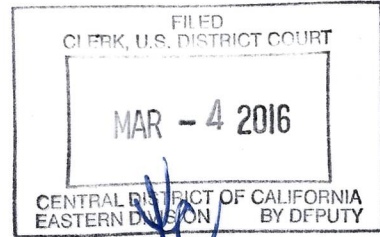


ORIGINAL

1 MICHAEL H. RUBIN, State Bar No. 214636
mrubin@wsgr.com
2 STEPHEN N. GIKOW, State Bar No. 302484
sgikow@wsgr.com
3 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
4 1 Market Street
Spear Tower, Suite 3300
5 San Francisco, CA 94107
Telephone: (415) 947-2000
6 Facsimile: (415) 947-2099



7 BRIAN M. WILLEN, *Pro Hac Vice* Admission Forthcoming
bwillen@wsgr.com
8 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
9 1301 Avenue of the Americas, 40th Floor
New York, NY 10019
10 Telephone: (212) 999-5800
Facsimile: (212) 999-5899
11 Attorneys for *Amicus Curiae*
12 Center for Democracy & Technology

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

LOGGED

27 MAR - 3 PM 3:11
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

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

ED No. CM 16-10 (SP)

~~PROPOSED~~ ORDER GRANTING
CENTER FOR DEMOCRACY &
TECHNOLOGY'S MOTION FOR
LEAVE TO FILE BRIEF AS
AMICUS CURIAE

[NOTE CHANGE MADE
BY THE COURT]

1 The Court, having read and considered the Center for Democracy &
2 Technology's Motion for Leave to File Brief as *Amicus Curiae* In Support of
3 Apple Inc.'s Motion to Vacate and In Opposition to Government's Motion to
4 Compel Assistance ("the Motion"), and finding good cause therefor, hereby orders
5 that:

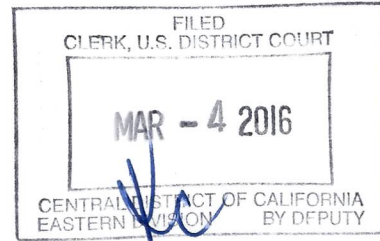
- 6 1. The Motion is granted and the Center for Democracy & Technology
7 has leave to file the Brief *Amicus Curiae* In Support of Apple Inc.'s
8 Motion to Vacate and In Opposition to Government's Motion to
9 Compel Assistance ("CDT *Amicus* Brief").
- 10 2. CDT *Amicus* Brief is accepted as filed.
- 11 ~~3. Should the Court deem it helpful, the Center for Democracy &
12 Technology will be allowed to present oral argument at further
13 hearings to be conducted in this case.~~

14 IT IS SO ORDERED.

15
16 Dated: March 4, 2016

17 By: 
18 _____
19 Hon. Sheri Pym
20
21
22
23
24
25
26
27
28

1 MICHAEL H. RUBIN, State Bar No. 214636
mrubin@wsgr.com
2 STEPHEN N. GIKOW, State Bar No. 302484
sgikow@wsgr.com
3 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
4 1 Market Street
Spear Tower, Suite 3300
5 San Francisco, CA 94107
Telephone: (415) 947-2000
6 Facsimile: (415) 947-2099



7 BRIAN M. WILLEN, *Pro Hac Vice* Admission Forthcoming
bwillen@wsgr.com
8 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
9 1301 Avenue of the Americas, 40th Floor
New York, NY 10019
10 Telephone: (212) 999-5800
Facsimile: (212) 999-5899

11 Attorneys for *Amicus Curiae*
12 Center for Democracy & Technology

13 UNITED STATES DISTRICT COURT
14 CENTRAL DISTRICT OF CALIFORNIA
15 EASTERN DIVISION

2016 MAR -3 PM 3:09

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

BY: _____

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

) ED No. CM 16-10 (SP)

) **BRIEF OF THE CENTER FOR
DEMOCRACY & TECHNOLOGY
AS AMICUS CURIAE IN SUPPORT
OF APPLE INC.'S MOTION TO
VACATE AND IN OPPOSITION TO
GOVERNMENT'S MOTION TO
COMPEL ASSISTANCE**

) **Hearing:**

) Date: March 22, 2016

) Time: 1:00 p.m.

) Place: Courtroom 3 or 4

) Judge: Hon. Sheri Pym

27
28

LOGGED

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

TABLE OF CONTENTS

	Page
INTRODUCTION	1
INTEREST OF THE AMICUS.....	2
ARGUMENT.....	3
I. ORDERING A PRIVATE COMPANY TO DEFEAT ITS OWN SECURITY MEASURES BY CREATING A NEW VERSION OF ITS SOFTWARE IS AN IMPERMISSIBLE EXPANSION OF THE ALL WRITS ACT AND CONTRARY TO CONGRESS’ DECISION TO WITHHOLD THAT POWER FROM LAW ENFORCEMENT	3
A. The Order the Government Seeks Is Not Allowed By the All Writs Act and Violates Apple’s Constitutional Rights	4
B. The All Writs Act Cannot Be Used to Override Congress’s Decision to Require Only Certain Kinds of Communications Providers to Include Backdoors in Their Technology	6
II. COMPELLING COMPANIES TO SUBVERT THEIR OWN SECURITY MEASURES WILL UNDERMINE PUBLIC TRUST IN CONNECTED DEVICES AND EMERGING TECHNOLOGIES	10
A. If the Government Wins This Case, a Wide Range of Other Technology Companies May Be Forced to Subvert Their Security Measures to the Detriment of Users Around the World.....	10
B. Giving the Government the New Power it Seeks Will Undermine User Trust and Legitimate Data Security in Concrete Ways.....	11
CONCLUSION	15

TABLE OF AUTHORITIES

Page(s)

CASES

1

2

3

4 *Additive Controls & Measurement Sys. v. Flowdata, Inc.*, 96 F.3d 1390
(Fed. Cir. 1996)4

5

6 *In re Order Requiring Apple, Inc. To Assist In the Execution of a*
Search Warrant Issued By This Court, 15-MC-1902 (JO), 2015
U.S. Dist. LEXIS 138755 (E.D.N.Y. Oct. 9, 2015) 8-9

7

8 *In re Order Requiring Apple, Inc. To Assist In the Execution of a*
Search Warrant Issued By This Court, 15-MC-1902 (JO) Dkt.
29, slip op. (E.D.N.Y. Feb. 29, 2016).....*passim*

9

10 *In re United States ex rel. an Order Authorizing Disclosure of Location*
Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md.
2011)4

11

12 *In re United States for an Order Authorizing the Use of a Pen Register*,
396 F. Supp. 2d 294 (E.D.N.Y 2005).....*passim*

13 *ITT Cmty. Dev. Corp. v. Barton*, 559 F.2d 1351 (5th Cir. 1978)4

14 *Pa. Bureau of Corr. v. United States Marshals Serv.*, 474 U.S. 34
(1985)3, 6

15 *U.S. Telecom Ass’n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).....6

16 *United States v. New York Tel. Co.*, 434 U.S. 159 (1977).....4

17

STATUTES

18 All Writs Act, 28 U.S.C. § 1651*passim*

19 Communications Assistance for Law Enforcement Act, 47 U.S.C. §§
20 1001, *et. seq.**passim*

21 U.S. Const. amend. I5

MISCELLANEOUS

23 “ASUS Settles FTC Charges That Insecure Home Routers and “Cloud”
24 Services Put Consumers’ Privacy At Risk” (Feb. 23, 2016),
[https://www.ftc.gov/news-events/press-releases/2016/02/asus-](https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put)
25 [settles-ftc-charges-insecure-home-routers-cloud-services-put](https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put)..... 12

26 Barbara Guttman and Edward Roback, *An Introduction to Computer*
Security: The NIST Handbook, National Institute of Standards
27 and Technology, Special Publication 800-12 (October 1995),
available at [http://csrc.nist.gov/publications/nistpubs/800-](http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)
28 [12/handbook.pdf](http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf) (last visited March 2, 2016)5

1 CALEA II: Risks of Wiretap Modifications to Endpoints (May 17,
2 2013), available at [https://www.cdt.org/files/pdfs/CALEAII-
techreport.pdf](https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf)..... 8, 9

3 Comments of the Center for Democracy & Technology on the Use of
4 Encryption and Anonymity in Digital Communications, as
5 submitted to the United Nations (Feb. 13, 2015), available at
[https://cdt.org/files/2015/02/CDT-comments-on-the-use-of-
encryption-and-anonymity-in-digital-communcations.pdf](https://cdt.org/files/2015/02/CDT-comments-on-the-use-of-encryption-and-anonymity-in-digital-communcations.pdf) 11

6 Ellen Nakashima and Andrea Peterson, “Report: Cybercrime and and
7 espionage costs \$445 billion annually,” *Wash. Post* (June 9,
8 2014), [https://.washingtonpost.com/world/security/report-
cybercrime-and-espionage-costs-445-billion-
annually/2014/06/08/8995291c-ecce-11e3-9f5c-
9075d5508f0a_story.html](https://.washingtonpost.com/world/security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html) 14

9 Ellen Nakashima, “Former national security officials urge government
10 to embrace rise of encryption,” *Wash. Post*. (Dec. 15, 2015),
11 [https://www.washingtonpost.com/world/national-
security/former-national-security-officials-urge-government-to-
embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-
12 9c4e-be37f66848bb_story.html?hpid=hp_regional-hp_cards_no-
name%3Ahomepage%2Fcard](https://www.washingtonpost.com/world/national-security/former-national-security-officials-urge-government-to-embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-9c4e-be37f66848bb_story.html?hpid=hp_regional-hp_cards_no-name%3Ahomepage%2Fcard) 14-15

13 *Going Dark: Encryption, Technology, and the balance Between Public
14 Safety and Privacy*, S. Comm. on the Judiciary, 114th Cong. (Jul.
15 8, 2015)..... 7, 8

16 Government Accountability Office, *Effective Patch Management is
Critical to Mitigating Software Vulnerabilities*, [http://www.gao.
gov/new.items/d031138t.pdf](http://www.gao.gov/new.items/d031138t.pdf)..... 13

17 Harold Abelson et. al., Keys Under Doormats: Mandating insecurity by
18 requiring government access to all data and communications 17
19 (July 6, 2015), available at
[https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-
CSAIL-TR-2015-026.pdf](https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf)..... 15

20 “Issue Brief: A “Backdoor” to Encryption for Government
21 Surveillance,” *Center for Democracy & Technology* (Dec. 15,
22 2015), [https://cdt.org/insight/issue-brief-a-backdoor-to-
encryption-for-government-surveillance/](https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/) 8

23 Nicole Perlroth and David E. Singer, “Obama Won’t Seek Access to
24 Encrypted User Data,” *New York Times* (Oct. 10, 2015),
[http://www.nytimes.com/2015/10/11/us/politics/obama-wont-
seek-access-to-encrypted-user-data.html](http://www.nytimes.com/2015/10/11/us/politics/obama-wont-see-access-to-encrypted-user-data.html) 8, 15

25 Press Release (Jan. 27, 2015), [https://www.ftc.gov/news-events/press-
releases/2015/01/ftc-report-internet-things-urges-companies-
26 adopt-best-practices](https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices) 12

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

“Read the Obama administration’s draft paper on technical options for the encryption debate,” *Wash. Post* (last visited Mar. 2, 2016), <http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/>..... 13

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

INTRODUCTION

As a nation, we are stunned and saddened when there are inexplicable attacks on innocent victims, and the tragedy in San Bernardino is no exception.

But the issues in this case go far beyond this one investigation or a single phone. This case is about giving the government the power to conscript technology providers to create new versions of their products intended solely to defeat the security features designed to safeguard their users. It is about minimizing technological vulnerabilities that could be exploited to the detriment of everyone who uses connected devices. A decision in favor of the government would set the stage for similar orders against a wide range of technology companies and all manner of products. It would set a precedent under which any company could be forced to spy on unknowing customers on behalf of law enforcement, and in the process be required to override its own security measures in ways that expose its users to malicious attacks. All of this could be done behind closed doors, *ex parte*, with little or no opportunity for the company or public to be heard.

We live in a world that is increasingly interconnected. You can monitor your sleeping baby through a webcam. You can use your phone to adjust your thermostat on your drive home and then use it to turn on your house lights. You can receive messages on your phone if your carbon monoxide alarm goes off. Your medical devices can make an emergency call for help if you become incapacitated. These are amazing and positive developments for the human experience, and they better our lives.

But these systems need to be safe from malicious third party attacks. A decision compelling Apple to weaken critical security features on its phones will leave the creators of a wide range of Internet-connected consumer products—cars, televisions, personal fitness trackers, even refrigerators and home security systems—vulnerable not only to government conscription by the United States and foreign regimes, but also to malicious attacks by criminals, state actors, and even terrorists.

1 When your whole house is capable of listening to you, poor security features on
2 these connected devices mean that you will have no control over who is hearing
3 your most private moments. And this will have been enabled by the very compa-
4 nies that create this technology, work hard to make it secure, and in whom users
5 must necessarily put their trust. If the government succeeds in this case, the rela-
6 tionship between technology providers and users will be forever altered. Users will
7 never know whether the companies whose products they use have been conscripted
8 by the government to break the essential privacy and security features that are sup-
9 posed to protect them.

10 That is not a world that this Court should welcome. And it is certainly not
11 one that should be created by judges acting without clear statutory authorization.
12 The Court should grant Apple’s motion to quash and deny the government’s mo-
13 tion to compel.

14 **INTEREST OF THE AMICUS**

15 The Center for Democracy & Technology (“CDT”) is a nonprofit advocacy
16 organization that works to ensure that the human rights we enjoy in the physical
17 world are realized online and that technology continues to serve as an empowering
18 force for people worldwide. Integral to this work is CDT’s representation of the
19 public interest in the creation of an open, innovative, and decentralized Internet
20 that promotes the constitutional and democratic values of free expression, privacy,
21 and individual liberty.

22 CDT was formed in 1994 as part of civil society’s efforts to push back
23 against the backdoors mandated by the Communications Assistance for Law En-
24 forcement Act, 47 U.S.C. §§ 1001, *et. seq.* (“CALEA”), a statute directly relevant
25 to this case and discussed in greater detail below. More than 20 years later, the
26 public conversation on these important issues continues, as technology rapidly ex-
27 pands into every portion of our lives. CDT advocates for strong online security and
28 privacy protections, which are essential to building the trust necessary for individ-

1 uals to adopt new technologies and access the multitude of benefits of an increas-
2 ingly interconnected world while also maintaining privacy in their most personal
3 communications, associations, interests, and activities. CDT is keenly aware of the
4 consequences of allowing the government to force private companies to break the
5 very security features they designed, and for that reason it has been a key partici-
6 pant in resisting efforts to expand CALEA to require technology providers like
7 Apple to create backdoors in their products for the benefit of law enforcement.

8 This case squarely implicates these concerns. CDT submits this *amicus curi-*
9 *ae* brief to urge the Court to confine the All Writs Act to the limited purpose for
10 which it was intended and to make clear the government does not have the power
11 to use the courts to conscript technology companies into the unauthorized service
12 of law enforcement.

13 ARGUMENT

14 **I. ORDERING A PRIVATE COMPANY TO DEFEAT ITS OWN SE-** 15 **CURITY MEASURES BY CREATING A NEW VERSION OF ITS** 16 **SOFTWARE IS AN IMPERMISSIBLE EXPANSION OF THE ALL** **WRITS ACT AND CONTRARY TO CONGRESS' DECISION TO** **WITHHOLD THAT POWER FROM LAW ENFORCEMENT**

17 The All Writs Act was enacted in 1789 for the limited purpose of allowing
18 the federal courts to issue auxiliary writs as needed to protect their jurisdiction. *Pa.*
19 *Bureau of Corr. v. United States Marshals Serv.*, 474 U.S. 34, 41-43 (1985). The
20 government now asks the Court to apply this old and narrow statute in a bold and
21 novel way: to order a private company to write new software designed to allow the
22 government to break the security features that the company has designed for the
23 protection of its users. This would transform a statute designed to help fill the in-
24 terstices of federal judicial power into an expansive tool for law enforcement offic-
25 ers to obtain substantive new powers—powers that Congress has, for good reason,
26 declined to convey.

1 **A. The Order the Government Seeks Is Not Allowed By the All Writs**
2 **Act and Violates Apple’s Constitutional Rights**

3 The order the government seeks in this case appears to be unprecedented. No
4 court has ever used the All Writs Act to conscript a private company to create a
5 brand new version of one of its products solely to defeat its own security measures.
6 To apply the Act in this novel way would stretch what is supposed to be a narrow,
7 gap-filling statute, with only limited application to third parties, beyond all meas-
8 ure. “Nothing ... suggests that the All Writs Act can be employed as a general li-
9 cense for district courts to grant relief against non-parties whenever such measures
10 seem useful or efficient.” *Additive Controls & Measurement Sys. v. Flowdata, Inc.*,
11 96 F.3d 1390, 1396 (Fed. Cir. 1996); *see also In re United States ex rel. an Order*
12 *Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp.
13 2d 526, 580 (D. Md. 2011) (“The fact that a party may be assisted in its discharge
14 of its rights or duties by the issuance of a writ is not a sufficient basis for the
15 writ.”) (citing *ITT Cmty. Dev. Corp. v. Barton*, 559 F.2d 1351, 1360 (5th Cir.
16 1978). Indeed, what the government would inflict on Apple are precisely the “un-
17 reasonable burdens” that “may not be imposed” on third parties. *United States v.*
18 *New York Tel. Co.*, 434 U.S. 159, 172 (1977).

19 A fitting response to the government’s request was supplied a decade ago in
20 another case where the All Writs Act was improperly invoked to justify the use of
21 a broad new investigative tool:

22 The government ... thus asks me to read into the All Writs Act an em-
23 powerment of the judiciary to grant the executive branch authority to
24 use investigative techniques either explicitly denied it by the legislative
25 branch, or at a minimum omitted from a far-reaching and detailed statu-
26 tory scheme that has received the legislature’s intensive and repeated
27 consideration. Such a broad reading of the statute invites an exercise of
28

1 judicial activism that is breathtaking in its scope and fundamentally in-
2 consistent with my understanding of the extent of my authority.
3 *In re United States for an Order Authorizing the Use of a Pen Register*, 396 F.
4 Supp. 2d 294, 326 (E.D.N.Y. 2005) (“*In re Pen Register*”). This understanding of
5 the proper judicial role in applying the All Writs Act was echoed earlier this week,
6 when a federal court in New York rejected the government’s application for an or-
7 der requiring Apple to bypass the security on one of its devices. *In re Order Re-*
8 *quiring Apple, Inc. To Assist In the Execution of a Search Warrant Issued By This*
9 *Court*, 15-MC-1902 (JO) Dkt. 29 (E.D.N.Y. Feb. 29, 2016) (“*In re Apple Order*”).
10 As Judge Orenstein explained, “what the government seeks here is to have the
11 court give it authority that Congress chose not to confer.” *Id.*, slip op. at 30. That is
12 even more true in this case.

13 Indeed, what the government seeks in this case would violate Apple’s con-
14 stitutional rights under the First Amendment. The order at issue would not merely
15 force Apple into an act of creative code writing, it would require the company to
16 speak in ways contrary to its basic principles and values, and in a manner that un-
17 dermines previous assurances the company has given its customers about the secu-
18 rity controls of its product. To comply, the company would have to “create a brand
19 new product that impairs the utility of the products it is in the business of selling.”
20 *In re Apple Order*, slip op. at 28. On top of that, Apple would have to authenticate
21 the newly created software using its own cryptographic “signature,” thereby verify-
22 ing as trustworthy a piece of code that the company considers to be malware.¹ This

23
24 ¹ “An electronic signature is a cryptographic mechanism that performs a similar
25 function as a written signature. It is used to verify the origin and contents of a mes-
26 sage. For example, a recipient of data (e.g., an email message) can verify who
27 signed the data and that the data was not modified after being signed. This also
28 means that the originator (e.g., sender of an email message) cannot falsely deny
having signed the data.” Barbara Guttman and Edward Roback, *An Introduction to
Computer Security: The NIST Handbook*, National Institute of Standards and Tech-
nology, Special Publication 800-12 (October 1995),
available at <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf> (last
visited March 2, 2016).

1 kind of compelled speech is inconsistent with the First Amendment. A basic re-
2 quirement for any order issued under the All Writs Act is that it must be “agreeable
3 to the usages and principles of law.” 28 U.S.C. § 1651(a). The order at issue here is
4 nothing of the sort.²

5 **B. The All Writs Act Cannot Be Used to Override Congress’s Deci-**
6 **sion to Require Only Certain Kinds of Communications Providers**
7 **to Include Backdoors in Their Technology**

8 “The All Writs Act is a residual source of authority to issue writs that are not
9 otherwise covered by statute. Where a statute specifically addresses the particular
10 issue at hand, it is that authority, and not the All Writs Act, that is controlling.” *Pa.*
11 *Bureau of Corr.*, 474 U.S. at 43. That is the situation here. Over the past several
12 decades, Congress, the Executive Branch, law enforcement, the private sector, and
13 CDT and other public-interest groups have been engaged in dialogue over precise-
14 ly the issues raised by this case: whether, and under what circumstances, providers
15 of communications technology, device manufacturers, and software developers
16 should be required to create “backdoors” that facilitate the government’s ability to
17 search those products.

18 In 1994, Congress enacted the Communications Assistance for Law En-
19 forcement Act (“CALEA”). The Act “requires telecommunications carriers and
20 equipment manufacturers to build into their networks technical capabilities to as-
21 sist law enforcement with authorized interception of communications and ‘call-
22 identifying information.’” *U.S. Telecom Ass’n v. FCC*, 227 F.3d 450, 454 (D.C.
23 Cir. 2000) (quoting 47 U.S.C. § 1002). The process that produced CALEA allowed
24 various stakeholders—including CDT—to participate, and the law itself was the
25 product of negotiation between those various interests. The resulting statute re-
26 quires “telecommunications carriers” to design their systems in ways that preserve

27 _____
28 ² Apple and other amici are ably briefing the multitude of constitutional con-
cerns raised by this case. CDT shares in these concerns.

1 the government's ability to intercept certain communications (47 U.S.C. § 1002(a))
2 but deliberately withholds obligations to facilitate government surveillance efforts
3 from other kinds of providers.

4 Among the providers that are expressly excluded from CALEA's mandates
5 are "information services" such as Apple (*id.* § 1002(b)(2)). See *In re Apple Order*,
6 slip op. at 16-17. Not only that, CALEA "provides that law enforcement agencies
7 cannot do precisely what the government suggests here: dictate to a private com-
8 pany in the business of manufacturing smartphones the extent to which it may in-
9 stall data security features on such devices." *Id.* at 35 n.29 (citing 47 U.S.C. §
10 1002(b)(1)(b)).

11 While CALEA is imperfect, it reflects a clear legislative choice about what
12 kinds of service providers should—and should not—be compelled to provide pri-
13 vate assistance for law enforcement. Indeed, as Judge Orenstein has explained, the
14 "absence from that comprehensive scheme of any requirement that Apple provide
15 the assistance sought here implies a legislative decision to prohibit the imposition
16 of such a duty." *In re Apple Order*, slip op. at 20. Congress's decision leaves no
17 room for the All Writs Act.

18 The impropriety of using that general statute to recalibrate the balance struck
19 by Congress is underscored by more recent events. In the last few years there has
20 been considerable public debate about whether to expand CALEA to impose obli-
21 gations on providers like Apple that were excluded from the statute's original
22 mandates. In 2015, Congress held hearings addressing whether new legislation
23 should be enacted to require device manufacturers (including Apple) and other
24 providers of emerging technologies to include backdoors in their products to cover
25 cases much like this one. *Going Dark: Encryption, Technology, and the balance*
26 *Between Public Safety and Privacy*, S. Comm. on the Judiciary, 114th Cong. (Jul.
27 8, 2015). This process allowed the relevant stakeholders to make their case. See,
28

1 *e.g., id.* (statements of Deputy Attorney General Sally Quillian Yates and FBI Di-
2 rector James B. Comey).

3 CDT, and many other interested parties, spoke out against those proposals,
4 arguing that incorporating backdoors would fundamentally weaken security fea-
5 tures that are designed to protect users from hackers and other unlawful intruders,
6 both domestic and foreign. *See* “Issue Brief: A “Backdoor” to Encryption for Gov-
7 ernment Surveillance,” *Center for Democracy & Technology* (Dec. 15, 2015),
8 [https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-](https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/)
9 [surveillance/](https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/). In a report coordinated by CDT, for example, a group of leading
10 cryptographers and security researchers explained that:

11 [The] FBI’s desire to expand CALEA mandates amounts to developing
12 for our adversaries capabilities that they may not have the competence,
13 access, or resources to develop on their own. In that sense, the endpoint
14 wiretap mandate of CALEA II may lower the already low barriers to
15 successful cybersecurity attacks.

16 *CALEA II: Risks of Wiretap Modifications to Endpoints* at 7 (May 17, 2013),
17 *available at* <https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf>.

18 After considering these arguments, the Obama Administration ultimately de-
19 cided not to seek legislation. *See* Nicole Perlroth and David E. Singer, “Obama
20 Won’t Seek Access to Encrypted User Data,” *New York Times*, (Oct. 10, 2015),
21 [http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-](http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html)
22 [encrypted-user-data.html](http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html). In making that decision, the Administration concluded
23 “that an effort to compel the companies to give the government access would fail,
24 both politically and technologically.” *Id.*; *see also In re Order Requiring Apple,*
25 *Inc. To Assist In the Execution of a Search Warrant Issued By This Court*, 15-MC-
26 1902 (JO), 2015 U.S. Dist. LEXIS 138755, at *9-10 (E.D.N.Y. Oct. 9, 2015) (ex-
27 plaining that “members of the executive and legislative branches have considered
28 updating [CALEA] to allow, among other things, the judicial authorization of the

1 precise investigative technique at issue here—and have not reached a consensus
2 that such action is warranted”).

3 In this case, however, the government acts as if this debate, and the resulting
4 decisions by the political branches, never happened. Instead, the FBI asks the
5 Court to use the All Writs Act to give it a power that was deliberately withheld in
6 the legislative arena. In fact, the authority that the government now seeks here is
7 broader than anything contemplated in the theoretical CALEA II, because it would
8 force companies to create new versions of products that are already in the mar-
9 ket—versions specifically designed to undo security features built into those prod-
10 ucts and relied upon by the consumers who purchased them.

11 This is an entirely unwarranted expansion of the All Writs Act. The Act is
12 not “a mechanism for the judiciary to give [the government] the investigative tools
13 that Congress has not.” *In re Pen Register*, 396 F. Supp. 2d at 325. There is good
14 reason for that rule. Sensitive and important public policy questions are properly
15 left to specific statutes that can balance competing concerns, rather than be re-
16 solved in an ad hoc manner citing a general statute enacted centuries ago for an en-
17 tirely different purpose. Indeed, it is at odds with basic separation-of-powers prin-
18 ciples to allow the Executive to circumvent the give-and-take of the legislative
19 process by seeking authority from the courts, often in proceedings “shielded from
20 public scrutiny.” *In re Apple Order*, slip op. at 29.

21 That is especially so here, where the relevant legislative debate has already
22 occurred and Congress has decided not to give law enforcement the kind of power
23 it seeks here without any meaningful statutory authorization. In such cases, the
24 courts rightly decline any invitation to “transform the AWA from a limited gap-
25 filling statute that ensures the smooth functioning of the judiciary itself into a
26 mechanism for upending the separation of powers by delegating to the judiciary a
27 legislative power bounded only by Congress’s superior ability to prohibit or
28

1 preempt.” *Id.* at 26. To do otherwise would be “an exercise of judicial activism that
2 is breathtaking in its scope.” *In re Pen Register*, 396 F. Supp. 2d at 326.

3 **II. COMPELLING COMPANIES TO SUBVERT THEIR OWN SECURITY MEASURES WILL UNDERMINE PUBLIC TRUST IN CON-**
4 **NECTED DEVICES AND EMERGING TECHNOLOGIES**

5 The government pretends that this case is only about a single investigation
6 and a solitary iPhone used by a deceased killer. But the expansive power that the
7 government is seeking cannot be limited to a single company, and certainly not to
8 one person’s phone. Compelling Apple to write software to defeat its own security
9 and to facilitate the hacking of its technology will set the stage for similar requests
10 aimed at a wide range of other providers and other devices. That will have far-
11 reaching consequences. Allowing the government to force technology companies
12 to rewrite or rewire their products at the direction of law enforcement will funda-
13 mentally alter the relationship between those companies and their users. It will
14 erode public trust across a variety of devices and applications. This will make
15 those technologies—and those who use them—less secure, not just from the gov-
16 ernment but from hackers, thieves, and repressive regimes.

17 **A. If the Government Wins This Case, a Wide Range of Other Tech-**
18 **nology Companies May Be Forced to Subvert Their Security**
Measures to the Detriment of Users Around the World

19 Although this case may concern a single company and a single smartphone,
20 the potential impact of this Court’s decision is far broader. People now use a wide
21 variety of advanced, Internet-enabled technologies. Once a precedent is established
22 that the All Writs Act can be used to force companies to break their own products,
23 any of these devices could be subject to a similar order. This has startling implica-
24 tions for security and privacy across a wide range of emerging technologies.

25 The government might next try to obtain an order requiring a smart TV
26 manufacturer to write new code that uses the television’s voice-recognition tech-
27 nology to record and report back what is being said in a customer’s living room. Or
28 the government could conscript a home-security company to issue a software up-

1 date to an in-home camera that would suddenly allow government agents to watch
2 the homeowner's every move. A court order could likewise require a wearable fit-
3 ness company to hijack a GPS-enabled fitness tracker, reporting to the government
4 real-time data about the wearer's location. These companies would be compelled
5 by law enforcement to defeat the very aspects of their products that are supposed to
6 protect users' privacy and security.

7 The result of all this would be profound. Citizens would be increasingly vul-
8 nerable to cybercriminals and others seeking to put their weakened devices to illicit
9 use. Some of the most vulnerable users of connected technologies, who heavily re-
10 ly on those technologies' privacy and security features, are those doing work in the
11 public interest: human rights activists, advocates, journalists, and others. These in-
12 dividuals place a premium on secure communications and data because they face
13 such obvious dangers from repressive regimes and others intent on thwarting their
14 activities. Weakening the technology that they rely on to do their jobs may expose
15 them to great harm, as well as deter others from taking on this important work. *See*
16 *Comments of the Center for Democracy & Technology on the Use of Encryption*
17 *and Anonymity in Digital Communications*, as submitted to the United Nations
18 (Feb. 13, 2015), *available at* [https://cdt.org/files/2015/02/CDT-comments-on-the-](https://cdt.org/files/2015/02/CDT-comments-on-the-use-of-encryption-and-anonymity-in-digital-communcations.pdf)
19 [use-of-encryption-and-anonymity-in-digital-communcations.pdf](https://cdt.org/files/2015/02/CDT-comments-on-the-use-of-encryption-and-anonymity-in-digital-communcations.pdf).

20 **B. Giving the Government the New Power it Seeks Will Undermine**
21 **User Trust and Legitimate Data Security in Concrete Ways**

22 In an increasingly connected world, security is the predicate to all of our dig-
23 ital lives. Businesses rely on the security of information to keep their customers'
24 data safe and their own information out of the hands of competitors and criminals.
25 Similar protections allow doctors to meet virtually with patients around the world;
26 they give online shoppers the confidence to send payment information to their fa-
27 vorite stores; they allow curious college students to be comfortable enough to
28 search for and read unpopular opinions; they are necessary features of any baby

1 monitor. As the Chairwoman of the FTC noted: “The only way for the Internet of
2 Things to reach its full potential for innovation is with the trust of American con-
3 sumers.” Press Release (Jan. 27, 2015), [https://www.ftc.gov/news-events/press-](https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices)
4 [releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices](https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices).

5 Unsurprisingly, therefore, technology companies devote considerable re-
6 sources to developing and implementing security and privacy features on their
7 products. They make representations about those features to consumers and regula-
8 tors, which help set consumer expectations about how technology works and what
9 protections they provide to users.³ Now, however, the FBI seeks to destabilize this
10 dynamic by demanding the power to force these same companies to create new
11 versions of their products that would undermine the very features that are supposed
12 to protect users and safeguard their information. That would profoundly undermine
13 companies’ relationships with their users.

14 How can people trust that the security features protecting the technologies
15 they rely on for work, education, friendship, and romance will actually keep them
16 secure if the government can force the same company who designs the product to
17 break it? This is a profound disruption. The public generally has to take on faith
18 that a given product or software update is secure: users are often not in a position
19 to independently verify the security of their devices or every software update. That
20 faith comes from a company’s statements about its products and from that compa-
21 ny’s history and reputation. By making companies into adjuncts of law enforce-
22 ment and compelling them to create new versions of their own products that defeat

23
24
25 ³ Indeed, government agencies, including the Federal Trade Commission and
26 the Federal Communications Commission, stand ready to hold the private sector
27 accountable for the promises they make about the security of their devices and, in
28 some cases, to require them to adopt certain kinds of security or data-protection
features. *See, e.g.*, “ASUS Settles FTC Charges That Insecure Home Routers and
“Cloud” Services Put Consumers’ Privacy At Risk” (Feb. 23, 2016),
[https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-](https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put)
[insecure-home-routers-cloud-services-put](https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put).

1 existing security and privacy features—but that still come with the company’s
2 cryptographic seal of approval—the order the government seeks here will directly
3 undermine that trust. When companies are forced to deceive their customers and
4 push out software updates for the benefit of law enforcement rather than for the
5 good of their users, those users will naturally come to distrust what those compa-
6 nies say and look skeptically at any new version of their products.

7 Disrupting the trust between technology providers and their users will have
8 real consequences, which are likely to be felt in several different ways.

9 First, users may be less willing to update the software on their devices,
10 which in turn will make those devices less secure over time. Software updates are
11 essential for keeping technology up-to-date, with the latest patches fixing the most
12 recent security vulnerabilities. Government Accountability Office, *Effective Patch*
13 *Management is Critical to Mitigating Software Vulnerabilities*, <http://www.gao.gov/new.items/d031138t.pdf>. There is serious concern that granting orders like the
14 one at issue here will diminish trust in such updates more generally. Indeed, the
15 Obama Administration’s own working group worried about this very thing. It ex-
16 plained that enabling “remote access to encrypted devices through current update
17 procedures ... could call into question the trustworthiness of established software
18 update channels,” which in turn might lead individuals “to turn off software up-
19 dates, rendering their devices significantly less secure as time passed and vulnera-
20 bilities were discovered by [sic] not patched.” “Read the Obama administration’s
21 draft paper on technical options for the encryption debate,” *Wash. Post* at 6 (last
22 visited Mar. 2, 2016), [http://apps.washingtonpost.com/g/documents/world/read-](http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/)
23 [the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-](http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/)
24 [debate/1753/](http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/). The order that the government seeks against Apple highlights this
25 very problem. As explained above, the order requires Apple to issue a new soft-
26 ware update designed specifically to undermine the company’s existing security
27 features. In order for the target device to accept the update, Apple would need to
28

1 verify the government-mandated update using its cryptographic signature. That
2 signature acts as a “wax seal” on the envelope containing the software update: it
3 tells users that the software update came from Apple and is safe to install. But if
4 the government can force Apple to sign software as legitimate that Apple actually
5 considers to be untrustworthy malware, it would call into question all future soft-
6 ware updates and cryptographic signatures, not just from Apple but from other
7 technology companies that may be subject to similar orders. If users distrustful of
8 government-mandated updates decline to install software updates more generally,
9 it would leave a cluster of these “unpatched” devices, which would be prime tar-
10 gets for criminals, malicious hackers, and others with nefarious intent. The exist-
11 ence of those devices would make other connected devices and even whole net-
12 works more vulnerable. Reports estimate that the U.S. already loses \$100 billion to
13 cybercrime every year. Ellen Nakashima and Andrea Peterson, “Report: Cyber-
14 crime and espionage costs \$445 billion annually,” *Wash. Post* (June 9, 2014),
15 [https://www.washingtonpost.com/world/national-security/
16 report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/
17 8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html](https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html). By fostering this dangerous
18 dynamic, the order the government seeks would help create a landscape even more
19 ripe for such abuse.

20 Second, if the U.S. government can demand these kinds of backdoors, other
21 governments more repressive and less restrained than our own will surely demand
22 them as well. This danger will make our technological infrastructure weaker and
23 more susceptible to foreign espionage and cyberattack.⁴ That is one important rea-
24 son why a respected group of former intelligence officers have argued that the FBI
25 is wrong to seek backdoor access to U.S. companies’ technology. Ellen

26 _____
27 ⁴ Fear of other governments gaining similar access was one of the main reasons
28 that the Obama Administration decided not to seek legislation requiring the very
kind of backdoor that the FBI is seeking here to exploit. *See* Perlroth and Singer,
supra.

1 Nakashima, “Former national security officials urge government to embrace rise of
2 encryption,” *Wash. Post.* (Dec. 15, 2015), [https://www.washingtonpost.com/
3 world/national-security/former-national-security-officials-urge-government-to-
4 embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-9c4e-be37f66848bb_
5 story.html](https://www.washingtonpost.com/world/national-security/former-national-security-officials-urge-government-to-embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-9c4e-be37f66848bb_story.html).

6 Third, if they are unable to trust that American technology providers are not
7 working behind the scenes to undermine their own products at the government’s
8 behest, people may turn to foreign products that are seen as more secure and less
9 vulnerable to hacking mandated by American law enforcement officers. Former
10 CIA director and NSA head Michael V. Hayden has expressed concern about this
11 exact problem, which he calls “the worst of all worlds: there will be unbreakable
12 encryption—it just won’t be made by American firms.” Nakashima, “Former na-
13 tional security officials urge government to embrace rise of encryption,” *supra*.
14 Not only would this undermine the interests of U.S. law enforcement, it would be a
15 major blow to the U.S. companies that produce these technologies—companies
16 that are currently worldwide leaders but might see their positions slip as consumers
17 seek hardware and software elsewhere. *See, e.g.*, Harold Abelson et. al., Keys Un-
18 der Doormats: Mandating insecurity by requiring government access to all data and
19 communications 17 (July 6, 2015), *available at* [https://dspace.mit.edu/
20 bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf](https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf).

21 CONCLUSION

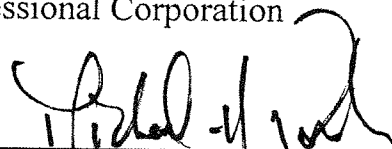
22 The Court has been asked to give law enforcement officials a broad new
23 power to compel private businesses to speak by writing—and ratifying as trustwor-
24 thy—software designed to circumvent their own security measures. The members
25 of the First Congress who drafted the All Writs Act—patriots for whom the experi-
26 ence of overbearing royal authority was still fresh in the mind—could hardly have
27 imagined such an application of the statute. This case threatens to dramatically un-
28

1 dermine all of our safety and privacy. The government's motion to compel should
2 be denied, and Apple's motion to vacate granted.

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

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: 
Michael H. Rubin

Attorneys for *Amicus Curiae*
Center for Democracy & Technology

1 MICHAEL H. RUBIN, State Bar No. 214636
mrubin@wsgr.com
2 STEPHEN N. GIKOW, State Bar No. 302484
sgikow@wsgr.com
3 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
4 1 Market Street
Spear Tower, Suite 3300
5 San Francisco, CA 94107
Telephone: (415) 947-2000
6 Facsimile: (415) 947-2099



7 BRIAN M. WILLEN, *Pro Hac Vice* Admission Pending
bwillen@wsgr.com
8 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
9 1301 Avenue of the Americas, 40th Floor
New York, NY 10019
10 Telephone: (212) 999-5800
Facsimile: (212) 999-5899

11 Attorneys for *Amicus Curiae*
12 Center for Democracy & Technology

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

2016 MAR 24 PM 3:10
CLERK, U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE
BY

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

ED No. CM 16-10 (SP)
PROOF OF SERVICE

LOGGED

PROOF OF SERVICE BY U.S. MAIL AND E-MAIL

I, Joanna Delaney, declare:

I am employed in City and County of San Francisco, State of California. I am over the age of 18 years and not a party to the within action. My business address is Wilson Sonsini Goodrich & Rosati, One Market Street, Spear Street, Suite 3300, San Francisco, CA 94105-1126.

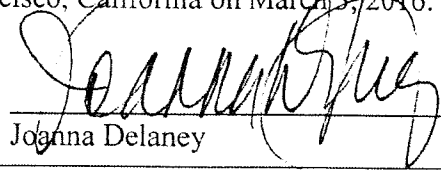
I am readily familiar with Wilson Sonsini Goodrich & Rosati's practice for collection and processing of correspondence for mailing with the United States Postal Service. In the ordinary course of business, correspondence would be deposited with the United States Postal Service on this date.

On this date, I served:

1. **CENTER FOR DEMOCRACY & TECHNOLOGY'S NOTICE OF MOTION AND MOTION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF APPLE INC.'S MOTION TO VACATE AND IN OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE**
2. **BRIEF OF CENTER FOR DEMOCRACY & TECHNOLOGY AS *AMICUS CURIAE* IN SUPPORT OF APPLE INC.'S MOTION TO VACATE AND IN OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE**
3. **[PROPOSED] ORDER GRANTING CENTER FOR DEMOCRACY & TECHNOLOGY'S MOTION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE***

on each person listed below, by placing the document(s) described above in an envelope addressed as indicated below, which I sealed. I placed the envelope(s) for collection and mailing with the United States Postal Service on this day, following ordinary business practices at Wilson Sonsini Goodrich & Rosati. In addition, I forwarded the document(s) by electronic transmission on this date to the Internet email addresses listed below.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed at San Francisco, California on March 3, 2016.


Joanna Delaney

Service List

Service Type	Counsel Served	Party
Mail & E-mail	Theodore J. Boutrous, Jr. Nicola T. Hanna Eric D. Vandeveld Gibson, Dunn & Crutcher LLP 333 South Grand Avenue Los Angeles, CA 90071-3197 Telephone: (213) 229-7000 Facsimile: (213) 229-7520 Email: tboutrous@gibsondunn.com nhanna@gibsondunn.com evandeveld@gibsondunn.com	Apple, Inc.
Mail & E-mail	Theodore B. Olson Gibson, Dunn & Crutcher LLP 1050 Connecticut Avenue, N.W. Washington, DC, 20036-5306 Telephone: (202) 955-8500 Facsimile: (202) 467-0539 Email: tolson@gibsondunn.com	Apple, Inc.
Mail & E-mail	Marc J. Zwillinger Jeffrey G. Landis Zwillgen PLLC 1900 M Street N.W., Suite 250 Washington, D.C. 20036 Telephone: (202) 706-5202 Facsimile: (202) 706-5298 Email: marc@zwillgen.com jeff@zwillgen.com	Apple, Inc.
Mail & E-mail	Eileen M. Decker Patricia A. Donahue Tracy L. Wilkison Allen W. Chiu 1500 United States Courthouse 7312 North Spring Street Los Angeles, California 90012 Telephone: (213) 894-0622/2435 Facsimile: (213) 894-8601 Email: Tracy.Wilkison@usdoj.gov Allen.Chiu@usdoj.gov	United States of America