| 1 2 3 4 5 6 7 8 | 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 |
|--------------------------------------|--|
| 9 | HUMAN RIGHTS WATCH |
| 10 | HOWAN RIGHTS WATCH |
| 11 | UNITED STATES DISTRICT COURT |
| 12 | CENTRAL DISTRICT OF CALIFORNIA |
| 13 | |
| | EASTERN DIVISION |
| 14 | IN THE MATTER OF THE SEARCH) ED No. CM 16-10 (SP) OF AN APPLE IPHONE SEIZED) |
| 16 17 | DURING THE EXECUTION OF A) BRIEF OF AMICI CURIAE SEARCH WARRANT ON A BLACK) PRIVACY INTERNATIONAL AND LEXUS IS300, CALIFORNIA) HUMAN RIGHTS WATCH |
| 18 | LICENSE PLATE 35KGD203 |
| 19 |) Hearing: |
| 20 |) Date: March 22, 2016) Time: 1:00 p.m. |
| 21 |) Place: Courtroom 3 or 4 |
| 22 |) Judge: Hon. Sheri Pym |
| 23 | |
| 24 | |
| 25 | |
| 26 | |
| 27 | |
| 28 | |
| | |

TABLE OF CONTENTS

| I. | INTRODUCTION |
|------|--|
| II. | INTERESTS OF AMICI CURIAE |
| | |
| III. | BACKGROUND |
| | A. The iPhone and its Passcode. |
| | B. Procedural History |
| 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 |
| | B. Compelling Technology Companies to Undermine the Security of their |
| | Products and Services Threatens the Security of the Internet |
| | 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. |
| | 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 |
| V. | CONCLUSION |
| | |

TABLE OF AUTHORITIES

OTHER AUTHORITIES

| Alice Truong, What Chinese slowdown? Apple's sales double in China on iPhone growth, Quartz (Oct. 27, 2015)19 |
|--|
| Andrea Peterson, Forbes Web site was compromised by Chinese cyberespionage group, researchers say, 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, Written Evidence to the UK Parliament Joint Comm. on the Draft Investigatory Powers Bill (IPB0093) (Jan. 7, 2016)14, 15, 16 |
| Apple Inc., iOS Security: iOS 9.0 or later (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, Data and Goliath (2015)10 |
| Council of Europe, European Commission for Democracy through Law, <i>Opinion</i> on the Federal Law on the Federal Security Service (FSB) of the Russian Federation (2012)14 |
| Dep't of Homeland Security, <i>Mobile Security Tip Card12</i> |
| 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., Written Evidence to the UK Parliamentary Joint Comm. on the Draft Investigatory Powers Bill (IPB0116) (Jan. 7, 2016)15 |
| Federal Law of the Russian Federation on the Federal Security Service Act (no. 40-FZ) 199513 |

| 1 2 | Human Rights Watch, China: Draft Counterterrorism Law a Recipe for Abuses (Jan. 20, 2015)17 |
|--------------|--|
| 3 4 | Human Rights Watch, Submission by HRW to the National People's Congress Standing Committee on the draft Cybersecurity Law (Aug. 4, 2015)19 |
| 5 6 7 | Turkey 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) |
| 8 | Investigatory Powers Bill 2015-16, Bill [143] (Gr. Brit.) 14, 15 |
| 9 | Jeff Mason, Exclusive: Obama sharply criticizes China's plans for new technology rules, Reuters (Mar. 2, 2015)18 |
| 11 12 | Kadhim Shubber, <i>BlackBerry gives Indian government ability to intercept messages</i> , Wired (July 11, 2013)16 |
| 13 | Katie Collins, <i>BlackBerry to leave Pakistan after refusing to ditch user privacy</i> , CNET (Dec. 1, 2015)16 |
| 15 16 | Kevin Poulsen, FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, Wired (Sept. 13, 2013)9, 10 |
| 17 | Lance Whitney, RIM averts BlackBerry ban in UAE, CNET (Oct. 8, 2010)17 |
| 18 | Law Library of Congress, Russian Federation Translation of National Legislation into English (March 2012)13 |
| 20 21 22 | Letter to Court, In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15-MC-1902 (E.D.N.Y. Feb. 17, 2016), Dkt. 2712 |
| 23 | Martin Kaste, Slippery Slope? Court Orders Apple to Unlock Shooter's iPhone, NPR (Feb. 18, 2016)12 |
| 25 26 | Noah Shachtman, Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals, Wired (July 23, 2012)13 |
| 27 | Patrick Howell O'Neill, <i>How cybercriminals use major news events to attack you</i> , The Daily Dot (Aug. 5, 2013)9 |

| 1 2 | President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (Dec. 12, 2013)11 |
|----------|---|
| 3 | Provisions of China's counterterrorism bill inspired by foreign laws: official, Xinhua (Dec. 27, 2015)19 |
| 5 6 | 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) |
| 8 9 | Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, delivered to the Human Rights Council, U.N. Doc. A/HRC/29/32, (May 22, 2015)17, 18, 20 |
| 11 | 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)19 |
| 13 14 | RIM to share some BlackBerry codes with Saudis, Reuters (Aug. 10, 2010)17 |
| 15 | Samm Sacks, Apple in China, Part I: What Does Beijing Actually Ask of Technology Companies?, Lawfare (Feb. 22, 2016) |
| 16 17 | The Right to Privacy in the Digital Age, G.A. Res. 69/166, pmbl., U.N. Doc. A/Res/69/166 (Feb. 10, 2014)21 |
| 18 | Tom Mitchell, Obama seeks reboot of China cyber laws, Fin. Times (Mar. 3, 2015) |
| 20 | U.S. Submission to the Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression (Feb. 26, 2015) |
| 22 | Vernon Silver & Ben Elgin, Torture in Bahrain Becomes Routine With Help From |
| 24 | Nokia Siemens, Bloomberg (Aug. 22, 2011)21 |
| 25 | |
| 26 | |
| 27 | |
| 28 | |

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? 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.

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 the protection of civil and human rights. Countries may seek to compel technology 2 companies to impair security for illegitimate purposes, including to stifle 3 expression, crush dissent, and facilitate arbitrary arrest and torture. In these 4 societies, secure technologies protect all members of society but especially 5 vulnerable ones – such as journalists, human rights defenders, and political 6 7 activists – by giving them a safe space to communicate, research, and organize. The U.S., by compelling technology companies to roll back these protections, risks 8 exposing the millions of individuals who reside and work in these places to abuse 9 10 11 12

13

14

15

16

17

18

19

20

21

22

23

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

Security features – including encryption and other measures – are integral to

II. **INTERESTS OF AMICI CURIAE**

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

²⁴ 25

²⁶ 27

²⁸

vulnerabilities in computer security, first with the goal of reporting or repairing them ("white hat"), but later to exploit them ("black hat"). The black hat iteration of hacking is the mainstream 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.

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

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

III. BACKGROUND

A. The iPhone and its Passcode

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

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

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

B. Procedural History

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

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Id. at *2.

hardware

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

Apple's reasonable technical assistance shall accomplish the following

function whether or not it has been enabled; (2) it will enable the FBI to

submit passcodes to the SUBJECT DEVICE for testing electronically

available on the SUBJECT DEVICE; and (3) it will ensure that when

on the device will not purposefully introduce any additional delay

between passcode attempts beyond what is incurred by Apple

the FBI submits passcodes to the SUBJECT DEVICE, software running

via the physical device port, Bluetooth, Wi-Fi, or other protocol

three important functions: (1) it will bypass or disable the auto-erase

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. 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".

2
 3
 4

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

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

Technical feasibility is a meaningless constraint because, in technical terms, many strategies for undermining the security of an iPhone may be feasible. As Apple hypothesizes, if it

can be forced to write code in this case to bypass security features and create new accessibility, what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously

⁴ Apple argues that the government's reading of the All Writs Act is unbounded for two reasons. First, it recognizes no contextual limitation; any warrant in any investigation could provide the basis for a supplemental All Writs Act Order to a third party. Dkt. 16 at *3 [Motion to Vacate]. Second, "under the government's formulation, any party whose assistance is deemed 'necessary' 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.

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

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

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

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

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

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

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

⁵ Apple presents the security hazards inherent in developing new software to weaken the iPhone's passcode protection, even if it is only to be deployed on a single iPhone. Dkt. 16 at *13-*14 [Motion to Vacate] (noting that the entire process "would need to be logged and recorded in case Apple's methodology is ever questioned, for example in court"); *id.* at *24-*25 (describing the alternative to building and destroying software for each law enforcement demand as "securing against disclosure or misappropriation" all physical and digital materials related to 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.

technique" because "[a]s soon as a tech firm updates its software, the tool vanishes").

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

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

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.].

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

In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them Eliminating the vulnerabilities — 'patching' them — strengthens the security of US Government, critical infrastructure, and other computer systems.

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

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

Alternatively, the government, which already stockpiles vulnerabilities, may be incentivized to expand this activity in order to share such vulnerabilities with companies compelled to host "watering hole" attacks. *See* Palow Decl. Ex. D [*Meet the woman*] ("Hess acknowledged that the 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

2

6

5

8

7

10

12 13

14 15

16 17

18

1920

21

2223

24

25

2627

28

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

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

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

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

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

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

into English (March 2012)].

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

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

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

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

⁸ In 2012, Eugene Kaspersky, CEO of Kaspersky Lab, which is headquartered in Russia and is one of the world's largest software security companies, stated that "the FSB ha[d] never made a 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 important for verifying – at least implicitly – that the FSB possesses the power to make such a request.

⁹ The English translation of this provision is contained in an unofficial translation of the 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

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." 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." 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

who . . . offers or provides a telecommunications service to persons in the United Kingdom".

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

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)

"makes explicit its reach beyond UK borders to, in effect any service provider with a connection

Palow Decl. Ex. O cl. 223(10) [IPB]. In its submission to the Parliamentary committee

(Jan. 7, 2016) [hereinafter Apple IPB Written Evidence]].

The Investigatory Powers Bill refers to this power as "equipment interference", a vague term that may encompass surveillance techniques beyond hacking.
 The Investigatory Powers Bill defines telecommunications provider as including "a person

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

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

with respect to National Security Notices or Technical Capability Notices. Id. at cl. 218.

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

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

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)].

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

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

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

¹⁶ Some countries simply seek to discourage the use of secure technologies altogether, in

tools." Palow Decl. Ex. X ¶ 41 [Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, delivered to the

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

Persons in Electronical [sic] Communication Service (Oct. 23, 2010)].

Cuba, and Pakistan. Id. at ¶ 41 nn. 28-30.

manners "tantamount to a ban, such as rules (a) requiring licenses for encryption use; (b) setting

weak technical standards for encryption; and (c) controlling the import and export of encryption

Human Rights Council, U.N. Doc. A/HRC/29/32, (May 22, 2015) [hereinafter "2015 Special Rapporteur Report"]. Countries that regulate in one or more of these manners include Ethiopia,

Communication Technologies Authority, By Law on the Procedures and Principles of Encoded

or Encrypted Communication between Public Authorities and Organizations and Real and Legal

17 18

20 21

19

22 23

25 26

24

27

28

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

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

¹⁸ Decryption usually takes one of two forms: mandatory key disclosure or targeted decryption orders. The former requires disclosure of the key necessary for decryption, permitting the government to access all information protected by the key. The latter requires only that specific information be decrypted and then turned over to the government. Both forms of decryption can require "corporations to cooperate with Governments, creating serious challenges that implicate individual users online." Palow Decl. Ex. X ¶ 45 [2015 Special Rapporteur Report]. Several 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

2 3 4

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

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

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

The US government has also recognized the critical importance of secure technologies to protect the rights to freedom of expression and association. It has voiced its support for "the development and robust adoption of strong encryption, which is a key tool to . . . promote freedoms of expression and association" and is "especially important in sensitive contexts where attribution could have negative political, social or personal consequences or when the privacy interests in the information are strong." Palow Decl. Ex. JJ, at 1 [U.S. Submission to the Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression (Feb. 26, 2015)]. It has accordingly, "as a matter of policy . . . long supported the development and use of strong encryption and anonymity-enabling tools online." *Id.* at 2. In particular, it has

provided funding to support the development and dissemination of anticensorship and secure communications technologies to ensure that human rights defenders and vulnerable civil society communities, such as journalists, LGBT activists and religious minorities, operating in repressive contexts are able [sic] communicate securely, associate safely, and express themselves freely online.

Id.

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

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

V. **CONCLUSION**

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

Dated: March 3, 2016

Respectfully submitted,

Caroline Wilson Palow (SBN 241031)

Scarlet Kim

PRIVACY INTERNATIONAL

62 Britton Street London EC1M 5UY United Kingdom

Telephone: +44.20.3422.4321

caroline@privacyinternational.org

Attorneys for Amici Curiae Privacy International and Human Rights Watch

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

| | 1900 M Street N.W., Suite 250 | |
|---------------|---------------------------------|------------------|
| | Washington, D.C. 20036 | |
| | Telephone: (202) 706-5202 | |
| | Facsimile: (202) 706-5298 | |
| | Email: marc@zwillgen.com | |
| | jeff@zwillgen.com | |
| Mail & E-mail | Eileen M. Decker | United States of |
| | Patricia A. Donahue | America |
| | 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.Chiu@usdoj.gov | |

*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