

1 Marcia Hofmann (Cal. Bar No. 250087)
2 Zeitgeist Law PC
25 Taylor Street
3 San Francisco, CA 94102
4 Telephone: (415) 830-6664
marcia@zeitgeist.law
5

6 Attorney for Amici Curiae
7 Access Now and Wickr Foundation
8

9 **UNITED STATES DISTRICT COURT**
10 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**
11 **EASTERN DIVISION**

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

Case No. 5:16-cm-00010-SP-1

**BRIEF OF AMICI CURIAE
ACCESS NOW AND WICKR
FOUNDATION IN SUPPORT OF
APPLE INC.'S MOTION TO
VACATE**

Date: March 22, 2016

Time: 1:00 p.m.

Place: Courtroom 3 or 4, 3rd Floor

Judge: Honorable 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

- INTEREST OF AMICI CURIAE..... 1
- SUMMARY OF THE ARGUMENT 2
- ARGUMENT..... 3
 - I. Ordering Apple to Weaken the Security of the Subject iPhone Will Have the Unintended Consequence of Generally Undermining Digital Security..... 3
 - II. Deliberately Weakening Digital Security Contravenes International Human Rights Law..... 6
 - A. Encryption Is Central to the Exercise of Human Rights in the Digital Age, Which International Law Requires the United States to Uphold..... 6
 - B. Apple’s Efforts to Protect the Privacy and Security of Users Align With International Norms on Business and Human Rights 11
 - III. The Government’s Request Will Endanger Users Around the World..... 13
- CONCLUSION..... 18

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

FEDERAL CASES

Kennedy v. Mendoza-Martinez,
372 U.S. 144 (1963) 8

Lawrence v. Texas,
539 U.S. 558 (2003) 8

Roper v. Simmons,
543 U.S. 551 (2005) 8

The Paquete Habana,
175 U.S. 677 (1900) 7

United States v. Machain,
504 U.S. 655 (1992) 8

STATE CASES

Boehm v. Superior Court,
178 Cal. App. 3d 494 (Cal. Ct. App. 1986) 8

People v. Levins Justice Newman,
22 Cal. 3d 620 (Cal. 1978) 8

Santa Barbara v. Adamson,
27 Cal. 3d 123 (Cal. 1980) 8

Sei Fuji v. California,
38 Cal. 2d 718 (Cal. 1952) 7

FEDERAL STATUTES

28 U.S.C. § 1651(a) 6

CONSTITUTIONAL PROVISIONS

U.S. Const. art. VI 7

OTHER AUTHORITIES

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

Access Now, *Digital Security Helpline*, <https://www.accessnow.org/digital-security-helpline>..... 15

Am. Bar Ass’n, Resolution 109 (Feb. 2012)..... 12

Arch Puddington and Tyler Roylance, Freedom House, Freedom in the World (2016)..... 14

Bruce Schneier, *Decrypting an iPhone for the FBI*, Schneier on Security (Feb. 22, 2016)..... 4

Bruce Schneier, *Decrypting an iPhone for the FBI*, Schneier on Security (Feb. 22, 2016), https://www.schneier.com/blog/archives/2016/02/decrypting_an_i.html..... 4

California Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013)..... 5

Charlie Rose, Television Interview of Cyrus Vance (Feb. 18, 2016) 4

Christopher Soghoian, *The Technology at the Heart of the Apple-FBI Debate, Explained*, WASHINGTON POST (Feb. 29, 2016) 5

Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 (1994)..... 10

Dep’t of Homeland Security, *Understanding Mobile Apps*, OnGuardOnline.gov (Sept. 2011)..... 5

Department of State, *Internet Freedom*, <http://www.state.gov/e/eb/cip/netfreedom/index.htm> 7

Fed. Trade Comm., *Mobile App Developers: Start With Security* (Feb. 2013) 5

Guiding Principles on Business and Human Rights: Implementing the Protect, Respect, and Remedy Framework, U.N. Doc. HR/PUB/11/04 (2011)..... 11, 12

Human Rights Committee, General Comment 16 (23rd Sess. 1988) 10

Human Rights Committee, General Comment 27, Freedom of Movement (Art. 12), U.N. Doc CCPR/C/21/Rev.1/Add.9 (1999) 10

1 Human Rights Council Res. 26/13, The Promotion, Protection and Enjoyment of
Human Rights on the Internet, U.N. Doc. A/HRC/RES/26/13 (June 29, 2012) 8

2

3 Human Rights Council, Human Rights and Transnational Corporations and Other
Business Enterprises, U.N. Doc. A/HRC/RES/17/4 (July 6, 2011)..... 12

4

5 Human Rights Council, Report of the Special Rapporteur on the Promotion and
Protection of the Right to Freedom of Opinion and Expression, David Kaye,
6 U.N. Doc.A/HRC/29/32 (May 22, 2015)9, 11, 14

7 Human Rights Council, Report of the Special Rapporteur on the Promotion and
8 Protection of the Right to Freedom of Opinion and Expression, Frank La Rue,
9 U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) 9

10 Human Rights Watch, *“They Know Everything We Do”: Telecom and Internet Surveillance in
Ethiopia* (March 25, 2014) 14

11

12 International Covenant on Civil and Political Rights. Dec. 16, 1966, S. Treaty Doc. No.
95-20, 6 I.L.M. 368, 999 U.N.T.S. 1717, 8, 10

13

14 International Principles on the Application of Human Rights to Communications
15 Surveillance (2013) 10

16 Iulia Ion, Rob Reeder, and Sunny Consolvo, Google, *New Research: Comparing How
Security Experts and Non-Experts Stay Safe Online* (July 23, 2015) 5

17

18 Jason McGahan, *She Tweeted Against the Mexican Cartels, They Tweeted Her Murder*, The
19 Daily Beat (Oct. 21, 2014)..... 17

20 Melanie Nathan, *Ugandan Communications Commission threatened to Arrest Citizens for using
Social Media*, O-blog-dee-o-blog-da (Feb. 19, 2016) 17

21

22 Org. for Econ. & Coop. Dev., Guidelines for Multinational Enterprises (2012) 12

23 Robert Graham (@ErrataRob), Twitter (Feb. 17, 2016, 11:52 AM),
24 <https://twitter.com/ErrataRob/status/699999978165530624> 4

25 Security in-a-Box, *Tools and Tactics for the LGBTI Community in the Middle-East and North
26 Africa*, <https://securityinabox.org/en/lgbti-mena> 17

27 The Federalist No. 43 (1788) (Alexander Hamilton)..... 6

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

Universal Declaration of Human Rights, G.A. Res. 217 A, U.N. GAOR (Dec. 10, 1948) 7, 8

U.S. Reservations, Declarations, and Understandings, International Covenant on Civil and Political Rights, 138 Cong. Rec. S4781-01 (daily ed. April 2, 1992..... 7

Wickr Foundation, *Education and Training*, <https://www.wickr.org/edu-programs>..... 15

INTEREST OF AMICI CURIAE

1
2 Access Now is a global civil society organization, founded in 2009 as a California
3 non-profit corporation, dedicated to defending and extending the digital rights of users
4 at risk around the world. With offices in ten countries, Access Now provides thought
5 leadership, policy recommendations, and technology advice to the public and private
6 sectors to ensure the internet's continued openness and universality. Access Now leads
7 an action-focused global community of over two hundred thousand users from more
8 than 185 countries. Access Now is particularly concerned with defending the lawful use
9 and integrity of encryption and secure communications technologies, the unencumbered
10 exercise of which is crucial for the exercise of freedom of speech in the digital age.
11

12
13
14 Wickr Foundation is a non-profit organization dedicated to supporting a strong
15 free society by championing private communications and uncensored access to
16 information. The key mission of Wickr Foundation is to provide education, digital
17 security and privacy tools for at-risk populations underserved by commercial markets.
18 The Foundation operates educational and public awareness programs for policy-makers,
19 youth, journalists, and human rights organizations. Wickr Foundation was launched by
20 Wickr Inc., a communication platform that enables anyone in the world to
21 communicate freely, privately, and securely.¹
22
23

24
25
26
27
28

¹ Pursuant to Federal Rule of Appellate Procedure 29(c)(5), amici state that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting the brief; and no person—other than amici, their members, or their counsel—contributed money that was intended to fund preparing or submitting the brief.

SUMMARY OF THE ARGUMENT

1
2 The government insists that this case is about a single iPhone, and that the
3 software solution it wants Apple to create will do nothing to weaken encryption. In
4 reality, this case could set precedent for law enforcement to demand that any
5 technology company impair the security of its products or services, and has potential to
6 do far-reaching harm.
7

8 Deliberately compromised digital security would undermine human rights around
9 the globe. Pursuant to international law, the United States has a duty to foster basic
10 human rights such as freedom of expression and privacy. The assistance sought by the
11 government not only diminishes the commitment of the United States to uphold those
12 fundamental rights in the digital age, but also keeps Apple from fulfilling its own
13 responsibilities to respect the human rights of users.
14

15
16 Technology and connectivity have empowered millions around the world to
17 demand social and political change—but criminals and authoritarian regimes exploit the
18 same technology to identify and persecute protesters, democracy activists, bloggers, and
19 journalists. In some countries, reliable security tools such as encryption can be the
20 difference between life and death. The relief sought by the government endangers
21 people globally who depend on robust digital security for their physical safety and
22 wellbeing.
23
24
25
26
27
28

ARGUMENT

I. Ordering Apple to Weaken the Security of the Subject iPhone Will Have the Unintended Consequence of Generally Undermining Digital Security

On February 16, 2016, upon the *ex parte* application of the government, Magistrate Judge Sheri Pym issued an order pursuant to the All Writs Act compelling Apple, Inc. to develop and sign a modified version of the iPhone operating system (“GovtOS”) that bypasses security features fundamental to protecting encrypted information on Apple’s mobile devices. Order Compelling Apple Inc. to Assist Agents in Search, ED No. 15-0451M, slip op. at 2 (C.D. Cal. Feb. 16, 2016). In essence, the government asked this Court to conscript Apple into service to make it easier for the FBI to brute-force into a user’s device by guessing the user’s passcode, which would decrypt user data. Memorandum of Points and Authorities in Support of Government’s *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search (“Gov. App.”) (ED-0451M).

The government claims that the software solution it wants “does nothing regarding the encryption aspect of the operating software, but instead implicates only the non-encryption additional features that Apple has programmed.” Gov. App. at 20. Despite this artful framing, the FBI seeks to compromise these additional features for the sole purpose of decrypting information on the phone. If encryption represents the lock on the door of an iPhone, the FBI essentially wants Apple to remove the door’s hinges. Once Apple’s security features are bypassed, one security expert estimates that a

1 standard four-digit numeric passcode could be guessed in about 13 minutes, and a six-
2 digit passcode in less than a day. Robert Graham (@ErrataRob), Twitter (Feb. 17, 2016,
3 11:52 AM), <https://twitter.com/ErrataRob/status/699999978165530624>.

4
5 While the government insists that GovtOS would be limited to this one phone,
6 Gov. App. at 7, realistically the modified operation system can be deployed again and
7 again to help the government access data on iPhones in a wide range of investigations.
8 As world-renowned technologist Bruce Schneier explains, “[T]he hacked software the
9 court and the FBI wants Apple to provide . . . would work on any phone of the same
10 model. It has to. Make no mistake; this is what a backdoor looks like.” Bruce Schneier,
11 *Decrypting an iPhone for the FBI*, Schneier on Security (Feb. 22, 2016).² Manhattan District
12 Attorney Cyrus Vance confirmed in an interview about this very matter that he
13 “absolutely” “want[s] access to all those phones that [he thinks] are crucial in a criminal
14 proceeding.” Charlie Rose, Television Interview of Cyrus Vance (Feb. 18, 2016).³

15
16
17
18 The unintended consequences of compelling Apple to provide the assistance
19 sought by the government will extend far beyond iPhones. If Apple is forced to develop
20 GovOS, there is no reason why other technology companies could not be compelled by
21 the courts to impair their security features in various ways, as well. And other
22 companies—particularly smaller and newer ones—may decide that the benefits of
23 building robust security into their products do not outweigh the costs associated with
24 later being required by the courts to enfeeble those efforts, which will incentivize them
25
26

27
28 ² https://www.schneier.com/blog/archives/2016/02/decrypting_an_i.html.

³ <http://www.charlierose.com/watch/60689812>.

1 to create less secure products in the first place.⁴

2 This Order will also have the side effect of diminishing consumer trust in
3 technology. Indeed, the government's actions in this case have already raised suspicions
4 about automatic system updates and patches that are necessary to fix known flaws.
5 Christopher Soghoian, *The Technology at the Heart of the Apple-FBI Debate, Explained*,
6 WASHINGTON POST (Feb. 29, 2016) (“If consumers fear that the software updates . . .
7 might secretly contain surveillance software from the FBI, many of them are likely to
8 disable those automatic updates”).⁵ Automatic updates are one of the most vital ways to
9 keep technology secure, according to security experts; they “are the seatbelts of online
10 security; they make you safer, period.” Iulia Ion, Rob Reeder, and Sunny Consolvo,
11 Google, *New Research: Comparing How Security Experts and Non-Experts Stay Safe Online*
12 (July 23, 2015).⁶ If consumers are unwilling to accept updates that make their
13 technology safer to use because of fear of surveillance, they will be at substantially
14 greater risk.

19 _____
20 ⁴ It is worth noting that the assistance demanded by the government is at cross-
21 purposes with guidance from other sectors of state and federal government that
22 strongly encourage the use of strong security measures to protect consumers' sensitive
23 mobile data. See Fed. Trade Comm., *Mobile App Developers: Start With Security* (Feb. 2013),
24 [https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-
25 start-security](https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security); California Attorney General, *Privacy on the Go: Recommendations for the Mobile
26 Ecosystem* (Jan. 2013), [http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/
27 privacy_on_the_go.pdf](http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf); Dep't of Homeland Security, *Understanding Mobile Apps*,
28 OnGuardOnline.gov (Sept. 2011), [https://www.onguardonline.gov/articles/0018-
understanding-mobile-apps](https://www.onguardonline.gov/articles/0018-understanding-mobile-apps).

⁵ [https://www.washingtonpost.com/news/the-switch/wp/2016/02/29/the-
technology-at-the-heart-of-the-apple-fbi-debate-explained](https://www.washingtonpost.com/news/the-switch/wp/2016/02/29/the-technology-at-the-heart-of-the-apple-fbi-debate-explained).

⁶ [https://googleonlinesecurity.blogspot.com/2015/07/new-research-comparing-how-
security.html](https://googleonlinesecurity.blogspot.com/2015/07/new-research-comparing-how-security.html).

1 **II. Deliberately Weakening Digital Security Contravenes International**
2 **Human Rights Law**

3 The All Writs Act empowers a court to issue an order that is “agreeable to the
4 usages and principles of law.” 28 U.S.C. § 1651(a). International human rights law is one
5 of the sources of authority the Court may consider when deciding whether such an
6 order is appropriate. GovtOS would undermine internationally protected human rights
7 such as privacy and freedom of expression, but the United States government and
8 Apple are obligated to uphold those rights. Thus, international human rights law weighs
9 against forcing Apple to create GovtOS.
10
11

12 **A. Encryption Is Central to the Exercise of Human Rights in the**
13 **Digital Age, Which International Law Requires the United States to**
14 **Uphold**
15

16 Even in a time of rapid technological development, the fundamental principles
17 on which our nation was founded remain the same: “the rights of humanity must in all
18 cases be duly and mutually respected.” The Federalist No. 43 (1788) (Alexander
19 Hamilton).⁷ Digital security is central to the exercise of those rights in the modern age.
20 Because this case raises profound questions about human rights to privacy and free
21 expression in the digital era, it is particularly appropriate for the Court to consider
22 guidance from international human rights law.
23
24
25
26
27

28 ⁷ http://thomas.loc.gov/home/histdox/fed_43.html.

1 The United States has a longstanding commitment to human rights. Nearly 70
2 years ago, it played a key role in helping the United Nations to shape the Universal
3 Declaration of Human Rights, which established a basic list of rights that should be
4 universally protected. Universal Declaration of Human Rights, G.A. Res. 217 A, U.N.
5 GAOR (Dec. 10, 1948) (“UDHR”).⁸ The United States continued to support a strong
6 framework for global human rights by signing and ratifying the International Covenant
7 on Civil and Political Rights. Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368, 999
8 U.N.T.S. 171 (“ICCPR”).⁹

11 More recently, the United States has recognized the importance of internet
12 technology to the advancement of human rights around the world, and has committed
13 to “ensur[ing] that any child, born anywhere in the world, has access to the global
14 Internet as an open platform on which to . . . express herself free from undue
15 interference or censorship.” Department of State, *Internet Freedom*,
16 <http://www.state.gov/e/eb/cip/netfreedom/index.htm> (last visited Feb. 29, 2016).¹⁰

19 Treaties like the ICCPR are part of the “supreme law of the land.” U.S. Const.
20 art. VI, para. 2. And indeed, “International law is part of our law.” *The Paquete Habana*,
21 175 U.S. 677, 700 (1900). While neither the Universal Declaration of Human Rights nor
22 the ICCPR is a self-executing instrument,¹¹ the “humane and enlightened objectives of
23
24

25 ⁸ <http://www.un.org/en/universal-declaration-human-rights/index.html>.

26 ⁹ https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&lang=en.

27 ¹⁰ <http://www.state.gov/e/eb/cip/netfreedom/index.htm>.

28 ¹¹ See U.S. Reservations, Declarations, and Understandings, International Covenant on

1 the United Nations Charter” are “entitled to respectful consideration” by the courts. *Sei*
2 *Fuji v. California*, 38 Cal. 2d 718, 725 (Cal. 1952).

3 Courts often refer to international law to provide guidance when deciding
4 important cases concerning human rights. *See, e.g., Lawrence v. Texas*, 539 U.S. 558, 573 &
5 577 (2003) (citing precedent from the European Court of Human Rights and noting
6 “The right the petitioners seek in this case has been accepted as an integral part of
7 human freedom in many other countries”); *Roper v. Simmons*, 543 U.S. 551, 567 & 578
8 (2005) (citing to the ICCPR and discussing the “overwhelming weight of international
9 opinion” against capital punishment for juveniles); *see also United States v. Machain*, 504
10 U.S. 655, 666-68 (1992); *Kennedy v. Mendoza-Martinez*, 372 U.S. 144, 160-61 (1963).

11 In particular, California courts have relied on international human rights treaties
12 and charters to provide greater insight on laws and rights, including the right to privacy.
13 *Santa Barbara v. Adamson*, 27 Cal. 3d 123, 130 n.2 (Cal. 1980) (Manuel, J., dissenting)
14 (citing the right to privacy in the UDHR in discussion of nontraditional living
15 arrangements); *see also Boehm v. Superior Court*, 178 Cal. App. 3d 494, 502 (Cal. Ct. App.
16 1986); *People v. Levins Justice Newman*, 22 Cal. 3d 620, 625 (Cal. 1978) (Newman, J.,
17 concurring).

18 Both the UDHR and the ICCPR recognize the rights to freedom of expression,
19 association, religion, and privacy. *See* UDHR Arts. 2, 12, 18-20; ICCPR Arts. 17-19, 21-
20 22. The rights that exist offline must be protected online, as well. Human Rights
21

22
23
24
25
26
27
28 Civil and Political Rights, 138 Cong. Rec. S4781-01 (daily ed. April 2, 1992).

1 Council Res. 26/13, The Promotion, Protection and Enjoyment of Human Rights on
2 the Internet, U.N. Doc. A/HRC/RES/26/13 at 2 (June 29, 2012).

3 In the modern age, the security of digital communications is central to the ability
4 of users to freely exercise basic human rights that have long been recognized as
5 fundamental. According to the United Nations Special Rapporteur for Freedom of
6 Expression:
7

8 [A]n open and secure Internet should be counted among the leading
9 prerequisites for the enjoyment of the freedom of expression today. But it is
10 constantly under threat, a space—not unlike the physical world—in which
11 criminal enterprise, targeted repression and mass data collection also exist.
12 It is thus critical that individuals find ways to secure themselves online, that
13 Governments provide such safety in law and policy and that corporate
14 actors design, develop and market secure-by-default products and services.
15
16
17

18 Human Rights Council, Report of the Special Rapporteur on the Promotion and
19 Protection of the Right to Freedom of Opinion and Expression, David Kaye, U.N.
20 Doc.A/HRC/29/32 at 19 (May 22, 2015) (“Kaye Report”).¹² In the face of the serious
21 threats that individuals face online, “encryption and anonymity, and the security
22 concepts behind them, provide the privacy and security necessary for the exercise of the
23 right to freedom of opinion and expression in the digital age.” *Id.*; see also Human Rights
24 Council, Report of the Special Rapporteur on the Promotion and Protection of the
25
26
27

28 ¹² www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

1 Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc.
2 A/HRC/23/40 at 20 (Apr. 17, 2013).¹³

3 The State's interference with human rights must be limited to what is
4 "appropriate" to fulfill "a predominantly important legal interest that is necessary in a
5 democratic society." International Principles on the Application of Human Rights to
6 Communications Surveillance (2013) ("Necessary and Proportionate Principles"),¹⁴ *see*
7 *also* Human Rights Committee, General Comment 27, Freedom of Movement (Art. 12),
8 U.N. Doc CCPR/C/21/Rev.1/Add.9 at 3 (1999). Respect for human rights requires
9 recognition that "compromising security for State purposes almost always compromises
10 security more generally[.]" Necessary and Proportionate Principles. As a result, it is
11 inappropriate for States to "compel service providers or hardware or software vendors
12 to build surveillance or monitoring capability into their systems, or to collect or retain
13 particular information purely for State Communications Surveillance purposes." *Id.*

14 International law forbids a State from arbitrarily or unlawfully interfering with
15 privacy. ICCPR Art. 17; Human Rights Committee, General Comment 16 (23rd Sess.
16 1988); Compilation of General Comments and General Recommendations Adopted by
17 Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994). Yet the
18 government's line of reasoning would justify government interference so sweeping that
19 there is no certainty how much cooperation the government could compel from private
20
21
22
23
24
25

26
27 ¹³ [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/
Session23/A.HRC.23.40_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

28 ¹⁴ <https://necessaryandproportionate.org>.

1 parties in the future. *See* Motion to Vacate Order Compelling Apple Inc. to Assist
2 Agents in Search, and Opposition to Government’s Motion to Compel Assistance at 26
3 (ECF No. 16) (listing examples of compelled speech the government’s argument could
4 justify).
5

6 Encryption is at the core of mobile security, creating a “zone of privacy”
7 fundamental for billions of people using mobile devices throughout the world to
8 express themselves “without arbitrary and unlawful interference to attack.” Kaye Report
9 at 5. It is critical to protect the ability to develop and use encryption coequally with the
10 human rights that it fosters. *See* Kaye Report at 11.
11

12 **B. Apple’s Efforts to Protect the Privacy and Security of Users Align**
13 **With International Norms on Business and Human Rights**
14

15 Pursuant to international law, Apple has a responsibility to respect the rights to
16 privacy and freedom of expression of its users. While many human rights obligations
17 fall upon the State, human rights instruments recognize that businesses serve as
18 “specialized organs of society performing specialized functions” and are therefore
19 “required to comply with all applicable laws and human rights.” Guiding Principles on
20 Business and Human Rights: Implementing the Protect, Respect, and Remedy
21 Framework, U.N. Doc. HR/PUB/11/04 at 1 (2011) (“Guiding Principles”).¹⁵ Apple’s
22 decision to deploy strong security measures in its devices is in line with its corporate
23
24
25
26

27 _____
28 ¹⁵ [http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusiness
HR_EN.pdf](http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

1 human rights responsibilities—efforts which would be undermined if Apple is forced to
2 create GovtOS.

3 The Human Rights Council unanimously endorsed the Guiding Principles in
4 2011 via a resolution co-sponsored by the United States. Human Rights Council,
5 Human Rights and Transnational Corporations and Other Business Enterprises, U.N.
6 Doc. A/HRC/RES/17/4 (July 6, 2011). In conjunction with the Organization for
7 Economic Co-operation and Development’s guidance (“OECD Guidelines”), the
8 Guiding Principles serve as the foundational articulation of the human rights duties of
9 businesses, and they “enjoy widespread support from the public, private and civil
10 society sectors.” Am. Bar Ass’n, Resolution 109 (Feb. 2012).¹⁶

11 The relief sought by the government undermines Apple’s ability to fulfill its
12 human rights responsibilities as provided by these international instruments. Companies
13 must “know and show that they respect human rights” by clearly communicating their
14 human rights policy commitments and identifying, avoiding, and mitigating any adverse
15 impacts related to their products. Guiding Principles at 14 and 16. For their part,
16 “[s]tates should set out clearly the expectation that all business enterprises domiciled in
17 their territory and/or jurisdiction respect human rights through their operation.”
18 Guiding Principles at 2. The OECD Guidelines advise corporations to “take reasonable
19 measures to ensure the security of personal data that they collect, store, process, or
20 disseminate.” Org. for Econ. & Coop. Dev., Guidelines for Multinational Enterprises
21
22
23
24
25
26

27
28 ¹⁶ https://www.americanbar.org/content/dam/aba/administrative/human_rights/hod_midyear_109.authcheckdam.pdf.

1 (2012). Apple should not be forced by the Court to waive its responsibilities under
2 these instruments. As another magistrate judge recently noted while denying a
3 government application to compel Apple to assist in the search of an iPhone:

4 [I]t is entirely appropriate to take into account the extent to which the
5 compromise of privacy and data security that Apple promises its customers
6 affects not only its financial bottom line, but also its decisions about the
7 kind of corporation it aspires to be. The fact that the government or a judge
8 might disapprove of Apple's preference to safeguard data security and
9 consumer privacy over the stated needs of a law enforcement agency is of
10 no moment: in the absence of any other legal constraint, that choice is
11 Apple's to make[.]
12
13
14

15 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This*
16 *Court*, No. 15-MC-1902 (JO), slip op. at 39 n.34 (E.D.N.Y. Feb. 29, 2016). While
17 effective law enforcement is an important interest, the United States government and
18 domestic companies must respect basic human rights such as freedom of expression
19 and privacy, for which strong encryption is foundational. The government's actions
20 here fail to uphold those essential rights, and also keep Apple from fulfilling its
21 responsibilities to do the same.
22
23

24 **III. The Government's Request Will Endanger Users Around the World**

25 While the government argues that the assistance it seeks from Apple is particular
26 to a single phone, the implications of building GovtOS are global. Substantial portions
27
28

1 of the world's population still live under oppressive regimes lacking basic human rights.
2 Arch Puddington and Tyler Roylance, Freedom House, *Freedom in the World* 12-13
3 (2016).¹⁷ Technology and expanded connectivity have empowered millions around the
4 world to demand social and political change. But the same technology can be exploited
5 to identify and persecute protesters, democracy activists, bloggers, and journalists.
6 Surveillance capabilities that were once available only to sophisticated attackers are now
7 routinely used by criminals and authoritarian regimes. *See, e.g.*, Human Rights Watch,
8 "They Know Everything We Do": *Telecom and Internet Surveillance in Ethiopia* (March 25,
9 2014).¹⁸ Even the most experienced users may unintentionally leak sensitive information
10 by using mobile devices and consumer applications that continuously collect user data
11 and are prone to leaks and breaches.
12
13
14

15 For users in countries with oppressive governments and other threatening
16 factions, mobile security provides safety from physical attack and arbitrary arrests.
17 Introducing intentional weaknesses into software "invariably undermine[s] the security
18 of all users online, since a backdoor, even if intended solely for government access, can
19 be accessed by unauthorized entities, including other States or non-State actors. Given
20 its widespread and indiscriminate impact, back-door access would affect,
21 disproportionately, all online users." Kaye Report at 14.
22
23
24
25
26

27 ¹⁷ https://freedomhouse.org/sites/default/files/FH_FITW_Report_2016.pdf.

28 ¹⁸ <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>.

1 Amici know firsthand about the critical importance of strong digital security for
2 users in other parts of the world. Among its other mission priorities, Access Now runs
3 a Digital Security Helpline, which operates around the clock to provide resources and
4 support to users at risk around the world. Access Now, *Digital Security Helpline*,
5 <https://www.accessnow.org/digital-security-helpline>. Wickr Foundation partners with
6 the Oslo Freedom Forum to offer Tech Lab, which trains activists and journalists from
7 authoritarian states how to protect their digital and physical safety when using consumer
8 technologies. Wickr Foundation, *Education and Training*, <https://www.wickr.org/edu>-
9 programs.
10

11
12 Through the Digital Security Helpline, Access Now has a unique view into the
13 threats faced by users and the importance of digital security that protects journalists,
14 activists, and dissidents around the world from entities who would retaliate against them
15 through arbitrary arrest, unlawful detention, and even torture.
16

- 17
- 18 • In a particularly egregious example, Access Now investigated the events that led
19 to the persecution of a Vietnamese blogger exercising legitimate speech rights.
20 The investigation revealed that the blogger had been identified due to an attack
21 that compromised his iPhone and allowed access to his personal accounts,
22 including iCloud, Facebook, and email. The blogger eventually had to move with
23 his family away from his home to a secure location to ensure their safety.
24
 - 25 • Access Now assisted activists with the deployment of mobile security strategies
26 to protect sensitive communications concerning a project to translate important
27
28

1 information about U.S. presidential elections to Asian-American and Pacific
2 Islander voters. The security measures were necessary to protect the contact
3 details and information of voters.

- 4 • Access Now attempted to help Ethiopian activists find secure mobile
5 communication channels. During the course of our interactions with the group,
6 several were arrested and their phones taken into custody, making it easy for the
7 government to gain access to any unencrypted data.
- 8 • Access Now helped South African activists find a secure mobile messaging
9 system that met their specific needs. During a particular period of political
10 turmoil, the activists were under surveillance and their private messages were
11 frequently leaked and posted publicly, putting their physical safety at high risk.

12 In several cases, users have indicated to Access Now staff that secure mobile
13 communication platforms and networks are crucial because fixed-line internet access is
14 costly and unreliable in their geographic locations. In areas underserved by internet
15 service providers or completely unconnected, mobile communications are often the best
16 and most reliable means of communication. For people in those areas, mobile security
17 may be critical to ensure physical safety.

18 Other reported incidents around the world are in line with the circumstances
19 Access Now has learned through the helpline. In Uganda, after shutting down internet
20 access, the Communications Commission threatened to prosecute for treason anyone
21 who used “security apps” to regain a connection. Melanie Nathan, *Ugandan*

1 *Communications Commission threatened to Arrest Citizens for using Social Media*, O-blog-dee-o-
2 blog-da (Feb. 19, 2016).¹⁹ In Mexico, members of a drug cartel gained access to a citizen
3 journalist's phone and discovered that she was responsible for a pseudonymous anti-
4 cartel Twitter account, which led to her gruesome murder. Jason McGahan, *She Tweeted*
5 *Against the Mexican Cartels, They Tweeted Her Murder*, The Daily Beat (Oct. 21, 2014).²⁰ In
6 countries where sexual orientation other than heterosexuality is forbidden, digital
7 communications can be the only way that lesbian, gay, bisexual or trans people "can
8 have a voice, organise themselves, formulate their regional discourses around their
9 issues and fight for recognition." Security in-a-Box, *Tools and Tactics for the LGBTI*
10 *Community in the Middle-East and North Africa*, <https://securityinabox.org/en/lgbti-mena>.
11 In such places, the anonymity and privacy that digital security tools such as encryption
12 provide can save lives.

13
14
15
16 / / /

17
18
19 / / /

20
21 / / /

22
23 / / /

24
25
26 ¹⁹ [http://oblogdeoblogda.me/2016/02/19/ugandan-communications-commission-](http://oblogdeoblogda.me/2016/02/19/ugandan-communications-commission-threaten-to-arrest-citizens-for-using-social-media)
27 [threaten-to-arrest-citizens-for-using-social-media](http://oblogdeoblogda.me/2016/02/19/ugandan-communications-commission-threaten-to-arrest-citizens-for-using-social-media).

28 ²⁰ [http://www.thedailybeast.com/articles/2014/10/21/she-tweeted-against-the-](http://www.thedailybeast.com/articles/2014/10/21/she-tweeted-against-the-mexican-cartels-they-tweeted-her-murder.html)
[mexican-cartels-they-tweeted-her-murder.html](http://www.thedailybeast.com/articles/2014/10/21/she-tweeted-against-the-mexican-cartels-they-tweeted-her-murder.html).

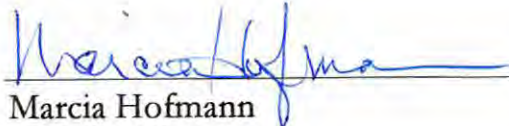
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CONCLUSION

Amici respectfully request that this Court grant Apple's motion to vacate the Order.

DATED: March 1, 2016

Respectfully submitted,



Marcia Hofmann
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
marcia@zeitgeist.law
Telephone: (415) 830-6664

Attorney for Amici Curiae
Access Now and Wickr Foundation

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

PROOF OF SERVICE

I, the undersigned, declare that I am a citizen of the United States; my business address is 25 Taylor Street, San Francisco, California 94102; I am employed in the City and County of San Francisco; I am over the age of eighteen (18) years and not a party to the within action.

On March 1, 2016, I served the foregoing document described as:

BRIEF OF AMICI CURIAE ACCESS NOW AND WICKR FOUNDATION IN SUPPORT OF APPLE INC.'S MOTION TO VACATE

on the interested party(ies) in this action by placing a true copy thereof enclosed in a sealed envelope addressed as follows:

Theodore J Boutrous, Jr.
Eric David Vandevelde
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071
213-229-7000

Allen W Chiu
AUSA - Office of US Attorney
National Security Section
312 North Spring Street, Suite 1300
Los Angeles, CA 90012
213-894-2435

Marc J Zwillinger
Jeffrey G Landis
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
202-296-3585

Tracy L Wilkison
AUSA Office of US Attorney
Chief, Cyber and Intellectual Property Crimes
Section
312 North Spring Street, 11th Floor
Los Angeles, CA 90012-4700
213-894-0622

Nicola T Hanna
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 92612-4412
949-451-3800

Counsel for Plaintiff USA

Theodore B Olson
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 20036-5306
202-955-8668

Counsel for Respondent Apple Inc.

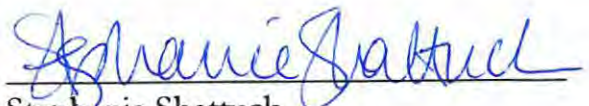
BY MAIL: I caused such envelope(s), fully prepaid, to be placed in the United States

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

mail at San Francisco, California. I am “readily familiar” with this firm’s practice for collection and processing of correspondence for mailing. Under that practice, it would be deposited with the United States Postal Service the same day, with postage thereon fully prepaid, at San Francisco, California, in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if the postal cancellation date on postage meter date is more than one day after date of deposit for mailing in affidavit.

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

DATED: March 1, 2016


Stephanie Shattuck