

FILED
CLERK U.S. DISTRICT COURT
MAR - 7 2016
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION
BY DEPUTY

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

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

ED No. CM 16-10-SP

~~[PROPOSED]~~ **DENYING** ORDER ~~GRANTING~~
MOTION OF INTEL
CORPORATION FOR LEAVE TO
FILE BRIEF AS AMICUS CURIAE

Judge: Hon. Sheri Pym

LOGGED

2016 MAR 3 AM 11:22
CLERK U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIF.
RIVERSIDE
BY

The Court, having considered the Motion of Intel Corporation for Leave to File Brief as Amicus Curiae, and having found good cause for the relief sought, HEREBY ORDERS that the Motion is GRANTED and that the Brief of Amicus Curiae attached to the Motion is deemed filed with this Court.

Dated: _____

Hon. Sheri Pym
United States Magistrate Judge

DENIED
BY ORDER OF
SHERI PYM
UNITED STATES MAGISTRATE JUDGE
ON March 7, 2016

Reason: Brief not signed by an attorney admitted to practice before this Court. See Local Rules 11-1, 83-2.1.1.1, 83-2.1.3.3.

LODGED

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

Daniel F. Katz*
dkatz@wc.com
Kannon K. Shanmugam*
kshanmugam@wc.com
Richmond T. Moore*
rtmoore@wc.com
David M. Krinsky*
dkrinsky@wc.com
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Telephone: (202) 434-5000
Facsimile: (202) 434-5029

William Faulkner (SBN 83385)
wfaulkner@mcmmanislaw.com
MCMANIS FAULKNER
One California Plaza
300 So. Grand Avenue, 37th Floor
Los Angeles, CA 90071
Telephone: (408) 279-8700
Facsimile: (408) 279-3244

**Pro Hac Vice Admission Pending*
Attorneys for Intel Corporation

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

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

Darren B. Bernhard*
darren.b.bernhard@intel.com
Vice President
Director of Antitrust & Commercial
Litigation
INTEL CORPORATION
1155 F Street, N.W.
Washington, DC 20004
Telephone: (202) 626-4380

Tanya L. Hunter (SBN 197761)
tanya.hunter@intel.com
Associate General Counsel
Antitrust & Commercial Litigation
INTEL CORPORATION
2200 Mission College Blvd.
Santa Clara, CA 95054
Telephone: (408) 765-2318
Facsimile: (408) 765-5157

ED No. CM 16-10-SP

**BRIEF OF INTEL CORPORATION
AS AMICUS CURIAE IN SUPPORT
OF APPLE INC.**

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

TABLE OF CONTENTS

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

TABLE OF AUTHORITIES.....ii

INTEREST OF AMICUS CURIAE 1

SUMMARY OF ARGUMENT 1

ARGUMENT 3

I. ENCRYPTION TECHNOLOGY IS ESSENTIAL FOR THE SECURITY OF THE GLOBAL ECONOMY AND CRITICAL INFRASTRUCTURE 3

II. THE ALL WRITS ACT DOES NOT AUTHORIZE WEAKENING THE SECURITY OF TECHNOLOGY COMPANIES’ PRODUCTS 5

 A. CALEA Does Not Require The Assistance Sought From Apple..... 6

 B. The Government Cannot Use The All Writs Act To Circumvent CALEA 8

III. GRANTING THE GOVERNMENT’S PROPOSED RELIEF WOULD ESTABLISH A DANGEROUS PRECEDENT 11

 A. Intel And Other Companies Are Likely Targets of Similar Demands 12

 B. Granting The Government’s Proposed Relief Would Create Precedent For Other Courts, Law-Enforcement Agencies, And Foreign Governments 13

 C. The Government’s Proposed Relief Raises Important Issues That Should Be Addressed Through Vigorous Public Debate 14

CONCLUSION 15

TABLE OF AUTHORITIES

CASES

1

2

3 *Cty. of Sacramento v. Lewis,*

4 523 U.S. 833 (1998)..... 11

5 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search*

6 *Warrant Issued By This Court,*

7 2016 WL 783565, Misc. No. 15-1902 (E.D.N.Y. Feb. 29, 2016)..... 9, 10, 11

8 *In re Application of the U.S. for an Order (1) Authorizing the Use of a*

9 *Pen Register & a Trap & Trace Device,*

10 396 F. Supp. 2d 294 (E.D.N.Y. 2005) 10

11 *In re Application of U.S. For An Order,*

12 849 F. Supp. 2d 526 (D. Md. 2011) 10

13 *Pennsylvania Bureau of Correction v. U.S. Marshals Service,*

14 474 U.S. 34 (1985).....6

15 *Plum Creek Lumber Co. v. Hutton,*

16 608 F.2d 1283 (9th Cir. 1979).....6

17 *Riley v. First National Fed. of the Blind of N.C., Inc.,*

18 487 U.S. 781 (1988)..... 11

19 *United States v. New York Telephone Co.,*

20 434 U.S. 159 (1977)..... 10, 11

STATUTES

21

22 28 U.S.C. § 1651 5, 6

23 47 U.S.C. § 1001 6, 7

24 47 U.S.C. § 1002 6, 7

25

26

27

28

TABLE OF AUTHORITIES
(Continued)

OTHER AUTHORITIES

1
2
3
4 Craig Whitlock & Missy Ryan, *U.S. Suspects Russia In Hack Of*
5 *Pentagon Computer Network*, Wash. Post (Aug. 6, 2015).....4
6
7 *Digital Telephony and Law Enforcement Access to Advanced Telecom-*
8 *munications Technologies and Services: Joint Hearings on H.R. 4922*
9 *and S. 2375 Before the S. Subcomm. On Technology and the Law of*
10 *the S. Comm. on the Judiciary and the H. Subcomm. On Civil and*
11 *Constitutional Rights of the H. Comm. on the Judiciary*, 103rd Cong.
12 11 (1994) (testimony of FBI Director Louis J. Freeh).....8
13
14 H.R. Rep. No. 103-827, pt. 1 (1994)..... 7, 8
15
16 Karoun Demirjian, *Apple Case Creates Fervor For Encryption Bill In*
17 *Congress*, Wash. Post (Feb. 25, 2016)..... 13
18
19 Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S.*
20 *over Data Access*, N.Y. Times (Sept. 7, 2015).....5
21
22 Mike McConnell, Michael Chertoff & William Lynn, *Why The Fear*
23 *Over Ubiquitous Data Encryption Is Overblown*, Wash. Post (July
24 28, 2015).....4
25
26 Office of Personnel Management, *Cybersecurity Resource Center*4
27
28 Paul Mozur, *New Rules in China Upset Western Tech Companies*, N.Y.
Times (Jan. 28, 2015)..... 14
Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 Colum.
Sci. & Tech. L. Rev. 416 (2012).....3
President’s Review Group on Intelligence & Communications Technolo-
gies, *Liberty and Security in a Changing World* (2013).....4
Saba Hamedy, *Sony Execs’ Salaries, Employee SSNs Allegedly Leaked*
In Breach, L.A. Times (Dec. 2, 2014)4

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. I 11

1 **INTEREST OF AMICUS CURIAE**

2 Intel is one of the world’s leading technology companies. Intel develops and
3 manufactures computer, communication, and other electronic components that are
4 used in servers, desktops, laptops, tablets, smartphones, and wearables. Intel also
5 develops and sells software and services that integrate security and technology.
6 Intel’s products are used in hundreds of millions of devices around the world by
7 everyday citizens, companies, and government agencies, among many others.

8 Through its expertise in hardware and software, Intel embeds security in many
9 facets of computing, and it offers solutions and services to help secure the world’s
10 most critical systems and networks. Intel thus has a unique perspective on the
11 potential consequences of a ruling that would weaken security features in technology
12 products. Intel submits this brief to assist the Court in considering the issues raised
13 by this case.

14 **SUMMARY OF ARGUMENT**

15 This case presents the vitally important question whether the government has
16 the authority to force a company to develop technology for the purpose of
17 circumventing the security features of its products. That question implicates the need
18 to achieve two related but separate goals: assisting law enforcement to obtain
19 information to conduct its investigations, on the one hand, and protecting the privacy
20 and security interests of the general public, on the other.

21 Crucially, Congress has already considered how to achieve these goals—and
22 has made the deliberate judgment *not* to confer the authority the government seeks
23 here. In the Communications Assistance for Law Enforcement Act (CALEA),
24 Congress specifically addressed what types of technical assistance companies should
25 provide to law enforcement. After careful consideration, Congress decided that
26 companies must provide law enforcement with certain assistance in intercepting data
27 but are not required affirmatively to decrypt information stored on their customers’
28 devices.

1 The Department of Justice and the FBI have made it clear in recent years that,
2 because of advancements in encryption technology, they are dissatisfied with the
3 limitations imposed by CALEA. As a result, the government has implemented a
4 strategy of attempting to compel technical assistance from companies through the All
5 Writs Act of 1789, thereby using that statute to obtain the same authority that
6 Congress withheld in CALEA. But the All Writs Act plainly does not confer the
7 sweeping authority that the government claims. The All Writs Act provides courts
8 with ancillary, “gap-filling” jurisdictional authority in the absence of more specific
9 congressional action; it does not permit law-enforcement agencies to defy Congress’s
10 will on an issue it has carefully considered and, under the guise of “gap-filling,” to
11 claim authority those agencies would simply like to have. The eighteenth-century
12 Congress that drafted the All Writs Act would be surprised to see it used to override a
13 specific judgment made by its twentieth-century successor. This Court should reject
14 the government’s improper use of the All Writs Act to alter the solution Congress
15 reached in CALEA.

16 Even if Congress had not already made the judgment in CALEA to withhold
17 such authority from the government, it would be bad policy to permit the government
18 to compel companies to weaken the security features of their products in order to
19 assist law enforcement. Companies such as Intel are in the business of improving the
20 security of their technology products, not undermining it. Requiring companies such
21 as Intel to weaken the security of their products would have serious repercussions for
22 personal privacy and the security of the digital infrastructure. And if the
23 government’s proposed relief were granted, technology companies would be subject
24 to the same types of demands from other law-enforcement agencies in the United
25 States, as well as foreign governments. Law-enforcement agencies have a critical
26 mission to protect national security and the American people. Recognizing the
27 importance of that mission, Intel responds to lawful demands for information from
28

1 government agencies. But Intel opposes a government mandate to weaken security
2 features in technology products.

3 For purposes of this motion, however, the key point is that evaluating these
4 competing and important policy considerations is a matter for Congress in the first
5 instance. Should Congress wish to reconsider the solution adopted in CALEA, it is of
6 course free to do so. But before the government is given the broad authority to force
7 a company to develop technology for the purpose of circumventing security features,
8 the issues that such authority would raise should be discussed and debated through
9 the democratic process, with consultation involving industry and other affected
10 stakeholders. Because the government currently does not have that authority,
11 Apple's motion to vacate should be granted.

12 ARGUMENT

13 I. ENCRYPTION TECHNOLOGY IS ESSENTIAL FOR THE SECURITY 14 OF THE GLOBAL ECONOMY AND CRITICAL INFRASTRUCTURE

15 The dispute between Apple and the government is part of a broader ongoing
16 debate over developments in encryption technology. Encryption is critical to the
17 global economy because it allows users to communicate and store information
18 securely and confidentially. Almost every sector of our economy relies on robust
19 encryption technology to protect against unauthorized access to sensitive information.
20 "In fact, encryption is the norm, not the exception, and is used in innumerable
21 ways—from protecting critical public infrastructure and sensitive personal
22 information, to securing communications and commercial transactions."¹ Intel's
23 customers demand hardware and software products that permit encryption.

24 The importance of strong encryption is highlighted by recent security breaches.
25 In November 2014, cybercriminals breached the computer systems of Sony Pictures
26

27 ¹ Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 Colum. Sci. &
28 Tech. L. Rev. 416, 453 (2012).

1 Entertainment and reportedly obtained the Social Security numbers and other
2 personal identifying information of tens of thousands of individuals.² The
3 government also recently reported that hackers had infiltrated the systems of the
4 Office of Personnel Management (OPM) and stolen the personal information of 21.5
5 million individuals, including 5.6 million fingerprints.³ Hackers have also penetrated
6 the e-mail system used by the Joint Chiefs of Staff.⁴

7 These documented security breaches, and the potential for others like them,
8 have led many experienced government officials to reject weakening cybersecurity as
9 a means to achieve greater national security. As an editorial by several high-ranking
10 former national security officials recently explained: “[T]he greater public good is a
11 secure communications infrastructure protected by ubiquitous encryption at the
12 device, server and enterprise level without building in means for government
13 monitoring.”⁵

14 Encryption technology has evolved significantly to meet the growing threat of
15 security breaches. To enhance the security of their products, companies have in
16 recent years created encryption technology where individual users’ devices (*e.g.*,
17 computers, tablets, and smartphones) have their own decryption keys to which only
18 the users have access. Where keys are stored only on users’ devices, the

19 _____
20 ² Saba Hamedy, *Sony Execs’ Salaries, Employee SSNs Allegedly Leaked In*
Breach, L.A. Times (Dec. 2, 2014) <goo.gl/0JVkot>.

21 ³ See OPM, Cybersecurity Resource Center <goo.gl/ukW8gb>.

22 ⁴ Craig Whitlock & Missy Ryan, *U.S. Suspects Russia In Hack Of Pentagon Com-*
23 *puter Network*, Wash. Post (Aug. 6, 2015) <goo.gl/WKCb1M>.

24 ⁵ Mike McConnell, Michael Chertoff & William Lynn, *Why The Fear Over Ubiq-*
25 *uitous Data Encryption Is Overblown*, Wash. Post (July 28, 2015) <goo.gl/c0BSCP>;
26 *see also* President’s Review Group on Intelligence & Communications Technologies,
27 *Liberty and Security in a Changing World* at 22 (2013) (arguing that “[t]he US Gov-
28 *ernment should take additional steps to promote security, by . . . supporting efforts to*
encourage the greater use of encryption technology for data in transit, at rest, in the
cloud, and in storage”) < goo.gl/45w2LN>.

1 manufacturer no longer holds keys to decrypt the data. Therefore, the use of this
2 technology largely places the ability to protect a user's information in the user's own
3 hands.⁶ Some companies that offer remote data storage in the "cloud" also permit
4 customers to have exclusive control over the decryption keys to their data.

5 One consequence of these developments in encryption technology is that it is
6 more difficult for law-enforcement officials to obtain certain data. Officials can no
7 longer access encrypted data simply by obtaining a master decryption key from the
8 manufacturer; instead, they must find another mechanism to retrieve data from the
9 device, such as obtaining individual decryption keys from the devices themselves.
10 Law-enforcement officials are thus increasingly seeking to enlist the assistance of
11 technology companies in retrieving decryption keys from their customers' devices or
12 finding another way to defeat the encryption.

13 In this case, the government is seeking to compel Apple to take an
14 unprecedented step: to create new software intended to weaken the existing security
15 features of an Apple product in order to facilitate an effort to unlock the iPhone by a
16 "brute force" attack on its passcode. To be clear, the government is not asking Apple
17 to extract data from a device using a key that Apple has, because Apple does not
18 possess the encryption key for the iPhone in question. Instead, the government hopes
19 to commandeer Apple's resources and software engineers to create software that has
20 not yet been developed for the purpose of undermining the security features present
21 on the phone. This attempt to force a technology company to decrease the security of
22 its technology is both unprecedented and unauthorized.

23 **II. THE ALL WRITS ACT DOES NOT AUTHORIZE WEAKENING THE** 24 **SECURITY OF TECHNOLOGY COMPANIES' PRODUCTS**

25 Enacted by the First Congress in 1789, the All Writs Act provides that "[t]he
26 Supreme Court and all courts established by Act of Congress may issue all writs

27
28 ⁶ See, e.g., Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S. over Data Access*, N.Y. Times (Sept. 7, 2015) <goo.gl/Y9984t>.

1 necessary and appropriate in aid of their respective jurisdictions and agreeable to the
2 usages and principles of law.” 28 U.S.C. § 1651(a). As the Ninth Circuit has
3 explained, the All Writs Act “is not a grant of plenary power to the federal courts,”
4 but is “designed to aid the courts in the exercise of their jurisdiction.” *Plum Creek*
5 *Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). The purpose of the All
6 Writs Act is to “fill[] the interstices of federal judicial power when those gaps
7 threatened to thwart the otherwise proper exercise of federal courts’ jurisdiction.”
8 *Pennsylvania Bureau of Correction v. U.S. Marshals Service*, 474 U.S. 34, 41 (1985).

9 Consistent with the gap-filling function performed by the All Writs Act, the
10 Supreme Court has made clear that, “[w]here a statute specifically addresses the
11 particular issue at hand, it is *that authority*, and not the All Writs Act, that is
12 controlling.” *Pennsylvania Bureau of Correction*, 474 U.S. at 43 (emphasis added).
13 The Act does not “authorize [courts] to issue ad hoc writs whenever compliance with
14 statutory procedures appears inconvenient or less appropriate.” *Id.*

15 **A. CALEA Does Not Require The Assistance Sought From Apple**

16 The All Writs Act does not apply here because, when Congress enacted
17 CALEA, it expressly refused to confer the authority that the government seeks.
18 CALEA imposed technical-assistance requirements on certain “telecommunications
19 carrier[s].” See 47 U.S.C. § 1002(a). In enacting CALEA, however, Congress
20 considered whether companies should be obligated to provide technical assistance to
21 unlock encrypted messages, and decided not to impose that requirement. Because
22 Congress made a considered judgment not to confer such authority in CALEA, the
23 government cannot claim that authority through the backdoor of the All Writs Act.

24 *First*, Congress declined to impose technical-assistance requirements on
25 companies that provide “information services,” such as Apple. 47 U.S.C.
26 § 1002(b)(2)(A). Those services were defined to include “electronic messaging
27 services,” *id.* § 1001(6)(B)(iii), which include e-mail and instant messaging. They
28 also included “service[s] that permit[] a customer to retrieve stored information from,

1 or file information for storage in, information storage facilities”—that is, services that
2 store and process data that have reached a destination and are at rest (whether in a
3 computer, a handheld device, or in the cloud). *Id.* § 1001(6)(B)(i). Apple is a
4 provider of “information services” and, as such, is indisputably not subject to
5 CALEA’s technical-assistance requirements.

6 *Second*, even if Apple were subject to those requirements, it would still not be
7 obliged to provide technical assistance for the purpose of penetrating end-to-end
8 encryption. Under Section 1002(b)(3), the telecommunications carriers covered by
9 CALEA “shall not be responsible for decrypting, *or ensuring the government’s*
10 *ability to decrypt*, any communication encrypted by a subscriber or customer, unless
11 the encryption was provided by the carrier and the carrier possesses the information
12 necessary to decrypt the communication.” *Id.* § 1002(b)(3) (emphasis added). In
13 other words, CALEA requires a company to decrypt data if it has access to a “master
14 key.” But if a user has encrypted data on his or her iPhone and Apple does not have
15 the information “necessary to decrypt” that phone, Apple has no responsibility to
16 “ensur[e] the government’s ability to decrypt” that iPhone. *Id.* § 1002(b)(3). For this
17 additional reason, CALEA’s express language precludes the government’s proposed
18 relief.

19 In enacting CALEA, Congress squarely considered where to draw the line in
20 allowing the government to compel access via third parties to encrypted technology.
21 In the legislative process, Congress was warned that “new and emerging
22 technologies” would pose “legitimate impediments” to the FBI’s surveillance efforts.
23 H.R. Rep. No. 103-827, pt. 1, at 14. Congress nonetheless deliberately chose not to
24 interfere with those technologies, because one of its goals was to “protect[] the
25 privacy of communications . . . without impeding the introduction of new
26 technologies, features, and services.” *Id.* at 9. Indeed, the House Report makes clear
27 that, because Congress wanted to “protect[] the right to use encryption,” nothing in
28 CALEA “would prohibit a carrier from deploying an encryption service for which it

1 does not retain the ability to decrypt communications for law enforcement access.”
2 *Id.* at 24. Apple deployed precisely such an encryption service on the iPhone, and
3 CALEA imposes no obligation on Apple to assist in defeating that encryption.

4 The legislative history also shows that the FBI was fully aware of CALEA’s
5 limitations. During the hearings that led to CALEA’s passage, then-FBI director
6 Louis Freeh told Senator Leahy that the government had elected not to seek authority
7 to compel third-party companies to decrypt devices:

8 Mr. FREEH. . . . We are not looking to introduce any
9 feature package that impedes technology. And, interestingly
10 enough, last Friday I sat in my building with 38
11 representatives of the industry, telecommunications
12 companies, and we asked them. We said give us one
13 example of a technological advancement or improvement
14 which you believe this feature package would inhibit. And
15 there was complete silence in the room.

16 Senator LEAHY. I might suggest one: A private company
17 that wants to build a computer, fax machine, telephone or
18 whatever that is encrypted.

19 Mr. FREEH. Well, but that is a different problem. We are
20 never asking the phone companies and this legislation does
21 not ask them to decrypt. It just tells them to give us the bits
22 as they have them. If they are [en]rypted, that is my
23 problem. But that is not going to be addressed in the
24 legislation.⁷

25 **B. The Government Cannot Use The All Writs Act To Circumvent**
26 **CALEA**

27 The government contends that, while CALEA’s express language does not
28 permit the relief it seeks, CALEA does not occupy the field and is silent on whether it
can order a technology company to weaken the security of its technology products.

29 _____
30 ⁷ *Digital Telephony and Law Enforcement Access to Advanced Telecommunica-*
31 *tions Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the*
32 *S. Subcomm. On Technology and the Law of the S. Comm. on the Judiciary and the*
33 *H. Subcomm. On Civil and Constitutional Rights of the H. Comm. on the Judiciary,*
34 *103rd Cong. 11 (1994) (testimony of FBI Director Louis J. Freeh).*

1 As a result, the government believes it can rely on the All Writs Act to provide the
2 requisite authority. But the fact that Congress chose *not* to grant certain authority to
3 the government in CALEA does not mean that Congress has not addressed the issue.
4 Given that Congress specifically considered granting, and ultimately declined to
5 grant, the authority the government seeks, resort to the All Writs Act is misplaced. In
6 light of Congress's considered decision in CALEA not to convey the authority that
7 the government seeks here, the government's reliance on the All Writs Act is an
8 attempted end-run around the legislative process.

9 In a recent opinion addressing a government demand to unlock an iPhone, a
10 magistrate judge squarely rejected the government's attempt to rely on the All Writs
11 Act. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search*
12 *Warrant Issued By This Court*, 2016 WL 783565, Misc. No. 15-1902 (E.D.N.Y. Feb.
13 29, 2016) (*Apple Order*). In that case, the court first examined CALEA, along with
14 other federal statutes, and reasoned that "[t]he absence from that comprehensive
15 scheme of any requirement that Apple provide the assistance sought here implies a
16 legislative decision to prohibit the imposition of such a duty." *Id.* at 20. The court
17 then explained that, even if CALEA "does not erect such a barrier to relief on its own
18 terms," *id.* at 21, the All Writs Act still "cannot be a means for the executive branch
19 to achieve a legislative goal that Congress has considered and rejected," *id.* at 26.
20 The court explained the stunningly broad implications of the government's view of
21 the All Writs Act:

22 [The government's] preferred reading of the law—which
23 allows a court to confer on the executive branch any
24 investigative authority Congress has decided to withhold, so
25 long as it has not affirmatively outlawed it—would
26 transform the [All Writs Act] from a limited gap-filling
27 statute that ensures the smooth functioning of the judiciary
28 itself into a mechanism for upending the separation of
powers by delegating to the judiciary a legislative power
bounded only by Congress's superior ability to prohibit or
preempt.

1 *Id.* The court also recognized that the government’s use of the All Writs Act was a
2 transparent attempt to circumvent the legislative process: “It is also clear that the
3 government has made the considered decision that it is better off securing such
4 crypto-legislative authority from the courts . . . rather than taking the chance that
5 open legislative debate might produce a result less to its liking.” *Id.* at 29.

6 Similarly, in *In re Application of U.S. For An Order*, 849 F. Supp. 2d 526 (D.
7 Md. 2011), a district court rejected the FBI’s attempt to invoke the All Writs Act to
8 obtain real-time GPS location data from a suspected criminal’s cellphone, concluding
9 that “[t]he government simply cannot use the All Writs Act to circumvent . . . statutes
10 that already occupy the space.” *Id.* at 583. The court explained that the attempted
11 use of the All Writs Act “may be the most troubling position the government has
12 taken in pursuit of this precise location data,” because “the government seeks an end
13 run around constitutional and statutory law.” *Id.* at 578. As the court reasoned, “the
14 government appears to see the All Writs Act as an alternative source of inherent
15 authority, rather than a limited, residual one.” *Id.* at 579; *see also In re Application of*
16 *the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace*
17 *Device*, 396 F. Supp. 2d 294, 326 (E.D.N.Y. 2005) (declining to “read into the All
18 Writs Act an empowerment of the judiciary to grant the executive branch authority to
19 use investigative techniques either explicitly denied it by the legislative branch, or at
20 a minimum omitted from a far-reaching and detailed statutory scheme”).

21 *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), relied on
22 heavily by the government, does not require a different result and only highlights the
23 absence of support for the government’s broad view of the All Writs Act. According
24 to the government, “*New York Telephone Co.* further illustrates that it is appropriate
25 for a court to rely on the All Writs Act unless a statute specifically addresses the
26 particular issue at hand.” Gov’t Mem. 23 [ECF #1]. But the government fails to
27 mention that, in *New York Telephone*, the Supreme Court repeatedly explained that
28 the use of the All Writs Act as a gap-filler was appropriate only insofar as it “was

1 consistent with the intent of Congress.” 434 U.S. at 172. The issue in *New York*
2 *Telephone* was whether the government could compel a telecommunications carrier
3 to provide assistance in installing pen registers, which are mechanical devices used to
4 intercept the numbers dialed on a telephone but not the content of the oral
5 communications. *Id.* at 161 n.1. Although no statute expressly required the carriers
6 to provide the FBI with technical assistance, the Court afforded that authority to the
7 government under the All Writs Act because “Congress clearly intended to permit the
8 use of pen registers by federal law enforcement officials.” *Id.* at 176. The Court
9 reasoned that “Congress did not view pen registers as posing a threat to privacy of the
10 same dimension as the interception of oral communications.” *Id.* at 168. This case
11 presents the opposite situation. CALEA reflects Congress’s intent *not* to confer the
12 requested authority on the government. *Apple Order 20. New York Telephone*
13 undermines, not supports, the government’s position.

14 In sum, given the abundant evidence from the text and legislative history of
15 Congress’s intent, the government’s invocation of the All Writs Act is improper.
16 This Court should reject the government’s sweeping and indefensible interpretation
17 of the All Writs Act and grant Apple’s motion.⁸

18 **III. GRANTING THE GOVERNMENT’S PROPOSED RELIEF WOULD** 19 **ESTABLISH A DANGEROUS PRECEDENT**

20 The issue before this Court has far-reaching policy implications. If the
21 government’s proposed interpretation of the All Writs Act were correct, there is no

22
23 ⁸ The government’s overreaching on the All Writs Act provides a sufficient basis
24 to adjudicate this case and grant Apple’s requested relief. It bears noting, however,
25 that an order forcing a company to create code to undermine the security features of
26 its products also potentially runs afoul of the First Amendment and raises due process
27 concerns. *See, e.g., Riley v. First National Fed. of the Blind of N.C., Inc.*, 487 U.S.
28 781, 796-97 (1988) (explaining that compelled speech restricts content and is subject
to rigorous scrutiny); *Cty. of Sacramento v. Lewis*, 523 U.S. 833, 845 (1998) (recog-
nizing that “[t]he touchstone of due process is protection . . . against arbitrary action
of government”).

1 logical reason why the government’s authority would be limited to Apple or iPhones;
2 the Act could also be used to require Intel and other technology companies to comply
3 with similar requests. It would establish a precedent for other courts, law-
4 enforcement agencies, and foreign governments. Forcing companies to create
5 technology to bypass security features would only weaken security and stifle
6 innovation. Because of the importance of these policy choices—for privacy rights
7 and security—they should be decided after public debate and deliberation; they
8 should not be decided by resort to the All Writs Act, an ancillary source of judicial
9 authority.

10 **A. Intel And Other Companies Are Likely Targets of Similar Demands**

11 Because Intel designs, manufactures, and distributes a wide variety of
12 technologies—including the chips in devices ranging from servers to wearables, as
13 well as software and services that are focused on security—it is likely to be
14 profoundly affected by the precedent that this Court sets. Intel’s products include
15 microprocessors used in a large number of the world’s computers. Microprocessors
16 are the primary computing “engine” in today’s computers; in many cases, it is Intel’s
17 chips that actually perform encryption and decryption. Many of Intel’s chips are
18 designed with features to facilitate encryption and to allow encryption to be used
19 more securely and in new ways. In addition, Intel is a leading developer and seller of
20 computer security software and services.

21 If the Court forces Apple to develop new software to help the government
22 break the security features that Apple designed into its iPhone, developers of
23 hardware components such as Intel may be subject to similar orders demanding that
24 they devote engineering resources to defeating the security features of their own
25 products. The government could also ask Intel to develop or enable technology that
26 would provide access to computers with Intel software installed on them.

27 Similarly, the government could enlist Intel to assist the government in its own
28 effort to defeat those security features. For example, it could require Intel to “sign”

1 the government’s own software. It is now commonplace for software updates to be
2 “cryptographically sign[ed].” *See* Neuenschwander Decl. ¶ 18, 27 [ECF #16-33].
3 Cryptographic signing is a technology—based on encryption technology—that can be
4 used to ensure that code or data can only be modified by an authorized user. That
5 technology, in turn, is used to ensure that software—for example, software updates—
6 are legitimate products of their purported manufacturers, and not counterfeits that
7 have been modified to contain malicious code. *See id.* Cryptographic signing is thus
8 crucial to computer security in the modern world. The authority the government is
9 seeking here raises the specter that the government will force Intel or other
10 manufacturers to “sign” software updates the government has created.

11 Given the scope of Intel’s products and services and its focus on security, it is
12 likely that a ruling in the government’s favor on its demand against Apple would lead
13 to similar demands against Intel and other technology companies.

14 **B. Granting The Government’s Proposed Relief Would Create**
15 **Precedent For Other Courts, Law-Enforcement Agencies, And**
16 **Foreign Governments**

17 If the Court accepts the government’s expanded view that it has the power to
18 command Apple to undermine the security of its products, it will set a legal precedent
19 that could have far-reaching consequences, both in the United States and beyond. As
20 Apple notes in its motion, law-enforcement officials across the United States have
21 already sought assistance from Apple in many other cases. *See* Apple Mot. 3 [ECF
22 16]. Indeed, the government has acknowledged that this Court’s decision will set a
23 precedent that will be “instructive for other courts.”⁹

24 A ruling in the government’s favor will have global ramifications as well. Like
25 Apple, Intel has operations in numerous countries, and it is subject to differing laws
26 and regulations worldwide. Foreign countries—particularly those with laws less

27
28 ⁹ Karoun Demirjian, *Apple Case Creates Fervor For Encryption Bill In Congress*,
Wash. Post (Feb. 25, 2016) <goo.gl/eH2U4C> (quoting FBI Director Comey).

1 protective of privacy interests than the United States—might view a ruling in the
2 government’s favor as an invitation to require technology companies such as Intel to
3 undermine the security of their products to suit foreign government interests. Indeed,
4 foreign governments have already made onerous demands on technology companies
5 to obtain data for law-enforcement purposes.¹⁰

6 **C. The Government’s Proposed Relief Raises Important Issues That**
7 **Should Be Addressed Through Vigorous Public Debate**

8 Intel’s fundamental position is that technology companies should not be forced
9 to undermine the security technology they have strived to create. Intel is in the
10 business of improving the security of its technology products, not defeating it. The
11 government should not interfere with Intel’s ability to protect the privacy and security
12 of its customers. While law-enforcement and national-security agencies have a
13 critical mission, no company should be compelled to weaken the security of its
14 products in pursuit of that mission. The government’s attempt to undermine the
15 security of technology products in order to meet its law-enforcement objectives raises
16 profound policy issues. Those issues should be discussed and debated through the
17 democratic process, with consultation involving industry and other affected
18 stakeholders.

19 As matters currently stand, however, the government does not have the
20 authority to force a company to develop technology for the purpose of circumventing
21 the security features of its products. Congress deliberately chose not to confer that
22 authority in CALEA, and the government may not use the All Writs Act to
23 circumvent Congress’s considered judgment. Apple’s motion to vacate should
24 therefore be granted.

25 _____
26 ¹⁰ See, e.g., Paul Mozur, *New Rules in China Upset Western Tech Companies*,
27 N.Y. Times (Jan. 28, 2015) <goo.gl/GZd6eA> (discussing Chinese regulations “re-
28 quiring companies that sell computer equipment to Chinese banks to turn over secret
source code, submit to invasive audits and build so-called back doors into hardware
and software”).

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

CONCLUSION

For the foregoing reasons, Intel respectfully requests that Apple's motion to vacate be granted.

Respectfully submitted,

By: *Daniel F. Katz*

Daniel F. Katz*
Kannon K. Shanmugam*
Richmond T. Moore*
David M. Krinsky*
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Telephone: (202) 434-5000
Facsimile: (202) 434-5029

William Faulkner (SBN 83385)
MCMANIS FAULKNER
One California Plaza
300 South Grand Avenue, 37th Floor
Los Angeles, CA 90071
Telephone: (408) 279-8700
Facsimile: (408) 279-3244

Darren B. Bernhard*
Vice President and Director of
Antitrust & Commercial Litigation
INTEL CORPORATION
1155 F Street, N.W.
Washington, DC 20004
Telephone: (202) 626-4380

Tanya L. Hunter (SBN 197761)
INTEL CORPORATION
2200 Mission College Boulevard
Santa Clara, CA 95054
Telephone: (408) 765-2318
Facsimile: (408) 765-5157

**Pro Hac Vice Admission Pending*

Attorneys for Intel Corporation

CERTIFICATE OF SERVICE

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

I, Olivia Spaulding, declare as follows:

I am employed in the County of Riverside, California; I am over the age of 18 years and am not a party to this action. My business address is Bosco Legal Services, Inc., 4651 Brookhollow Circle, Suite C, Riverside, CA 92509. On March 3, 2016, I served the foregoing Motion of Intel Corporation for Leave to File Brief of Amicus Curiae and its attachments on the parties stated below, by placing them in a sealed envelope with postage thereon fully prepaid for delivery to the following:

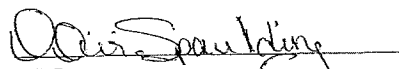
Theodore J. Boutrous, Jr.
Nicola T. Hanna
Eric D. Vandeveld
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071

Theodore B. Olson
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036

Marc J. Zwillinger
Jeffrey G. Landis
ZWILLGEN PLLC
1900 M Street N.W., Suite 250
Washington, DC 20036

Eileen M. Decker
United States Attorney
Patricia A. Donahue
Assistant United States Attorney
Chief, National Security Division
Tracy L. Wilkinson
Assistant United States Attorney
Chief, Cyber and Intellectual Property
Crimes Section
Allen W. Chiu
Assistant United States Attorney
Terrorism and Export Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, CA 90012

This certificate is executed on March 3, 2016, in Riverside, California. I certify under penalty of perjury that the foregoing is true and correct.


Name: Olivia Spaulding

ORIGINAL

LODGED

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


Daniel F. Katz*
dkatz@wc.com
Kannon K. Shanmugam*
kshanmugam@wc.com
Richmond T. Moore*
rtmoore@wc.com
David M. Krinsky*
dkrinsky@wc.com
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Telephone: (202) 434-5000
Facsimile: (202) 434-5029

William Faulkner (SBN 83385)
wfaulkner@mcmanslaw.com
MCMANIS FAULKNER
One California Plaza
300 So. Grand Avenue, 37th Floor
Los Angeles, CA 90071
Telephone: (408) 279-8700
Facsimile: (408) 279-3244

**Pro Hac Vice Admission Pending*
Attorneys for Intel Corporation

Darren B. Bernhard*
darren.b.bernhard@intel.com
Vice President
Director of Antitrust &
Commercial Litigation
INTEL CORPORATION
1155 F Street, N.W.
Washington, DC 20004
Telephone: (202) 626-4380

Tanya L. Hunter (SBN 197761)
tanya.hunter@intel.com
Associate General Counsel
Antitrust & Commercial Litigation
INTEL CORPORATION
2200 Mission College Boulevard
Santa Clara, CA 95054
Telephone: (408) 765-2318
Facsimile: (408) 765-5157

2016 MAR -3 AM 11:20
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE
BY 

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

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

ED No. CM 16-10-SP

**CORPORATE DISCLOSURE
STATEMENT AND NOTICE OF
INTERESTED PARTIES**

Hearing:

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

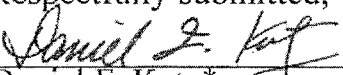
FILED BY FAX

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

Pursuant to Federal Rule of Civil Procedure 7.1, the undersigned, counsel for amicus Intel Corporation, certifies that Intel Corporation has no parent corporation, and no publicly held corporation owns 10 percent or more of its stock.

Pursuant to Local Rule 7.1-1, the undersigned further certifies that as of this date, Intel Corporation is not aware of any entities that may have a pecuniary interest in the outcome of this case, other than parties Apple Inc. and the United States of America. These representations are made to enable the Court to evaluate possible disqualification or recusal.

Dated: March 3, 2016

Respectfully submitted,
By: 
Daniel F. Katz*
Kannon K. Shanmugam*
Richmond T. Moore*
David M. Krinsky*
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Telephone: (202) 434-5000
Facsimile: (202) 434-5029

William Faulkner (SBN 83385)
MCMANIS FAULKNER
One California Plaza
300 So. Grand Avenue, 37th Floor
Los Angeles, CA 90071
Telephone: (408) 279-8700
Facsimile: (408) 279-3244

Darren B. Bernhard*
Vice President and Director of
Antitrust & Commercial Litigation
INTEL CORPORATION
1155 F Street, N.W.
Washington, DC 20004
Telephone: (202) 626-4380

Tanya L. Hunter (SBN 197761)
INTEL CORPORATION
2200 Mission College Blvd.
Santa Clara, CA 95054
Telephone: (408) 765-2318
Facsimile: (408) 765-5157

**Pro Hac Vice Admission Pending*
Attorneys for Intel Corporation

CERTIFICATE OF SERVICE

I, Olivia Spaulding, declare as follows:

I am employed in the County of Riverside, California; I am over the age of 18 years and am not a party to this action. My business address is Bosco Legal Services, Inc., 4651 Brookhollow Circle, Suite C, Riverside, CA 92509. On March 3, 2016, I served the foregoing Corporate Disclosure Statement and Notice of Interested Parties on the parties stated below, by placing it the United States Postal Service in a sealed envelope with postage thereon fully prepaid, addressed as follows:

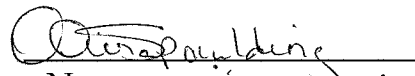
Theodore J. Boutrous, Jr.
Nicola T. Hanna
Eric D. Vandavelde
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071

Eileen M. Decker
UNITED STATES ATTORNEY
Patricia A. Donahue
Assistant United States Attorney
Chief, National Security Division
Tracy L. Wilkinson
Assistant United States Attorney
Chief, Cyber and Intellectual Property
Crimes Section
Allen W. Chiu
Assistant United States Attorney
Terrorism and Export Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012

Theodore B. Olson
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036

Marc J. Zwillinger
Jeffrey G. Landis
ZWILLGEN PLLC
1900 M Street N.W., Suite 250
Washington, DC 20036

This certificate is executed on March 3, 2016, in Riverside, California. I certify under penalty of perjury that the foregoing is true and correct.


Name: Olivia Spaulding