

CAROLINE WILSON PALOW (SBN 241031)

caroline@privacyinternational.org

SCARLET KIM

scarlet@privacyinternational.org

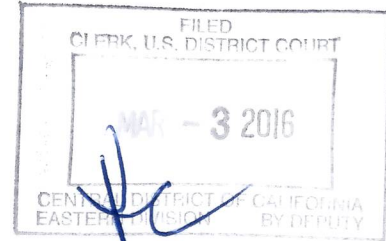
PRIVACY INTERNATIONAL

62 Britton Street

London EC1M 5UY

United Kingdom

Telephone: +44.20.3422.4321



Attorneys for *Amici Curiae*

PRIVACY INTERNATIONAL

HUMAN RIGHTS WATCH

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

IN THE MATTER OF THE SEARCH) ED No. CM 16-10 (SP)
OF AN APPLE IPHONE SEIZED)
DURING THE EXECUTION OF A) **BRIEF OF *AMICI CURIAE***
SEARCH WARRANT ON A BLACK) **PRIVACY INTERNATIONAL AND**
LEXUS IS300, CALIFORNIA) **HUMAN RIGHTS WATCH**
LICENSE PLATE 35KGD203)
) **Hearing:**
) Date: March 22, 2016
) Time: 1:00 p.m.
) Place: Courtroom 3 or 4
) Judge: Hon. Sheri Pym

LODGED

FILED
MAR - 3 PM 1:49
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	INTERESTS OF <i>AMICI CURIAE</i>	2
III.	BACKGROUND	3
	A. The iPhone and its Passcode	3
	B. Procedural History	4
IV.	ARGUMENT	6
	A. The Order Sets a Far-reaching Precedent that the Government May Compel Technology Companies to Undermine the Security of their Products and Services	6
	B. Compelling Technology Companies to Undermine the Security of their Products and Services Threatens the Security of the Internet	8
	C. The Order Signals to Other Countries that it is Permissible and Appropriate to Compel Technology Companies to Undermine the Security of their Products and Services	12
	D. Other Countries Will Compel Technology Companies to Undermine the Security of their Products and Services In Order to Commit Civil and Human Rights Abuses	19
V.	CONCLUSION	22

TABLE OF AUTHORITIES

OTHER AUTHORITIES

Alice Truong, <i>What Chinese slowdown? Apple's sales double in China on iPhone growth</i> , Quartz (Oct. 27, 2015) -----	19
Andrea Peterson, <i>Forbes Web site was compromised by Chinese cyberespionage group, researchers say</i> , Wash. Post (Feb. 10, 2015)-----	10
Ankit Panda, <i>Beijing Strikes Back in US-China Tech Wars</i> , The Diplomat (Mar. 6, 2015) -----	18
Apple Inc. and Apple Dist. Int'l, <i>Written Evidence to the UK Parliament Joint Comm. on the Draft Investigatory Powers Bill (IPB0093)</i> (Jan. 7, 2016)14, 15, 16	
Apple Inc., <i>iOS Security: iOS 9.0 or later</i> (Sept. 2015) -----	4
Ben Elgin, Vernon Silver & Alan Katz, <i>Iranian Police Seizing Dissidents Get Aid of Western Companies</i> , Bloomberg (Oct. 31, 2011) -----	21
Bruce Schneier, <i>Data and Goliath</i> (2015)-----	10
Council of Europe, European Commission for Democracy through Law, <i>Opinion on the Federal Law on the Federal Security Service (FSB) of the Russian Federation</i> (2012) -----	14
Dep't of Homeland Security, <i>Mobile Security Tip Card</i> -----	12
Ellen Nakashima, <i>Meet the woman in charge of the FBI's most controversial high-tech tools</i> , Wash. Post (Dec. 8, 2015)-----	9, 11
Eva Galperin, <i>Don't get your sources in Syria killed</i> , Committee to Protect Journalists (May 21, 2012) -----	21
Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc., <i>Written Evidence to the UK Parliamentary Joint Comm. on the Draft Investigatory Powers Bill (IPB0116)</i> (Jan. 7, 2016)-----	15
Federal Law of the Russian Federation on the Federal Security Service Act (no. 40-FZ) 1995 -----	13

1	Human Rights Watch, <i>China: Draft Counterterrorism Law a Recipe for Abuses</i>	
2	(Jan. 20, 2015) -----	17
3	Human Rights Watch, <i>Submission by HRW to the National People's Congress</i>	
4	<i>Standing Committee on the draft Cybersecurity Law</i> (Aug. 4, 2015) -----	19
5	Turkey Information and Communication Technologies Authority, <i>By Law on the</i>	
6	<i>Procedures and Principles of Encoded or Encrypted Communication between</i>	
7	<i>Public Authorities and Organizations and Real and Legal Persons in Electronical</i>	
	<i>[sic] Communication Service</i> (Oct. 23, 2010) -----	17
8	Investigatory Powers Bill 2015-16, Bill [143] (Gr. Brit.) -----	14, 15
9	Jeff Mason, <i>Exclusive: Obama sharply criticizes China's plans for new technology</i>	
10	<i>rules</i> , Reuters (Mar. 2, 2015)-----	18
11	Kadhim Shubber, <i>BlackBerry gives Indian government ability to intercept</i>	
12	<i>messages</i> , Wired (July 11, 2013) -----	16
13	Katie Collins, <i>BlackBerry to leave Pakistan after refusing to ditch user privacy</i> ,	
14	CNET (Dec. 1, 2015)-----	16
15	Kevin Poulsen, <i>FBI Admits It Controlled Tor Servers Behind Mass Malware</i>	
16	<i>Attack</i> , Wired (Sept. 13, 2013)-----	9, 10
17	Lance Whitney, <i>RIM averts BlackBerry ban in UAE</i> , CNET (Oct. 8, 2010) -----	17
18	Law Library of Congress, <i>Russian Federation Translation of National Legislation</i>	
19	<i>into English</i> (March 2012)-----	13
20	Letter to Court, <i>In re Order Requiring Apple, Inc. to Assist in the Execution of a</i>	
21	<i>Search Warrant Issued by this Court</i> , No. 15-MC-1902 (E.D.N.Y. Feb. 17,	
22	2016), Dkt. 27 -----	12
23	Martin Kaste, <i>Slippery Slope? Court Orders Apple to Unlock Shooter's iPhone</i> ,	
24	NPR (Feb. 18, 2016) -----	12
25	Noah Shachtman, <i>Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals</i> ,	
26	Wired (July 23, 2012) -----	13
27	Patrick Howell O'Neill, <i>How cybercriminals use major news events to attack you</i> ,	
28	The Daily Dot (Aug. 5, 2013)-----	9

1	President's Review Group on Intelligence and Communications Technologies,	
2	<i>Liberty and Security in a Changing World</i> (Dec. 12, 2013) -----	11
3	<i>Provisions of China's counterterrorism bill inspired by foreign laws: official,</i>	
4	Xinhua (Dec. 27, 2015) -----	19
5	<i>Report of the Special Rapporteur on the promotion and protection of human rights</i>	
6	<i>and fundamental freedoms while countering terrorism, Martin Scheinin,</i>	
7	<i>delivered to the Human Rights Council, U.N. Doc. A/HRC/13/37</i> (Dec. 28, 2009)	
	-----	19
8	<i>Report of the Special Rapporteur on the promotion and protection of the right to</i>	
9	<i>freedom of opinion and expression, David Kaye, delivered to the Human Rights</i>	
10	<i>Council, U.N. Doc. A/HRC/29/32, (May 22, 2015) -----</i>	17, 18, 20
11	<i>Report of the Special Rapporteur on the promotion and protection of the right to</i>	
12	<i>freedom of opinion and expression, Frank La Rue, delivered to the Human Rights</i>	
13	<i>Council, U.N. Doc. A/HRC/23/40</i> (Apr. 23, 2013) -----	19
14	<i>RIM to share some BlackBerry codes with Saudis, Reuters</i> (Aug. 10, 2010)-----	17
15	Samm Sacks, <i>Apple in China, Part I: What Does Beijing Actually Ask of</i>	
16	<i>Technology Companies?</i> , Lawfare (Feb. 22, 2016)-----	18
17	The Right to Privacy in the Digital Age, G.A. Res. 69/166, pmbl., U.N. Doc.	
18	A/Res/69/166 (Feb. 10, 2014)-----	21
19	Tom Mitchell, <i>Obama seeks reboot of China cyber laws</i> , Fin. Times (Mar. 3, 2015)	
20	-----	17
21	U.S. Submission to the Special Rapporteur on the Promotion of the Right to	
22	Freedom of Opinion and Expression (Feb. 26, 2015)-----	20, 21
23	Vernon Silver & Ben Elgin, <i>Torture in Bahrain Becomes Routine With Help From</i>	
24	<i>Nokia Siemens</i> , Bloomberg (Aug. 22, 2011)-----	21

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Compelling Apple, Inc. (“Apple”) to remove security features from its iPhone will have global and wide-ranging implications. It is for this reason that Privacy International and Human Rights Watch (“HRW”) submit this *amicus curiae* brief. Both organizations have spent years monitoring and critiquing the surveillance practices and human rights records of governments worldwide. This matter sits at an important crossroads that has arisen in that space. The path the United States takes will impact how other governments will approach the increasing tension between their desire for ready access to electronic data and the need for robust security features that allow us to communicate, express ourselves, and assert our fundamental rights in a digital age. If the Order stands, governments around the world may view it as encouragement to preference the former by similarly requiring technology companies to undermine the security of their products and services. Many countries are already considering such powers.

The mere existence of the power the government seeks may erode the security infrastructure of the Internet. If Apple can be compelled to undermine its security features, what confidence can users of Apple and other technology products and services actually place in those features? For instance, would it be appropriate to trust a software security update from a company that could be compelled to include malicious software – often called malware – in that update?¹ Yet these security updates are crucial to protecting all of our data and devices, since they are normally deployed to fix vulnerabilities that might otherwise be exploited by hackers, including criminals and foreign agents.²

¹ “Malware” refers to any software that performs unwanted tasks, typically for the benefit of a third party. Malware can range from a simple irritant to a serious breach of privacy (e.g. stealing data from a computer).

² “Hacking” can refer to several different activities. In computing terms, it originally described the hobby of computer programming and encompassed the idea of finding creative solutions to technology problems. The term gradually evolved to describe the activity of finding

1 Security features – including encryption and other measures – are integral to
 2 the protection of civil and human rights. Countries may seek to compel technology
 3 companies to impair security for illegitimate purposes, including to stifle
 4 expression, crush dissent, and facilitate arbitrary arrest and torture. In these
 5 societies, secure technologies protect all members of society but especially
 6 vulnerable ones – such as journalists, human rights defenders, and political
 7 activists – by giving them a safe space to communicate, research, and organize.
 8 The U.S., by compelling technology companies to roll back these protections, risks
 9 exposing the millions of individuals who reside and work in these places to abuse
 10 by their governments.

11 For all of these reasons, Privacy International and HRW strongly urge the
 12 Court to consider the wider implications of the Order compelling Apple to assist in
 13 the search of the iPhone at issue. They hope this submission will help the Court in
 14 making the difficult decision it faces.

15 II. INTERESTS OF *AMICI CURIAE*

16 Privacy International is a nonprofit, nongovernmental organization based in
 17 London dedicated to defending the right to privacy around the world. Established
 18 in 1990, Privacy International undertakes research and investigations into state and
 19 corporate surveillance with a focus on the technologies that enable these practices.
 20 It has litigated or intervened in cases implicating the right to privacy in the courts
 21 of the US, the United Kingdom (“U.K.”) and Europe, including the European
 22 Court of Human Rights. To ensure universal respect for the right to privacy,
 23 Privacy International advocates for strong national, regional and international laws
 24

25
 26 vulnerabilities in computer security, first with the goal of reporting or repairing them (“white
 27 hat”), but later to exploit them (“black hat”). The black hat iteration of hacking is the mainstream
 28 usage of the term and is the definition adopted throughout this brief. That definition encompasses
 the activity of any attacker – including criminals and foreign agents – seeking to exploit a
 vulnerability in computer security.

1 that protect privacy. It also strengthens the capacity of partner organizations in
2 developing countries to do the same.

3 Human Rights Watch (“HRW”) has been reporting on abuses connected to
4 the practice of state surveillance since its inception more than three decades ago as
5 Helsinki Watch, with particular focus on mass surveillance practices since 2013.
6 HRW’s reports detail abuses of rights connected to surveillance around the globe
7 (for example, in China, Ethiopia, Saudi Arabia, and the U.S.), and its advocacy
8 involves legal analysis and submissions on the various legal authorities (actual or
9 proposed) for surveillance practices to the relevant bodies of the United Nations
10 (“U.N.”), the U.S., the U.K., the UN High Commissioner for Human Rights, the
11 Special Rapporteur for Freedom of Expression, as well as comment and analysis
12 on the laws of many other countries in respect of these issues.

13 **III. BACKGROUND**

14 **A. The iPhone and its Passcode**

15 The device at the heart of this dispute is an iPhone 5c running operating
16 system (“iOS”) 9. *Ex Parte* Application for Order Compelling Apple Inc. to Assist
17 Agents in Search, *In the Matter of the Search of an Apple iPhone Seized during the*
18 *Execution of a Search Warrant on a Black Lexus IS300, California License Plate*
19 *35KGD203* (“*Apple iPhone*”), ED No. 15-0451M *1, *4 (C.D. Cal. Feb. 16, 2016)
20 [hereinafter “*Ex Parte* Application”]. In September 2014, Apple announced that
21 “iPhones . . . operating Apple’s then-newest operating system, iOS 8, would
22 include hardware-and software-based encryption of the password-protected
23 contents of the devices by default.” Declaration of Erik Neuenschwander in
24 Support of Apple’s Motion to Vacate, *Apple iPhone*, ED No. 15-0451M, ¶ 8 (C.D.
25 Cal. Feb. 16, 2016), Dkt. 16, attach. 33 [hereinafter “*Neuenschwander Decl.*”].
26 What this development meant was that individuals with an iPhone running iOS 8
27 or newer operating systems could, by setting up a passcode, enable encryption of
28 their iPhone data. *Id.* at ¶ 9; *see also* Declaration of Caroline Wilson Palow in

1 support of Brief of *Amici Curiae* Privacy International and Human Rights Watch
 2 [hereinafter “Palow Decl.”], Ex. A, at 12 [Apple Inc., *iOS Security: iOS 9.0 or*
 3 *later* (Sept. 2015) [hereinafter “*iOS Security I*”]]. The data on the device cannot be
 4 decrypted without the correct cryptographic key, and this key is protected by a key
 5 derived from the user-chosen passcode. Palow Decl. Ex. A at 12 [*iOS Security*]. In
 6 short, “[t]he end result is a person must know that passcode to read [the iPhone’s]
 7 data.” Dkt. 16, attach. 33 ¶ 9 [Neuenschwander Decl.].

8 Apple has devised a number of safeguards to protect against “brute-force”
 9 attempts to determine the passcode. First, Apple uses a “large iteration count”,
 10 which “functions to slow attempts to unlock an iPhone”. *Id.* at ¶ 11. The iteration
 11 count is “calibrated so that . . . it would take more than 5 ½ years to try all
 12 combinations of a six-character alphanumeric passcode with lowercase letters and
 13 numbers.” Palow Decl. Ex. A at 12 [*iOS Security*]. Second, Apple imposes
 14 escalating time delays after each entry of an invalid passcode. *Id.*; Dkt. 16, attach.
 15 33 ¶ 12 [Neuenschwander Decl.]. Finally, an individual can turn on the “Erase
 16 Data” setting, which automatically wipes the keys needed to read the encrypted
 17 data after ten consecutive incorrect attempts to enter the passcode. Dkt. 16, attach.
 18 33 ¶ 12 [Neuenschwander Decl.]; Palow Decl. Ex. A at 12 [*iOS Security*].

19 **B. Procedural History**

20 On February 16, 2016, the government filed an *ex parte* application in this
 21 Court for an order pursuant to the All Writs Act, 28 U.S.C. § 1651, compelling
 22 Apple to “provide assistance to agents of the Federal Bureau of Investigation
 23 (“FBI”) in their search of a cellular telephone.” *Ex Parte* Application, at *1. That
 24 same day, this Court issued an order compelling Apple to provide “reasonable
 25 technical assistance to law enforcement agents in obtaining access to the data on
 26 the SUBJECT DEVICE.” Order Compelling Apple, Inc. to Assist Agents in
 27 Search, *Apple iPhone*, ED No. 15-0451M, *2 (C.D. Cal. Feb. 16, 2016)
 28 [hereinafter “Order”]. The Order specified that

1 Apple's reasonable technical assistance shall accomplish the following
2 three important functions: (1) it will bypass or disable the auto-erase
3 function whether or not it has been enabled; (2) it will enable the FBI to
4 submit passcodes to the SUBJECT DEVICE for testing electronically
5 via the physical device port, Bluetooth, Wi-Fi, or other protocol
6 available on the SUBJECT DEVICE; and (3) it will ensure that when
7 the FBI submits passcodes to the SUBJECT DEVICE, software running
8 on the device will not purposefully introduce any additional delay
9 between passcode attempts beyond what is incurred by Apple
10 hardware.

11 *Id.* at *2.

12 On February 16, 2016, Apple informed the government and this Court that it
13 would seek relief from the Order. Scheduling Order, *Apple iPhone*, ED No. CM
14 16-10 ¶ 1 (C.D. Cal. Feb. 16, 2016), Dkt. 9 [hereinafter "Scheduling Order"]. On
15 February 19, 2016, the government filed a motion to compel Apple to comply with
16 the Order. Government's Motion to Compel Apple, Inc. to Comply with this
17 Court's February 16, 2016 Order Compelling Assistance in Search, *Apple iPhone*,
18 ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016), Dkt. 1 [hereinafter "Motion to
19 Compel"]. That day, this Court issued a Scheduling Order setting a briefing
20 schedule for Apple's application for relief, which instructed that "[a]ny amicus
21 brief shall be filed by not later than March 3, 2016, along with an appropriate
22 request seeking leave of the Court to file such brief." Dkt. 9, at ¶ 4(ii) [Scheduling
23 Order]. On February 26, 2016, Apple filed its application for relief and opposition
24 to the government's Motion to Compel. Apple Inc.'s Motion to Vacate Order
25 Compelling Apple Inc. to Assist Agents in Search, and Opposition to
26 Government's Motion to Compel Assistance, *Apple iPhone*, Ed No. CM 16-10 *6
27 (C.D. Cal. Mar. 22, 2016), Dkt. 16 [hereinafter "Motion to Vacate"].
28

IV. ARGUMENT

A. The Order Sets a Far-reaching Precedent that the Government May Compel Technology Companies to Undermine the Security of their Products and Services

This Court's Order, by requiring Apple to develop new software to weaken the iPhone's passcode protection, establishes a precedent that the government may compel technology companies to undermine the security of their products and services. This dramatic expansion of the government's investigative authority is not limited to a single device manufactured by a single company. Rather, this new power could conceivably extend to any service or device – laptop, mobile phone, or the increasing number of other things connected to the Internet – provided by any company.

The government downplays the assistance it seeks from Apple, describing it as “providing the FBI with the opportunity to determine the passcode” to an iPhone. Dkt. 1 at *2 [Motion to Compel]. But the government's submissions critically overlook the *purpose* for which Apple would develop new software under the Order. That purpose is explicitly to weaken the security of one of its products. Apple designed the subject iPhone so that a user, by setting up a passcode, automatically enables encryption of her data. The cryptographic key to decrypt the data is protected by a key derived from the user's passcode. Thus, the passcode is essential to the decryption process and is therefore a critical element of the security of the iPhone.³ By compelling Apple to “modify” its operating system, the government is compelling it to “modify” a critical security feature of the iPhone.

Amici contend that this so-called “modification” is nothing short of hacking. In neutral terms, hacking is about exploring – often in creative fashion –

³ The government's assertion that it is asking Apple to “writ[e] a program that turns off non-encryption features” is not technically accurate. Dkt. 1 at *14 [Motion to Compel]. As explained above, the passcode is a fundamental part of the iPhone's encryption process and cannot therefore be objectively described as a “non-encryption feature”.

1 vulnerabilities in computer security. But it is only in its negative connotation that it
2 encompasses the activity of exploiting those vulnerabilities to deliberately
3 undermine security. That negative connotation of hacking is what the government
4 seeks to compel from Apple. It asks Apple to design and then create software that
5 purposefully creates cracks in the iPhone's security.

6 Although the government represents that "the Order is tailored for and
7 limited to this particular phone", Dkt. 1 at *14 [Motion to Compel], the legal
8 theory upon which it rests is unbounded. In simple terms, and in the government's
9 own words, the All Writs Act, 28 U.S.C. § 1651, compels "reasonable third-party
10 assistance that is necessary to exercise a warrant."⁴ Dkt. 1 at *7 [Motion to
11 Compel]. For the government, "reasonable" boils down to technical feasibility; its
12 overarching proposition is that "Apple retains . . . the technical ability to comply
13 with the Order, and so should be required to obey it." *Id.* at *1; *see also id.* at *13-
14 *14.

15 Technical feasibility is a meaningless constraint because, in technical terms,
16 many strategies for undermining the security of an iPhone may be feasible. As
17 Apple hypothesizes, if it
18 can be forced to write code in this case to bypass security features and
19 create new accessibility, what is to stop the government from
20 demanding that Apple write code to turn on the microphone in aid of
21 government surveillance, activate the video camera, surreptitiously
22
23

24 ⁴ Apple argues that the government's reading of the All Writs Act is unbounded for two reasons.
25 First, it recognizes no contextual limitation; any warrant in any investigation could provide the
26 basis for a supplemental All Writs Act Order to a third party. Dkt. 16 at *3 [Motion to Vacate].
27 Second, "under the government's formulation, any party whose assistance is deemed 'necessary'
28 by the government falls within the ambit of the All Writs Act and can be compelled to do
anything the government needs to effectuate a lawful court order." *Id.* at *25-*26. Privacy
International does not repeat those arguments here but focuses on the government's
interpretation of what is "reasonable third-party assistance" under the All Writs Act.

1 record conversations, or turn on location services to track the phone's
2 user?

3 Dkt. 16 at *4 [Motion to Vacate]; *see also id.* at *25-*26. Apple possesses the
4 technical capability to write and deploy such code.

5 If the government can compel Apple – because it is technically feasible – to
6 develop code to weaken iPhone security under the All Writs Act, it can compel any
7 other technology company to similarly sabotage its own devices. The proliferation
8 of Internet-connected devices – from computers to cars to refrigerators –
9 exponentially increases the ways the government could seek such assistance. And
10 the technology companies that could be conscripted into government service are
11 not limited to those that manufacture devices. Every day, more and more of our
12 lives are conducted in the digital realm. Equally, more and more of our physical
13 realm is governed and mediated by digital technologies. Many companies provide
14 services in both realms, from hosting websites to storing documents to transferring
15 money between bank accounts. Every one of these companies could conceivably
16 be compelled to develop software that weakens the security of these services and
17 the data, often precious to the individual to which it relates, that it stores.

18 **B. Compelling Technology Companies to Undermine the Security of their**
19 **Products and Services Threatens the Security of the Internet**

20 Compromising the security of a single technology product, like an iPhone,
21 can send negative ripple effects throughout the Internet. Those effects are
22 enhanced where what is compromised is a server or a network, to which hundreds
23 or thousands of people may connect. And the ramifications of compromising a
24 device, server or network are perilously amplified should the government seek to
25 regularly compel technology companies to undertake such activity.

1 A powerful example of how undermining a single service can breach the
 2 security of many is a “watering hole” attack.⁵ This type of attack can target a
 3 group, such as a business or organization, by identifying a website frequented by
 4 its members and placing malware on it. *See* Palow Decl. Ex. B [Patrick Howell
 5 O’Neill, *How cybercriminals use major news events to attack you*, The Daily Dot
 6 (Aug. 5, 2013)] (defining a “watering hole” attack and describing common
 7 iterations). The malware silently compromises the devices that visit the website, by
 8 dropping additional malware onto those devices, which can allow the attacker to
 9 access sensitive data or even control the affected devices. *See id.*

10 Under an All Writs Act order, the government could compel a web hosting
 11 provider to implement a “watering hole” attack by developing and installing
 12 custom code on a website (or multiple websites) that it operates. Indeed, the FBI
 13 has already admitted to deploying such an attack itself. *See* Palow Decl. Ex. C
 14 [Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware*
 15 *Attack*, Wired (Sept. 13, 2013) [hereinafter *FBI Admits It Controlled Tor Servers*]].
 16 An order under the All Writs Act would permit the FBI to instead compel a
 17 company to carry out the attack, an alternative it is likely to prefer. *See* Palow
 18 Decl. Ex. D [Ellen Nakashima, *Meet the woman in charge of the FBI’s most*
 19 *controversial high-tech tools*, Wash. Post (Dec. 8, 2015) [hereinafter “*Meet the*
 20 *woman*”]] (citing Amy Hess, executive assistant director for the FBI’s Science and
 21 Technology Branch, as stating that “hacking computers is not a favored FBI

22 ⁵ Apple presents the security hazards inherent in developing new software to weaken the
 23 iPhone’s passcode protection, even if it is only to be deployed on a single iPhone. Dkt. 16 at *13-
 24 *14 [Motion to Vacate] (noting that the entire process “would need to be logged and recorded in
 25 case Apple’s methodology is ever questioned, for example in court”); *id.* at *24-*25 (describing
 26 the alternative to building and destroying software for each law enforcement demand as
 27 “securing against disclosure or misappropriation” all physical and digital materials related to
 28 such software); Dkt. 16, attach. 33 ¶¶ 39-43 [Neuenschwander Decl.] (indicating that it would be
 “unrealistic” to “truly destroy the actual operating system and the underlying code”, which
 remains “persistent”). Privacy International does not repeat those arguments here but focuses on
 how undermining a technology service rather than a device can impact the security of the
 Internet.

1 technique” because “[a]s soon as a tech firm updates its software, the tool
2 vanishes”).

3 A “watering hole” attack is particularly pernicious from a security
4 perspective because the attacker typically selects legitimate, trusted websites,
5 which may receive hundreds or thousands of daily visitors. A recent example of
6 such an attack occurred in November 2014, when Chinese hackers infected
7 Forbes.com as a way of targeting visitors working in the US defense and financial
8 services industries. *See* Palow Decl. Ex. E [Andrea Peterson, *Forbes Web site was*
9 *compromised by Chinese cyberespionage group, researchers say*, Wash. Post (Feb.
10 10, 2015) [hereinafter “*Forbes Web site was compromised*”]]. Moreover, even
11 where the attack targets a specific group of individuals, every visitor to the
12 compromised website is vulnerable to a security breach. In the FBI “watering hole”
13 attack cited above, the government compromised every site – and every visitor to
14 those sites – hosted by a particular server, some of which had no relation to the
15 government’s investigation. Palow Decl. Ex. C [*FBI Admits It Controlled Tor*
16 *Servers*].

17 The security of the Internet operates like a fragile ecosystem, where a
18 compromised device or service can negatively affect many other users. That
19 ecosystem is unlikely to survive should the government seek to regularly compel
20 technology companies to undermine the security of their products or services.⁶ In
21 the “watering hole” attack scenario, regular attacks would spell disaster, in part
22 because many “watering hole” attacks rely on what are called zero day
23 vulnerabilities. A zero day vulnerability refers to a security flaw in software that is
24 unknown to the vendor. *See* Palow Decl. Ex. F at 145-46 [Bruce Schneier, *Data*
25 *and Goliath* (2015)] (“Unpublished vulnerabilities are called ‘zero-day’
26 vulnerabilities; they’re very valuable to attackers because no one is protected

27
28 ⁶ Apple describes the security implications of repeated requests to weaken the passcode
protection on the iPhone. *See* Dkt. 16, attach. 33 ¶¶ 46-47 [Neuenschwander Decl.].

1 against them, and they can be used worldwide with impunity.”). When researchers
 2 and others discover vulnerabilities, they typically report the flaw to the company
 3 responsible for the security of the affected software. If companies are regularly
 4 asked to host “watering hole” attacks, they may have conflicting incentives. On the
 5 one hand, they might wish to fix such vulnerabilities for the public good; on the
 6 other hand, they might be compelled to stockpile such vulnerabilities for future use
 7 in a “watering hole” attack.⁷ The stockpiling of zero days can potentially leave
 8 millions of individuals as well as companies vulnerable to attack, a perverse
 9 situation that has led President Barack Obama’s own Review Group on
 10 Intelligence and Communications Technologies to conclude:

11 In almost all instances, for widely used code, it is in the national interest
 12 to eliminate software vulnerabilities rather than to use them

13 Eliminating the vulnerabilities — ‘patching’ them — strengthens the
 14 security of US Government, critical infrastructure, and other computer
 15 systems.

16 Palow Decl. Ex. G at 219-220 [President’s Review Group on Intelligence and
 17 Communications Technologies, *Liberty and Security in a Changing World* (Dec.
 18 12, 2013)].

19 Now consider the software update process. A software update, also known
 20 as a “patch”, is a piece of software released by companies to fix or improve an
 21 existing product. Software updates often fix security vulnerabilities, which hackers
 22 can otherwise exploit to deliver malware. For this reason, the US government
 23 encourages the downloading and installation of software updates as critical cyber

24
 25 ⁷ Alternatively, the government, which already stockpiles vulnerabilities, may be incentivized to
 26 expand this activity in order to share such vulnerabilities with companies compelled to host
 27 “watering hole” attacks. See Palow Decl. Ex. D [*Meet the woman*] (“Hess acknowledged that the
 28 bureau uses zero-days—the first time an official has done so. She said the trade-off is one the
 bureau wrestles with. ‘What is the greater good—to be able to identify a person who is
 threatening public safety?’ Or to alert software makers to bugs that, if unpatched, could leave
 consumers vulnerable?”).

1 security measures. For example, a “Mobile Security Tip Card” published by the
2 Department of Homeland Security advises Americans:

3 Install updates for apps and your device’s operating system as soon as
4 they are available. Keeping the software on your mobile device up to date
5 will prevent attackers from being able to take advantage of known
6 vulnerabilities.

7 Palow Decl. Ex. H [Dep’t of Homeland Security, *Mobile Security Tip Card*].

8 Co-opting the software update process is analogous to what the government
9 is asking Apple to do in the Order – that is using the power it claims under the All
10 Writs Act to convert a mechanism traditionally used to improve security into one
11 that subverts it. Should the government seek to do this regularly, which it will if
12 the Court upholds the Order, *see* Palow Decl. Ex. I [Letter to Court, *In re Order*
13 *Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this*
14 *Court*, No. 15-MC-1902 (E.D.N.Y. Feb. 17, 2016), Dkt. 27] (describing twelve
15 other All Writs Act orders against Apple sought by the government); Palow Decl.
16 Ex. J [Martin Kaste, *Slippery Slope? Court Orders Apple to Unlock Shooter’s*
17 *iPhone*, NPR (Feb. 18, 2016)] (quoting Cyrus Vance, Manhattan District Attorney,
18 as stating that he has “about 155 to 160 devices . . . running on iOS 8” that he
19 would like to access), it will fundamentally cripple such core security mechanisms.
20 It will broadly undermine trust in software updates, leading users not to install
21 them. By not installing software updates, consumers will be increasingly
22 vulnerable to security attacks by hackers exploiting unpatched vulnerabilities in the
23 products and services they use.

24 **C. The Order Signals to Other Countries that it is Permissible and**
25 **Appropriate to Compel Technology Companies to Undermine the**
26 **Security of their Products and Services**

27 Many foreign governments are increasingly seeking the power to compel
28 technology companies operating within their jurisdictions to undermine the

1 security of their products both for law enforcement and intelligence-gathering
 2 purposes. Emboldened by the US example, these countries may soon place
 3 heightened pressure on companies to comply. Technology companies can – and
 4 often do – resist these assertions of power in foreign contexts, but it will be
 5 increasingly difficult for them to do so should the US government be permitted to
 6 assert this power itself.

7 In Russia, for example, the government already claims the power to compel
 8 technology companies to assist Russian law enforcement or intelligence agencies
 9 in exactly the manner that the US government seeks from Apple, *i.e.* through
 10 hacking their own products or services. Article 15 of the Federal Law of the
 11 Russian Federation on the Federal Security Service Act (no. 40-FZ) 1995 (“FSB
 12 Act”), provides:

13 [L]egal entities in the Russian Federation providing . . . electronic
 14 communications services of all types . . . shall be under obligation, at the
 15 request of federal security service organs, to include in the apparatus
 16 additional hardware and software and create other conditions required . . .
 17 to implement operational/technical measures.⁸

18 Palow Decl. Ex. L.⁹ The FSB is a Russian agency that carries out both law
 19 enforcement and intelligence activities. *See* Palow Decl. Ex. L, art. 8 [FSB
 20 Act] (defining the main activities of the FSB as “counter-intelligence;

21
 22 ⁸ In 2012, Eugene Kaspersky, CEO of Kaspersky Lab, which is headquartered in Russia and is
 23 one of the world’s largest software security companies, stated that “the FSB ha[d] never made a
 24 request to tamper with his software”. Palow Decl. Ex. K [Noah Shachtman, *Russia’s Top Cyber
 Sleuth Foils US Spies, Helps Kremlin Pals*, *Wired* (July 23, 2012)]. Kaspersky’s statement is
 25 important for verifying – at least implicitly – that the FSB possesses the power to make such a
 26 request.

27 ⁹ The English translation of this provision is contained in an unofficial translation of the
 28 legislation by the Council of Europe and found at Legislationline.org, which is maintained by the
 Organization for Security and Co-operation in Europe. The Library of Congress lists
 Legislationline.org as an online resource for finding translations of Russian laws. Palow Decl.
 Ex. M at 4 [Law Library of Congress, Russian Federation Translation of National Legislation
 into English (March 2012)].

combating terrorism; combating crime; intelligence; border activity; safeguarding information security”); *see also* Palow Decl. Ex. N, at ¶ 30 [Council of Europe, European Commission for Democracy through Law, *Opinion on the Federal Law on the Federal Security Service (FSB) of the Russian Federation* (2012)] (describing the FSB as “exercis[ing] considerable powers, including police powers”).

The UK is also considering legislation to compel companies to hack their own products or services, and it will only take encouragement from the precedent this Order could set. The Investigatory Powers Bill would authorize UK law enforcement and intelligence agencies to hack electronic devices to obtain “communications” or “any other information”, including through surveillance techniques, such as remotely “listening to a person’s communications or other activities.”¹⁰ Palow Decl. Ex. 0 cl. 88 [Investigatory Powers Bill 2015-16, Bill [143] (Gr. Brit.) [hereinafter “IPB”]]. The Investigatory Powers Bill explicitly compels “telecommunications providers” to assist the UK government in implementing its hacking operations, unless “not reasonably practicable.”¹¹ *Id.* at cl. 111. In addition, the Investigatory Powers Bill authorizes the UK government to issue “National Security Notices” and “Technical Capability Notices”, both of which could compel telecommunications providers to assist the government in

¹⁰ The Investigatory Powers Bill refers to this power as “equipment interference”, a vague term that may encompass surveillance techniques beyond hacking.

¹¹ The Investigatory Powers Bill defines telecommunications provider as including “a person who . . . offers or provides a telecommunications service to persons in the United Kingdom”. Palow Decl. Ex. O cl. 223(10) [IPB]. In its submission to the Parliamentary committee examining the Investigatory Powers Bill, Apple indicated that “[w]ith the exception of certain limited retail and human resources data, Apple is not established in the UK”, but that the Bill “makes explicit its reach beyond UK borders to, in effect any service provider with a connection to UK consumers.” Palow Decl. Ex. P ¶¶ 21-25 [Apple Inc. and Apple Distrib. Int’l, *Written Evidence to the UK Parliament Joint Comm. on the Draft Investigatory Powers Bill* (IPB0093) (Jan. 7, 2016) [hereinafter Apple IPB Written Evidence]].

vague and sweeping terms.¹² *Id.* at cls. 216-218. All of these powers could be deployed to force technology companies to undermine the security of their own products and services.¹³ Moreover, such powers would be exercised in secret, for the Investigatory Powers Bill gags telecommunications providers from revealing information about any hacking assistance they may have been forced to provide to the government. *Id.* at cls. 114, 218(8).

Apple's submission to the Parliamentary committee examining the Investigatory Powers Bill highlights the above concerns. Palow Decl. Ex. P [Apple IPB Written Evidence]. With respect to the hacking provisions in particular, Apple expressed dismay that "the bill could make private companies implicated in the hacking of their customers." *Id.* at ¶ 53. Google, Facebook, Twitter, Yahoo, and Microsoft jointly filed a submission to the committee as well, "reject[ing] any proposals that would require companies to deliberately weaken the security of their products via backdoors, forced decryption, or any other means." Palow Decl. Ex. Q ¶ 3(a) [Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc., Written Evidence to the UK Parliamentary Joint Comm. on the Draft Investigatory Powers Bill (IPB0116) (Jan. 7, 2016)]. Apple warned presciently that "[i]f the UK

¹² A National Security Notice would require a telecommunications provider "to carry out any conduct, including the provision of services or facilities" where the UK government "considers [it] necessary in the interests of national security." Palow Decl. Ex. O cl. 216 [IPB Bill]. A Technical Capability Notice would require a telecommunications provider to, *inter alia*, "provide facilities or services of a specified description" or "remov[e] . . . electronic protection applied by or on behalf of that operator to any communications or data." *Id.* at cl. 217.

¹³ Compounding concerns about such powers, the Investigatory Powers Bill lacks a meaningful judicial authorization process, as understood in U.S. legal terms, when the U.K. government seeks a warrant to hack. In this scenario, the Home Secretary may issue a warrant subject to "approval" by a Judicial Commissioner ("JC"), which is a new position created by the Investigatory Powers Bill. *Id.* at cl. 97. Although a JC must have held high judicial office (defined to include the US equivalent of sitting as a district level judge or above), she is appointed by the Prime Minister and sits for a term of three years. *Id.* at cls. 194-195. The Investigatory Powers Bill also places significant limitations on the scrutiny a JC can exercise in reviewing the warrant. *See id.* at cl. 97. And it does not require any form of judicial approval with respect to National Security Notices or Technical Capability Notices. *Id.* at cl. 218.

Government forces these capabilities, there's no assurance they will not be imposed in other places where protections are absent." Palow Decl. Ex. P ¶ 11 [Apple IPB Written Evidence]. That argument applies even more forcefully in the US context. Should the Order stand, Apple and other technology companies will have difficulty mounting credible opposition to the powers the UK government seeks, not least because once the technological capability is developed it will be hard for Apple to refuse to deploy it for other governments.

A host of other countries also try to compel technology companies to undermine the security of their products through the use of "backdoors".¹⁴ BlackBerry Ltd. ("BlackBerry"), a Canadian company, has wrangled with several countries over whether to grant their agencies backdoor access to its customers' encrypted data. In December 2015, BlackBerry was prepared to shut down operations in Pakistan rather than accede to demands from the government to access encrypted communications sent and received in the country. Palow Decl. Ex. R [Katie Collins, *BlackBerry to leave Pakistan after refusing to ditch user privacy*, CNET (Dec. 1, 2015)]. In the past, however, BlackBerry has negotiated arrangements with the United Arab Emirates, Saudi Arabia, and India involving some measure of government access to encrypted data.¹⁵ Palow Decl. Ex. U [Kadhim Shubber, *BlackBerry gives Indian government ability to intercept messages*, Wired (July 11, 2013)]; Palow Decl. Ex. V [Lance Whitney, *RIM averts*

¹⁴ A backdoor is a method for remotely bypassing security to access a program, computer or network. A backdoor can be a legitimate point of access to allow maintenance by an authorized administrator. It can also be an unauthorized point of access. Apple and others contend that what the government is requesting in this case is a "backdoor." *Amici* submit, as explained above, *see supra* p. 6-7, that what the government is asking can also be construed as requiring Apple to hack its own iPhone. Both backdoors and compelled hacking are a serious threat to the security of technology products and services.

¹⁵ BlackBerry has also faced requests for backdoors from Russia and Indonesia; it is unclear how it resolved those requests. *See* Palow Decl. Ex. S [*Government asks RIM to open access to wiretap Blackberry users*, Jakarta Post (Sept. 15, 2011)]; Palow Decl. Ex. T [Maria Kiselyova and Guy Faulconbridge, *BlackBerry firm seeks security 'balance' in Russia*, Reuters (Apr. 25, 2011)].

1 *BlackBerry ban in UAE*, CNET (Oct. 8, 2010)]; Palow Decl. Ex. W [*RIM to share*
2 *some BlackBerry codes with Saudis*, Reuters (Aug. 10, 2010)].

3 Some countries have resorted to “key escrow” systems to try to obtain
4 access to encrypted data.¹⁶ A “key escrow” is a kind of backdoor, in which
5 technology companies offering encryption services (or individuals using
6 encryption) must store copies of decryption keys with the government or a “trusted
7 third party”. Turkey, for example, passed regulations in 2010 “requiring encryption
8 suppliers to provide copies of [decryption] keys to government regulators before
9 offering their encryption tools to users.”¹⁷ Palow Decl. Ex. X ¶ 44 [*2015 Special*
10 *Rapporteur Report*].

11 In 2015, technology companies fought vigorously against a draft
12 Counterterrorism Law in China that would have required both backdoors and a
13 “key escrow” regime. *See* Palow Decl. Ex. Z [Tom Mitchell, *Obama seeks reboot*
14 *of China cyber laws*, Financial Times (Mar. 3, 2015)] (noting that “US and
15 European corporate executives have expressed alarm over . . . Chinese legislation
16 targeting telecom companies [and] internet service providers”); Palow Decl. Ex.
17 AA [Human Rights Watch, *China: Draft Counterterrorism Law a Recipe for*
18 *Abuses* (Jan. 20, 2015)]. The US government also heavily criticized these
19 measures, with President Barack Obama, Secretary of State John Kerry and US

20 ¹⁶ Some countries simply seek to discourage the use of secure technologies altogether, in
21 manners “tantamount to a ban, such as rules (a) requiring licenses for encryption use; (b) setting
22 weak technical standards for encryption; and (c) controlling the import and export of encryption
23 tools.” Palow Decl. Ex. X ¶ 41 [*Report of the Special Rapporteur on the promotion and*
24 *protection of the right to freedom of opinion and expression, David Kaye, delivered to the*
25 *Human Rights Council*, U.N. Doc. A/HRC/29/32, (May 22, 2015) [hereinafter “*2015 Special*
26 *Rapporteur Report*”]. Countries that regulate in one or more of these manners include Ethiopia,
27 Cuba, and Pakistan. *Id.* at ¶ 41 nn. 28-30.

28 ¹⁷ These regulations are available in English on the website of Turkey’s Information and
Communications Technologies Authority. Palow Decl. Ex. Y art. 5 [Information and
Communication Technologies Authority, By Law on the Procedures and Principles of Encoded
or Encrypted Communication between Public Authorities and Organizations and Real and Legal
Persons in Electronical [sic] Communication Service (Oct. 23, 2010)].

1 Trade Representative Michael Froman advocating against them in direct exchanges
 2 with the Chinese government. *See* Palow Decl. Ex. BB [Ankit Panda, *Beijing*
 3 *Strikes Back in US-China Tech Wars*, The Diplomat (Mar. 6, 2015)]; Palow Decl.
 4 Ex. CC [Jeff Mason, *Exclusive: Obama sharply criticizes China's plans for new*
 5 *technology rules*, Reuters (Mar. 2, 2015)] (“In an interview with Reuters,
 6 [President] Obama said he was concerned about Beijing’s plans . . . [to] require
 7 technology firms to hand over [decryption] keys, the passcodes that help protect
 8 data, and install security ‘backdoors’ in their systems to give Chinese authorities
 9 surveillance access.”). The final version of the Counterterrorism Law, which
 10 passed in December 2015, softened some of these requirements, a small victory
 11 that may not have been won had this Court’s Order existed at the time. *See* Palow
 12 Decl. Ex. DD [Samm Sacks, *Apple in China, Part I: What Does Beijing Actually*
 13 *Ask of Technology Companies?*, Lawfare (Feb. 22, 2016)]. However, the
 14 Counterterrorism Law still requires technology companies to provide “technical
 15 interfaces, decryption, and other technical assistance and support” and Chinese
 16 authorities will be working out the details of the types of assistance companies will
 17 be compelled to provide in the coming year.¹⁸ *Id.*

18 China is still in the midst of fleshing out a new legal and regulatory regime
 19 governing technology companies. *See id.* It is poised to become Apple’s largest
 20 market during this period and Chinese officials will be closely observing the US’s
 21 approach to secure technologies. *See* Palow Decl. Ex. EE [Alice Truong, *What*

22 ¹⁸ Decryption usually takes one of two forms: mandatory key disclosure or targeted decryption
 23 orders. The former requires disclosure of the key necessary for decryption, permitting the
 24 government to access all information protected by the key. The latter requires only that specific
 25 information be decrypted and then turned over to the government. Both forms of decryption can
 26 require “corporations to cooperate with Governments, creating serious challenges that implicate
 27 individual users online.” Palow Decl. Ex. X ¶ 45 [2015 *Special Rapporteur Report*]. Several
 28 countries authorize key disclosure by law, including France, Spain and the United Kingdom. *Id.*
 at ¶ 45 n.35.

Chinese slowdown? *Apple's sales double in China on iPhone growth*, Quartz (Oct. 27, 2015)]. In July 2015, the Chinese government released a draft Cybersecurity Law, which outlines obligations for technology companies operating in China. *Id.* Those obligations include requiring that companies “provide unspecified ‘necessary assistance’ to police when investigating crimes and for ‘state security reasons’”. Palow Decl. Ex. FF [Human Rights Watch, *Submission by HRW to the National People's Congress Standing Committee on the draft Cybersecurity Law* (Aug. 4, 2015)]. The outcome of this case and other US government requests to compel companies to undermine the security of their products are likely to influence the final version of the Cybersecurity Law. Indeed, a Chinese official has stated that China studied U.S. and European national laws in drafting the Counterterrorism Law and implied those examples may have influenced its decision to soften its approach. Palow Decl. Ex. GG [*Provisions of China's counterterrorism bill inspired by foreign laws: official*, Xinhua (Dec. 27, 2015)].

D. Other Countries Will Compel Technology Companies to Undermine the Security of their Products and Services In Order to Commit Civil and Human Rights Abuses

Secure technologies are fundamental to the protection of the right to freedom of expression and opinion. States take advantage of weaknesses in these technologies to attack these rights. These attacks, including through mass surveillance, data collection, and online censorship and filtering, are well documented. *See* Palow Decl. Ex. HH [*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, delivered to the Human Rights Council*, U.N. Doc. A/HRC/23/40 (Apr. 23, 2013)]; Palow Decl. Ex. II ¶ 34 [*Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, delivered to the Human Rights Council*, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009)] (describing how surveillance measures

1 in many countries “have a chilling effect on users, who are afraid to visit websites,
2 express their opinions or communicate with other persons for fear that they will
3 face sanctions”). In the face of these attacks, secure technologies:

4 enable private communications and can shield an opinion from outside
5 scrutiny, particularly important in hostile political, social, religious and
6 legal environments. Where States impose unlawful censorship through
7 filtering and other technologies, [they] . . . may empower individuals to
8 circumvent barriers and access information and ideas without the
9 intrusion of authorities. Journalists, researchers, lawyers and civil
10 society rely on [secure technologies] to shield themselves (and their
11 sources, clients and partners) from surveillance and harassment.

12 Palow Decl. Ex. X ¶ 12 [*2015 Special Rapporteur Report*].

13 The US government has also recognized the critical importance of secure
14 technologies to protect the rights to freedom of expression and association. It has
15 voiced its support for “the development and robust adoption of strong encryption,
16 which is a key tool to . . . promote freedoms of expression and association” and is
17 “especially important in sensitive contexts where attribution could have negative
18 political, social or personal consequences or when the privacy interests in the
19 information are strong.” Palow Decl. Ex. JJ, at 1 [U.S. Submission to the Special
20 Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression
21 (Feb. 26, 2015)]. It has accordingly, “as a matter of policy . . . long supported the
22 development and use of strong encryption and anonymity-enabling tools online.”

23 *Id.* at 2. In particular, it has

24 provided funding to support the development and dissemination of anti-
25 censorship and secure communications technologies to ensure that
26 human rights defenders and vulnerable civil society communities, such
27 as journalists, LGBT activists and religious minorities, operating in
28

1 repressive contexts are able [sic] communicate securely, associate
2 safely, and express themselves freely online.

3 *Id.*

4 Secure technologies can also play a vital role in protecting other
5 fundamental civil and human rights. Some states have exploited vulnerabilities in
6 these technologies not only to target activists, dissidents, and political opponents
7 but also to arrest and torture these individuals. *See generally* Palow Decl. Ex. KK
8 [The Right to Privacy in the Digital Age, G.A. Res. 69/166, pmb., U.N. Doc.
9 A/Res/69/166 (Feb. 10, 2014)] (“[n]oting with deep concern that, in many
10 countries, persons and organisations engaged in promoting and defending human
11 rights and fundamental freedoms frequently face threats and harassment and suffer
12 insecurity as well as unlawful or arbitrary interference with their right to privacy as
13 a result of their activities”). The Committee to Protect Journalists, for example, has
14 advised reporters to use encryption tools when communicating with sources in
15 Syria or risk their well-being. Palow Decl. Ex. LL [Eva Galperin, *Don’t get your*
16 *sources in Syria killed*, Committee to Protect Journalists (May 21, 2012)]
17 (describing the Syrian surveillance regime as “extensive” and the use of malware
18 by “pro-Syrian government hackers”). In Bahrain, former political prisoners have
19 reported that they were beaten and interrogated while being shown transcripts of
20 text messages and other communications intercepted by the government. Palow
21 Decl. Ex. MM [Vernon Silver & Ben Elgin, *Torture in Bahrain Becomes Routine*
22 *With Help From Nokia Siemens*, Bloomberg (Aug. 22, 2011)]. Activists and
23 journalists detained in Iran have reported similar incidents. Palow Decl. Ex. NN
24 [Ben Elgin, Vernon Silver & Alan Katz, *Iranian Police Seizing Dissidents Get Aid*
25 *of Western Companies*, Bloomberg (Oct. 31, 2011)] (describing the experience of a
26 journalist who was shown “transcripts of his mobile phone calls, e-mails and text
27 messages during his detention”).
28

1 **V. CONCLUSION**

2 For all of these reasons, Privacy International and HRW strongly urge the
3 Court to consider the wider implications of the Order compelling Apple to assist in
4 the search of the iPhone at issue.

5
6
7
8
9
10 Dated: March 3, 2016

Respectfully submitted,

11
12 By 
13 Caroline Wilson Palow (SBN 241031)
14 Scarlet Kim
15 PRIVACY INTERNATIONAL
16 62 Britton Street
17 London EC1M 5UY
18 United Kingdom
19 Telephone: +44.20.3422.4321
20 caroline@privacyinternational.org

21 Attorneys for *Amici Curiae*
22 Privacy International and
23 Human Rights Watch
24
25
26
27
28

PROOF OF SERVICE

I am a citizen of the United States of America and employed in London, the United Kingdom. I am over the age of 18 and not a party to the within action. My business address is Privacy International, 62 Britton Street, London EC1M 5UY, United Kingdom.

On March 3, 2016, I caused to be served through mail (FedEx) and/or e-mail on each person on the attached Service List the foregoing document described as:

**BRIEF OF *AMICI CURIAE* PRIVACY INTERNATIONAL
AND HUMAN RIGHTS WATCH**

Service List


Service Type	Counsel Served	Party
E-mail*	Theodore J. Boutrous, Jr. Nicola T. Hanna Eric D. Vandeverde 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 evandeverde@gibsondunn.com	Apple, Inc.
E-mail*	Theodore B. Olson Gibson, Dunn & Crutcher LLP 1050 Connecticut Avenue, N.W. Washington, D.C. 20036-5306 Telephone: (202) 955-8500 Facsimile: (202) 467-0539 Email: toolson@gibsondunn.com	Apple, Inc.
E-mail*	Marc J. Zwillinger Jeffrey G. Landis Zwillgen PLLC	Apple, Inc.

	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	
Mail & E-mail	Eileen M. Decker Patricia A. Donahue Tracy L. Wilkison Allen W. Chui 1500 United States Courthouse 7312 North Spring Street Los Angeles, California 90012 Telephone: (213) 894-0622/2435 Facsimile: (213) 894-8601-7520 Email: Tracy.Wilkison@usdoj.gov Allen.Chui@usdoj.gov	United States of America

*Apple, Inc. has consented in writing to service by electronic means in accordance with Federal Rule of Civil Procedure 5(b)(E), Local Civil Rule 5-3.1.1, and Local Criminal Rule 49-1.3.2(b).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I have made service at the direction of a member of the bar of this Court.

Executed on March 3, 2016 in London, United Kingdom


Sara Nelson