on the third party.

8 The government relies primarily on *United States v. New York Telephone Co.*,
9 434 U.S. 159 (1977). But that decision is a world removed from the circumstances
10 in this case. There, the Supreme Court concluded that the Act could support an
11 order to a telephone provider to assist with a pen register—i.e., to give the
12 government a list of phone numbers dialed by a particular suspect. *Id.* at 174-78.
13 But the Court went to great lengths to emphasize the limits of its holding. It noted
14 that the “meager assistance” the government sought would not be “in any way
15 burdensome” to the company, required only “minimal effort on the part of the
16 Company,” and entailed “no disruption to its operations.” *Id.* at 174-75. Indeed, the
17 company “concede[d] that it regularly employ[ed]” pen registers in the ordinary
18 course of business “for the purposes of checking billing operations, detecting fraud,
19 and preventing violations of law.” *Id.* The Court also noted that the company was
20 “a highly regulated public utility with a duty to serve the public,” and could not
21 claim to have a “substantial interest in not providing assistance.” *Id.* at 174.

22 The *New York Telephone* Court also emphasized that the use of the All Writs
23 Act to compel assistance with a pen register aligned with congressional intent.
24 Through Title III, Congress “clearly intended to permit the use of pen registers by
25 federal law enforcement officials.” 434 U.S. at 176; *see also id.* at 165-68. Courts
26 have recognized that as a “critical[] differen[ce]” between *New York Telephone* and
27 cases, like this one, in which such congressional authorization is lacking. *In re*
28 *Application of U.S.*, 849 F. Supp. 2d at 579.

1 Multiple other cases (several of which the government cites) are in the same
2 vein: they approve the use of the All Writs Act to require the installation of pen
3 registers or other similar surveillance devices already approved by Congress and
4 routinely used by telephone companies in the ordinary course of business and for
5 their own business purposes. *See, e.g., In re Application of U.S. for an Order*
6 *Authorizing an In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d
7 1122, 1129-30 (9th Cir. 1980) (approving use of All Writs Act to require phone
8 company to assist with tracing numbers dialed from suspects' phones); *Application*
9 *of U.S. for an Order Authorizing Installation of Pen Register*, 610 F.2d 1148, 1154
10 (3d Cir. 1979) (relying on *New York Telephone* in pen register case); *United States*
11 *v. Mosko*, 654 F. Supp. 402 (D. Colo. 1987) (same); *In re Application of U.S. for an*
12 *Order Directing a Provider of Commc'ns Servs. to Provide Tech. Assistance*, ___ F.
13 Supp. 3d ___, 2015 WL 5233551 (D.P.R. Aug. 27, 2015) (phone company's
14 assistance in consensual monitoring of electronic communication).

15 In only one (unreported) case has a court even *suggested* that the All Writs
16 Act might appropriately be used as the government seeks here. *See In re XXX, Inc.*,
17 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014). But, as explained by Apple (*see*
18 *Motion to Vacate* [ECF No. 16] at 28), that opinion was issued without adversarial
19 briefing, failed properly to analyze *New York Telephone*, misunderstood the type of
20 technical assistance sought by the government, and by its own admission never
21 considered the burden or adverse effect on the third-party company. Its reasoning,
22 moreover, was comprehensively addressed and refuted by the district court in *In re*
23 *Apple*, 2015 WL 5920207, at *4-7, which explains why *New York Telephone* and the
24 other All Writs Act case law cannot support the government's approach here. *See*
25 *also Apple*, 2016 WL 783565, at *17-27.

26 V. CONCLUSION

27 For the foregoing reasons, *Amici* respectfully urge the Court to deny the
28 government's Motion to Compel and to grant Apple's Motion to Vacate.

1 DATED: March 3, 2016

Respectfully submitted,

2
3 MUNGER, TOLLES & OLSON LLP

4
5
6 By: 
7 JONATHAN H. BLAVIN

8 Attorneys for *Amici Curiae*

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ORIGINAL

LODGED



1 JEROME C. ROTH (State Bar No. 159483)
 jerome.roth@mto.com
 2 ROSEMARIE T. RING (State Bar No. 220769)
 rose.ring@mto.com
 3 JONATHAN H. BLAVIN (State Bar No. 230269)
 jonathan.blavin@mto.com
 4 JOSHUA PATASHNIK (State Bar No. 295120)
 josh.patashnik@mto.com
 5 MUNGER, TOLLES & OLSON LLP
 560 Mission Street
 6 Twenty-Seventh Floor
 San Francisco, California 94105-2907
 7 Telephone: (415) 512-4000
 Facsimile: (415) 512-4077

9 ARIEL C. GREEN (State Bar No. 304780)
 ariel.green@mto.com
 10 MUNGER, TOLLES & OLSON LLP
 355 South Grand Avenue
 11 Thirty-Fifth Floor
 Los Angeles, California 90071-1560
 12 Telephone: (213) 683-9100
 Facsimile: (213) 687-7302

Attorneys for *Amici Curiae*

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

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

Case No. ED CM 10-16-SP
**CORPORATE DISCLOSURE
 STATEMENT OF *AMICI CURIAE*
 AIRBNB, INC.; ATLISSIAN PTY.
 LTD.; AUTOMATTIC INC.;
 CLOUDFLARE, INC.; EBAY INC.;
 GITHUB, INC.; KICKSTARTER,
 PBC; LINKEDIN CORPORATION;
 MAPBOX INC.; A MEDIUM
 CORPORATION; MEETUP, INC.;
 REDDIT, INC.; SQUARE, INC.;
 SQUARESPACE, INC.; TWILIO
 INC.; TWITTER, INC.; AND
 WICKR INC.**

Judge: Hon. Sheri Pym

1 **CORPORATE DISCLOSURE STATEMENT OF *AMICI CURIAE***

2 Counsel to *Amici Curiae* are aware of no rule obligating *Amici Curiae* to file
3 a corporate disclosure statement or statement of interested parties of the nature
4 contemplated by Rule 7.1 of the Federal Rules of Civil Procedure and Civil Local
5 Rule 7.1-1 of the United States District Court for the Central District of California.
6 In an abundance of caution, however, *Amici Curiae* Airbnb, Inc. (“Airbnb”);
7 Automattic Inc. (“Automattic”); Atlassian Pty. Ltd. (“Atlassian”); CloudFlare, Inc.
8 (“CloudFlare”); eBay Inc. (“eBay”); GitHub, Inc. (“GitHub”); Kickstarter, PBC
9 (“Kickstarter”); LinkedIn Corporation (“LinkedIn”); Mapbox Inc. (“Mapbox”);
10 Medium Corporation (“Medium”); Meetup, Inc. (“Meetup”); Reddit, Inc.
11 (“Reddit”); Square, Inc. (“Square”); Squarespace, Inc. (“Squarespace”); Twilio Inc.
12 (“Twilio”); Twitter, Inc. (“Twitter”); and Wickr Inc. (“Wickr”) hereby file this
13 corporate disclosure statement.

14 Airbnb states that it has no parent corporation and that no publicly held
15 corporation owns more than 10% of Airbnb’s stock.

16 Atlassian states that its ultimate parent corporation is Atlassian Corporation
17 Plc and that no publicly held corporation owns more than 10% of the stock of
18 Atlassian Corporation Plc.

19 Automattic states that it has no parent corporation and that no publicly held
20 corporation owns more than 10% of Automattic’s stock.

21 CloudFlare states that it has no parent corporation and that no publicly held
22 corporation owns more than 10% of CloudFlare’s stock.

23 eBay states that it has no parent corporation and that no publicly held
24 corporation owns more than 10% of eBay’s stock.

25 GitHub states that it has no parent corporation and that no publicly held
26 corporation owns more than 10% of GitHub’s stock.

27 Kickstarter states that it has no parent corporation and that no publicly held
28 corporation owns more than 10% of Kickstarter’s stock.

1 LinkedIn states that it has no parent corporation and that no publicly held
2 corporation owns more than 10% of LinkedIn's stock.

3 Mapbox states that it has no parent corporation and that no publicly held
4 corporation owns more than 10% of Mapbox's stock.

5 Medium states that it has no parent corporation and that no publicly held
6 corporation owns more than 10% of Medium's stock.

7 Meetup states that it has no parent corporation and that no publicly held
8 corporation owns more than 10% of Meetup's stock.

9 Reddit states that it has no parent corporation and that no publicly held
10 corporation owns more than 10% of Reddit's stock.

11 Square states that it has no parent corporation and that no publicly held
12 corporation owns more than 10% of Square's stock.

13 Squarespace states that it has no parent corporation and that no publicly held
14 corporation owns more than 10% of Squarespace's stock.

15 Twilio states that it has no parent corporation and that no publicly held
16 corporation owns more than 10% of Twilio's stock.

17 Twitter states that it has no parent corporation and that no publicly held
18 corporation owns more than 10% of Twitter's stock.

19 Wickr states that it has no parent corporation and that no publicly held
20 corporation owns more than 10% of Wickr's stock.

21

22

23

24

25

26

27

28

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

DATED: March 3, 2016

Respectfully submitted,

MUNGER, TOLLES & OLSON LLP

By: 
JONATHAN H. BLAVIN

Attorneys for *Amici Curiae*

LOGGED

ORIGINAL

1 JEROME C. ROTH (State Bar No. 159483)
 jerome.roth@mto.com
 2 ROSEMARIE T. RING (State Bar No. 220769)
 rose.ring@mto.com
 3 JONATHAN H. BLAVIN (State Bar No. 230269)
 jonathan.blavin@mto.com
 4 JOSHUA PATASHNIK (State Bar No. 295120)
 josh.patashnik@mto.com
 5 MUNGER, TOLLES & OLSON LLP
 560 Mission Street
 6 Twenty-Seventh Floor
 San Francisco, California 94105-2907
 7 Telephone: (415) 512-4000
 Facsimile: (415) 512-4077
 8

2016 MAR -3 AM 11:54
 CLERK U.S. DISTRICT COURT
 CENTRAL DISTRICT OF CALIF.
 RIVERSIDE
 BY

FILED
 CLERK, U.S. DISTRICT COURT
 MAR -3 2016
 CENTRAL DISTRICT OF CALIFORNIA
 EASTERN DIVISION BY DEPUTY

9 ARIEL C. GREEN (State Bar No. 304780)
 ariel.green@mto.com
 10 MUNGER, TOLLES & OLSON LLP
 355 South Grand Avenue
 11 Thirty-Fifth Floor
 Los Angeles, California 90071-1560
 12 Telephone: (213) 683-9100
 Facsimile: (213) 687-7302
 13

Attorneys for *Amici Curiae*

14
 15 UNITED STATES DISTRICT COURT
 16 CENTRAL DISTRICT OF CALIFORNIA
 17 EASTERN DIVISION
 18

19 IN THE MATTER OF THE SEARCH
 OF AN APPLE IPHONE SEIZED
 20 DURING THE EXECUTION OF A
 SEARCH WARRANT ON A BLACK
 21 LEXUS IS300, CALIFORNIA
 LICENSE PLATE 35KGD203
 22

Case No. ED CM 16-10-SP
**PROOF OF SERVICE RE MOTION
 OF AIRBNB, INC.; ATLISSIAN
 PTY. LTD.; AUTOMATTIC INC.;
 CLOUDFLARE, INC.; EBAY INC.;
 GITHUB, INC.; KICKSTARTER,
 PBC; LINKEDIN CORPORATION;
 MAPBOX INC.; A MEDIUM
 CORPORATION; MEETUP, INC.;
 REDDIT, INC.; SQUARE, INC.;
 SQUARESPACE, INC.; TWILIO
 INC.; TWITTER, INC.; AND
 WICKR INC. FOR LEAVE TO
 FILE BRIEF AS *AMICI CURIAE***

Judge: Hon. Sheri Pym

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

PROOF OF SERVICE

I, the undersigned, declare that I am a citizen of the United States; my business address is 355 S. Grand Ave, Floor 35, Los Angeles, California 90071; I am employed in the City and County of Los Angeles; and I am over the age of eighteen (18) years and not a party to the within action.

On March 3, 2016, I served the foregoing documents described as:

- **Notice of Manual Filing or Lodging;**
- **Motion of Airbnb, Inc., Atlassian Pty. Ltd., Automattic Inc., CloudFlare, Inc., eBay Inc.; GitHub, Inc.; Kickstarter, PBC, LinkedIn Corporation, Mapbox Inc., A Medium Corporation, Meetup, Inc., Reddit, Inc., Square, Inc., Squarespace, Inc., Twilio Inc., Twitter, Inc., and Wickr Inc. for Leave to File Brief as *Amici Curiae*;**
- **Proposed Order Granting Motion of Airbnb, Inc., Atlassian Pty. Ltd., Automattic Inc., CloudFlare, Inc., eBay Inc.; GitHub, Inc.; Kickstarter, PBC, LinkedIn Corporation, Mapbox Inc., A Medium Corporation, Meetup, Inc., Reddit, Inc., Square, Inc., Squarespace, Inc., Twilio Inc., Twitter, Inc., and Wickr for Leave to File Brief as *Amici Curiae*;**
- **Declaration of Jonathan H. Blavin in Support of the Motion of Airbnb, Inc., Atlassian Pty. Ltd., Automattic Inc., CloudFlare, Inc., eBay Inc.; GitHub, Inc.; Kickstarter, PBC, LinkedIn Corporation, Mapbox Inc., A Medium Corporation, Meetup, Inc., Reddit, Inc., Square, Inc., Squarespace, Inc., Twilio Inc., Twitter, Inc., and Wickr for Leave to File Brief as *Amici Curiae*;**
- **Corporate Disclosure Statement of *Amici Curiae* Airbnb, Inc., Atlassian Pty. Ltd., Automattic Inc., CloudFlare, Inc., eBay Inc.; GitHub, Inc.; Kickstarter, PBC, LinkedIn Corporation, Mapbox Inc.,**

1 **A Medium Corporation, Meetup, Inc., Reddit, Inc., Square, Inc.,**
2 **Squarespace, Inc., Twilio Inc., Twitter, Inc., and Wickr; and**
3 ▪ **Brief of *Amici Curiae* Airbnb, Inc., Atlassian Pty. Ltd., Automattic**
4 **Inc., CloudFlare, Inc., eBay Inc.; GitHub, Inc.; Kickstarter, PBC,**
5 **LinkedIn Corporation, Mapbox Inc., A Medium Corporation,**
6 **Meetup, Inc., Reddit, Inc., Square, Inc., Squarespace, Inc., Twilio Inc.,**
7 **Twitter, Inc., and Wickr**

8 on the interested parties in this action by placing true copies thereof enclosed
9 in sealed envelopes addressed as follows:

10 **Eric David Vandevelde**
11 **Theodore J Boutrous, Jr**
12 Gibson Dunn and Crutcher LLP
13 333 South Grand Avenue
14 Los Angeles, CA 90071

Allen W Chiu
 Tracy L Wilkison
 AUSA - Office of US Attorney
 National Security Section
 312 North Spring Street Suite 1300
 Los Angeles, CA 90012

15 **Jeffrey G Landis**
16 **Marc J Zwillinger**
17 Zwillgen PLLC
18 1900 M Street NW Suite 250
19 Washington, DC 20036

Counsel for Plaintiff United States

20 **Nicola T Hanna**
21 Gibson Dunn and Crutcher LLP
22 3161 Michelson Drive 12th Floor
23 Irvine, CA 92612-4412

24 **Theodore B Olson**
25 Gibson Dunn and Crutcher LLP
26 1050 Connecticut Avenue NW
27 Washington, DC 20036-5306

28 Counsel for Respondent Apple, Inc.

 BY MAIL: I caused such envelopes, fully prepaid, to be placed in the United States mail at Los Angeles, California. I am “readily familiar” with this firm’s practice for collection and processing of correspondence for mailing. Under that practice, it would be deposited with the United States Postal Service the same day, with postage thereon fully prepaid, at Los Angeles, California, in the ordinary

1 course of business. I am aware that on motion of the party served, service is
2 presumed invalid if the postal cancellation date on the postage meter date is more
3 than one day after the date of deposit for mailing in this affidavit.

4 BY E-MAIL: On March 3, 2016, I sent a courtesy copy of the listed
5 documents to the e-mail addresses listed below:

6 **Eric David Vandavelde**
7 **Theodore J Boutrous, Jr**
8 evandavelde@gibsondunn.com
9 tboutrous@gibsondunn.com

Allen W Chiu
Tracy L Wilkison
allen.chiu@usdoj.gov
tracy.wilkison@usdoj.gov

Jeffrey G Landis
Marc J Zwillinger
jeff@zwillgen.com
marc@zwillgen.com

Counsel for Plaintiff United States

Nicola T Hanna
nhanna@gibsondunn.com

Theodore B Olson
tolson@gibsondunn.com

14 Counsel for Respondent Apple, Inc.

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

18
19 DATED: March 3, 2016

20
21
22 
23
24
25
26
27
28

Mary L Pantoja