DAVID GREENE (SBN 160107)
davidg@eff.org
CINDY COHN (SBN 145997)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JENNIFER LYNCH (SBN 240701)
NATE CARDOZO (SBN 259097)
SOPHIA COPE (SBN 233428)
ANDREW CROCKER (SBN 291596)
JAMIE WILLIAMS (SBN 279046)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amici Curiae Electronic Frontier Foundation and 46 Technologists, Researchers and Cryptographers

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	Case No: 16-cm-00010-SP **~~[PROPOSED]~~ ORDER RE APPLICATION OF ELECTRONIC FRONTIER FOUNDATION AND 46 TECHNOLOGISTS, RESEARCHERS, AND CRYPTOGRAPHERS TO PARTICIPATE IN THIS CASE AS *AMICI CURIAE***

IT IS HEREBY ORDERED that the application of Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers to participate in this case as *amici curiae* is **GRANTED** and the proposed brief submitted with the application is deemed filed.

DATED: March 3, 2016 BY: _____

Honorable Sheri Pym
United States Magistrate Judge

DAVID GREENE (SBN 160107)
davidg@eff.org
CINDY COHN (SBN 145997)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JENNIFER LYNCH (SBN 240701)
NATE CARDOZO (SBN 259097)
SOPHIA COPE (SBN 233428)
ANDREW CROCKER (SBN 291596)
JAMIE WILLIAMS (SBN 279046)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amici Curiae Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	Case No: 16-cm-00010-SP **PROOF OF SERVICE**

I am a citizen of the United States and employed in San Francisco, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is 815 Eddy Street, San Francisco, CA 94109. On this date, I served the following:

[PROPOSED] ORDER RE APPLICATION OF ELECTRONIC FRONTIER FOUNDATION AND 46 TECHNOLOGISTS, RESEARCHERS, AND CRYPTOGRAPHERS TO PARTICIPATE IN THIS CASE AS *AMICI CURIAE*

and caused to be served by U.S. Mail, postage thereon fully prepaid, true and correct copies of the foregoing on:

Theodore B Olson
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 20036-5306
202-955-8668
Fax: 202-530-9575
Email: tolson@gibsondunn.com

Theodore J Boutrous , Jr
Eric David Vandevelde
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
213-229-7000
Fax: 213-229-7520
Email: tboutrous@gibsondunn.com
Email: evandevelde@gibsondunn.com

Nicola T Hanna
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 92612-4412
949-451-3800
Fax: 949-451-4220
Email: nhanna@gibsondunn.com

Marc J Zwillinger
Jeffrey G Landis
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
202-296-3585
Fax: 202-706-5298
Email: marc@zwillgen.com
Email: jeff@zwillgen.com

Counsel for Respondent

Allen W Chiu
AUSA - Office of US Attorney
National Security Section
312 North Spring Street Suite 1300
Los Angeles, CA 90012
213-894-2435
Fax: 213-894-6436
Email: allen.chiu@usdoj.gov

Tracy L Wilkison
AUSA Office of US Attorney
Chief, Cyber and Intellectual Property
Crimes Section
312 North Spring Street 11th Floor
Los Angeles, CA 90012-4700
213-894-0622
Fax: 213-894-0141
Email: tracy.wilkison@usdoj.gov

Counsel for Plaintiff

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed this March 3, 2016 in San Francisco, California

Cynthia Dominguez

DAVID GREENE (SBN 160107)
davidg@eff.org
CINDY COHN (SBN 145997)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JENNIFER LYNCH (SBN 240701)
NATE CARDOZO (SBN 259097)
SOPHIA COPE (SBN 233428)
ANDREW CROCKER (SBN 291596)
JAMIE WILLIAMS (SBN 279046)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amici Curiae Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 3KGD203	Case No: 16-cm-00010-SP **BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND 46 TECHNOLOGISTS, RESEARCHERS, AND CRYPTOGRAPHERS** Date: March 22, 2016 Time: 1:00 PM Courtroom: 3 or 4 Judge: Hon. Sheri Pym

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

INTRODUCTION

What the government blandly characterizes as a request for technical assistance raises one of the most serious issues facing the security of information technology: the extent to which manufacturers of secure devices like Apple can be conscripted by the government to undermine the security of those devices.

Amici curiae submitting this brief have a special interest in helping this Court understand that its Order places a significant burden on the free speech rights of Apple and its programmers by compelling them to write code and then to use their digital signature to endorse that code to the FBI, their customers and the world. Apple's code and digital signature, separately and together, affirm a commitment and belief regarding the authenticity of the code and the value of their customer's privacy and security. The order compels Apple and its engineers to repudiate that belief, and undermine the very security they designed. In other contexts, compelled speech and affirmations of belief that substantially hinder the speaker's ability to communicate its desired message are clearly unconstitutional. That the Order compels the speech and affirmation in code instead of prose does not change the result. The Order is unconstitutional, and thus not permissibly authorized by the All Writs Act.

STATEMENT OF INTEREST

Individual *amici* are technologists, researchers, and cryptographers, including pioneers in digital signature technology, who develop secure technologies and systems and/or rely on them to create many of the digital services at the center of

modern life. The ability to securely shop, bank, communicate, and engage in countless other activities online are made possible by the technologies and systems conceived, built, and tested by *amici*.[1]

Encryption and cryptography-based systems like digital signatures are the linchpin of the security of digital devices and the software that runs on them. *Amici* have a vested interest in ensuring that these systems remain both uncompromised and ubiquitous so that everyone can trust that their activities using those devices are secure. Individual *amici* thus oppose government efforts to compel anyone to develop code that undermines, bypasses or otherwise limits the security that encryption provides and jeopardizes the trust encryption enables.

For 25 years, *amicus* Electronic Frontier Foundation (EFF) has represented the interests of these and many other technology creators as they seek to build the secure infrastructure that all of us can trust. EFF also represents the interests of users of digital devices who need security, privacy, and protection from hackers, malware, and overbroad government surveillance.

TECHNICAL BACKGROUND

The Order here requires Apple to write code that will undermine several security features it intentionally built into the iPhone and then to digitally sign that code to trick a phone into running it. To understand how this Order implicates the

[1] Brief biographies of the amici are found in Appendix A, filed herewith.

First Amendment, *amici* offer some background to explain that a digital signature is a form of endorsement that promotes trust in, and safety of devices, upon which hundreds of millions of people around the world rely every day.

A. Digital Signatures And Apple's Use Of Them As Endorsement

Pioneered by *amici* Martin Hellman, Ronald Rivest, and others, digital signatures are cryptographic systems that are in many ways analogous to physical signatures because they communicate authenticity, trust, and validity of origin. Digital signatures have thus rightly been given a legal significance on par with that of physical signatures. *See, e.g.*, Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 *et seq;* 21 C.F.R. §§ 11.3(5), 11.30 (FDA regulations requiring the use of digital signatures for transmission of electronic records in order to their "ensure the authenticity, integrity, and as appropriate, the confidentiality").

To the extent the analogy breaks down, it is only because digital signatures are *more reliable* communicators than physical signatures. Unlike physical signatures, digital signatures strongly protect against forgery and tampering with documents' contents by mathematically validating the precise content of what a person or organization has signed. They are ubiquitous in commerce and computer security and vital to checking the authenticity of e-mails, devices, computer programs, financial transactions, network connections, websites, and more. In the context of

software updates for computers and smartphones, digital signatures ensure a person downloading the update that he or she is receiving it from the trusted source. Digital signatures allow people to log in securely via trustworthy Internet accounts, and are required for modern access control devices like bankcards.

When Apple signs code, its digital signature communicates Apple's trust in that code. The signature is its endorsement and stamp of approval that communicates the company's assurance that each and every line of signed code was produced by or approved by Apple.[2]

Apple has shown a strong commitment to protecting the integrity and trust of this security system, using its signing key to communicate that it has done its best to ensure that signed code will protect the features designed by Apple to secure the device's user against unauthorized access. Similarly, Apple's signing process prevents against the intentional introduction of security vulnerabilities into its operating system. Apple's choice to require that any operating system updates be digitally signed is a powerful part of protecting the devices' security.[3] Thus, even if

---

[2] Apple's signature is the result of a mathematical calculation using a secret numeric signing key known only to Apple. The signature enables an Apple device to use its own verification key to verify that the software is indeed produced by Apple and has not been modified by any third party. Only someone in possession of Apple's secret key can produce a signature with the appropriate mathematical properties to be recognized as valid.

[3] For this reason, the signing key is a very important piece of information, among the crown jewels of the entire company. Consistent with the best practices in the information security field, the signing key must be subject to extreme precautions against unauthorized disclosure.

the government wrote its own version of iOS without Apple's compelled assistance, it would still need Apple to sign the software, endorsing it as authentic, in order for the phone to accept the code.

B. The Code The Order Compels Apple To Write

The Order also compels Apple to have its programmers write code that will undermine its own system, disabling important security features that Apple wrote into the version of iOS at issue. This code would defeat the very purpose of the security features: to protect users against access by someone who has stolen the phone or otherwise has physical access to it. This protection is important to users, since over 3 million cell phones were stolen in 2015 alone.[4]

The code would defeat the following three security features:

- erase its keys after 10 incorrect passcode guesses (if enabled);
- impose increasingly long delays after consecutive incorrect passcode guesses to slow down guessing (also known as "rate limiting"); and
- requires individual passcodes be typed in by hand.

These features are intended to protect the tremendously sensitive information that is stored and processed by mobile phones, in response to widespread anxiety about mobile phone safety and security and reflect Apple's commitment to robust

[4] Consumer Reports, *3.1 Million Smart Phones Were Stolen In 2013, Nearly Double the Year Before* (Apr. 17, 2014), http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html.

security engineering.[5] Apple's ongoing effort to develop and document these robust security features is also its response to its customers' demand for safer mobile devices, and reflects industry best practices in several respects.[6]

Each of these security features represents a deliberate choice by Apple in what the code says and does, and each serves Apple's broader purpose of making good on its promise of security to its customers. To remove or disable these security features, Apple's programmers must edit iOS, writing new code they do not want to write, and with which Apple not only vehemently disagrees, but that it believes is wrong for society as a whole.

By compelling Apple to write and then digitally sign new code, the Order forces Apple to first write a message to the government's specifications, and then adopt, verify and endorse that message as its own, despite its strong disagreement with that message. The Court's Order is thus akin to the government dictating a letter endorsing its preferred position and forcing Apple to transcribe it and sign its unique and forgery-proof name at the bottom.

---

[5] *See generally* Apple, "iOS Security" (Sept. 2015), *available at:* https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[6] *See, e.g.,* National Institute of Standards and Technology, NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications (Dep't of Commerce, December 2010) at 6 (recommending use of a high iteration count in key derivation for encrypted storage to discourage brute force attacks); Federal Trade Commission, "Start With Security: A Guide for Business" (Federal Trade Commission, June 2015) *available at:* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (noting requirement that services that accept passwords should "suspend or disable user credentials after

ARGUMENT

I. THE FIRST AMENDMENT PROHIBITS THE GOVERNMENT FROM COMPELLING A PERSON TO SPEAK, ESPECIALLY WHEN THE COMPULSION HINDERS THE SPEAKER'S ABILITY TO COMMUNICATE ITS DESIRED MESSAGE

The Order is unconstitutional because it compels Apple to express itself in conflict with its stated beliefs. The Order forces Apple to say something it does not want to say and that it believes is "dangerous."[7] It then forces Apple to endorse code it does not want to endorse and thereby undermine the trust it has established in its digital signature.

Each of these acts of compelled expression implicate the First Amendment independently, but together they are even more harmful, hindering Apple's ability to communicate its desired messages to its users, and to the world, into the future.

As the Supreme Court has repeatedly held, "it is . . . a basic First Amendment principle that 'freedom of speech prohibits the government from telling people what they must say.'" *Agency for Int'l Development v. Alliance for Open Society Int'l*, 133 S. Ct. 2321, 2327 (2013) ("*AID*") (quoting *Rumsfeld v. Forum for Academic and Institutional Rights, Inc.,* 547 U. S. 47, 61 (2006)). "'At the heart of the First Amendment lies the principle that each person should decide for himself or herself

---

a certain number of unsuccessful login attempts" to prevent brute force attacks).

[7] *See* Tim Cook, "A Message to Our Customers." Apple.com (Feb. 16, 2016) *available at:* http://www.apple.com/customer-letter/ The software the government wants Apple to produce and sign "is not software that Apple wants created, deployed or released." Neuenschwander Declaration, ¶ 28.

the ideas and beliefs deserving of expression, consideration, and adherence.'" *Id.* (quoting *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 641 (1994)). The compelled speech doctrine prevents the Government from "manipulat[ing] the public debate through coercion rather than persuasion." *Turner Broadcasting*, 512 U.S. at 641. "The government may not . . . compel the endorsement of ideas that it approves." *Knox v. SEIU*, 132 S. Ct. 2277, 2288 (2012)

As a result, government mandates that one speak or publish are subject to exacting strict scrutiny. *Pacific Gas & Elec. Co. v. Public Util. Comm'n of Cal.*, 475 U.S. 1, 20–21 (1986) ("*PG&E*"); *Frudden v. Pilling*, 742 F.3d 1199, 1203 (9th Cir. 2014). A speech mandate will thus be unconstitutional unless it is a narrowly tailored means of serving a compelling state interest. *Frudden*, 742 F.3d at 1207. *But see Miami Herald Co. v. Tornillo*, 418 U.S. 241, 258 (1974) (finding speech compulsion to be per se unconstitutional intrusion into the editorial process of a newspaper without strict scrutiny analysis).

The "compelled speech" doctrine is a flexible doctrine with broad application. It has been applied to the full spectrum of expression, and mixed conduct and expression, well beyond the conventional spoken or written word, and in a variety of contexts.[8] *AID*, 133 S. Ct. at 2328–39. For example, in *Wooley v. Maynard*, 430 U.S.

[8] The compelled speech doctrine protects corporations to the same extent it protects human beings, including both commercial and non-commercial entities. *See, e.g., Riley v. Nat'l Federation of the Blind of N.C.*, 487 U.S. 781 (1988) (charitable solicitation by nonprofit entities); *PG&E*, 475 U.S. 1 (private energy utility); *Video*

705, 713 (1977), the Supreme Court struck down a New Hampshire law requiring automobiles to display license plates bearing the state motto "Live Free or Die." In *Hurley v. Irish–American Gay, Lesbian and Bisexual Group of Boston, Inc.*, 515 U.S. 557, 564 (1995), the Court found that compelling organizers of a private parade to include a group whose message the parade organizers wanted to exclude unconstitutionally interfered with the parade organizers' desired message. Importantly for this case, the Court rejected the Massachusetts appellate courts' findings that the parade was conduct, not speech, and had no articulable message or purpose, and thus raised no First Amendment problem. *Id.* In *West Virginia Bd. of Ed. v. Barnette*, 319 U.S. 624, 636 (1943), the Court struck down a state law requiring public school students to both salute the American flag and recite the Pledge of Allegiance. And in *Frudden*, 742 F.3d at 1206, the Ninth Circuit applied the compelled speech doctrine to strike down school's uniform policy requiring all students to wear shirts with the motto "Tomorrow's Leaders."

Of particular relevance here, the compelled speech doctrine prevents the government from forcing its citizens to be hypocrites. *See AID*, 133 S. Ct. at 2331 (explaining that the speech compulsion would cause the speaker to express its own beliefs "only at the price of evident hypocrisy"). Indeed, the doctrine is founded on

---

Software Dealers Ass'n v. Schwarzenegger, 556 F.3d 950 (9th Cir. 2009), *aff'd on other grounds sub nom., Brown v. Entertainment Merchants Ass'n*, 131 S. Ct 2729 (2011) ("*VSDA*") (video game manufacturers and sellers).

the importance of preserving personal integrity through autonomy of thought and action: "[W]hen dissemination of a view contrary to one's own is forced upon a speaker intimately connected with the communication advanced, the speaker's right to autonomy over the message is compromised." *Hurley*, 515 U.S. at 576.

The prohibition on compelled speech is thus especially potent when the government requires the speaker to affirm a belief the speaker does not hold. "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein." *Barnette*, 319 U.S. at 642. *See also Wooley*, 430 U.S. at 714 ("[W]e are faced with a state measure which forces an individual, as part of his daily life—indeed, constantly while his automobile is in public view—to be an instrument for fostering public adherence to an ideological point of view he finds unacceptable.").

Nevertheless, the doctrine applies regardless of whether the compelled speech contains a discernible ideological message, *Frudden*, 742 F.3d at 1206, or the speaker has an ideological motive for refusing to speak. *Wooley,* 430 U.S. at 713 n.10.

A speech compulsion is thus almost always unconstitutional when, as here, it interferes with the speaker's general ability to communicate its desired message.

Riley, 487 U.S. at 795 ("Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech."). This is true even when it is clear that the speaker is communicating the government's message and not its own. In *AID*, 133 S. Ct. at 2322, the Supreme Court thus explained that forcing plaintiff to "pledge allegiance to the Government's policy of eradicating prostitution," in exchange for accepting government funds, would harm the speaker's ability to express its contrary viewpoint when it was not using the government's funds.

Likewise, the compelled speech doctrine prohibits the government from requiring persons to use their own communication channels and resources to disseminate the government's preferred message. Thus, in *PG&E*, 475 U.S. at 20–21, the Court struck down a mandate that a private utility include a consumer watchdog's newsletter in the envelope the utility used to mail bills to customers. Likewise, in *Wooley*, 430 U.S. at 713, the Court held the statute unconstitutional because it required citizens to use their cars as mobile billboards for the state's message. And in *Tornillo*, 418 U.S. at 258, the Court struck down a Florida right-of-reply law that required any newspaper that criticized a political candidate to publish that candidate's reply in the newspaper.[9]

[9] The compelled speech doctrine has been applied in full effect in contexts in which speakers often have somewhat reduced First Amendment rights, such as public schools, *Barnette*, 319 U.S. 624; *Frudden*, 742 F.3d 1199; highly regulated industries like utilities, *PG&E*, 475 U.S. 1; and product advertising. *VSDA*, 556 F.3d 950 (finding statutory requirement that video game retailers place government-approved rating on packaging to be an unconstitutional speech compulsion). An exception, not

The government's speech compulsion is no less offensive when the speaker has the opportunity to disavow the message it has been forced to communicate. *AID*, 133 S. Ct. at 2331-32. In *Wooley,* Maynard could have placed a bumper sticker on his car that expressly rejected the state motto on his license plate. He could have written editorials making his beliefs known or testified in public hearings. But the harm to his First Amendment rights would persist. The speech compulsion burdened him with the responsibility of publicly and continuously disclaiming the speech he was compelled to display.

II. WRITING AND SIGNING CODE IS SPEECH PROTECTED BY THE FIRST AMENDMENT.

This case involves technological communication in ways that many speech cases do not. But the form of communication does not alter the fundamental First Amendment principles at stake. The values that underlie the compelled speech doctrine—freedom of thought and integrity in one's beliefs—are as fundamental here as in any other context. If Apple were required to declare verbal support for the government's belief that technological backdoors or other forms of mandatory access by the government are necessary, such as in a blog post or public testimony, it would

---

applicable here, is when the government compels purely factual and noncontroversial commercial speech for the purposes of preventing consumer deception. *Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626 (1985). In such situations the compelled speech requirement is reviewed under a less rigorous standard. *Id.* That standard does not apply where the commercial actor is required to "carry[] the State's controversial opinion" in its advertising. *VSDA*, 556 F.3d at 953, 956.

be easy to spot the First Amendment violation. That Apple's communicates in the language of computer code and Apple's digital signature verifying that code, rather than spoken words, in a parade, on a t-shirt or a license plate, does not make the prohibition on compelled speech any less applicable.

It is long settled that computer code, including the code that makes up Apple's iOS operating system and its security features including encryption, is a form of protected speech under the First Amendment. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000); *Bernstein v. DOJ*, 176 F.3d 1132, 1146 (9th Cir. 1999), *vacated on other grounds*, 192 F.3d 1308 (9th Cir. 1999).[10] Code consistently receives First Amendment protection because code, like a written musical score, "is an expressive means for the exchange of information and ideas." *Junger*, 209 F.3d at 484.

In *Corley*, which similarly considered code that could be used to undermine security, the Second Circuit held that "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in 'code,' *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment." 273 F.3d at 445–46. *See also Hurley*, 515 U.S. at 569 (explaining that

[10] As here, the cases that established First Amendment protection for computer code involved protection for encryption and data protection software. *See e.g. Bernstein,* 176 F.3d at 1136; *Junger,* 209 F.3d at 482; *Corley,* 273 F.3d at 434.

the First Amendment protects not readily understood expression such as "the paintings of Jackson Pollock, music of Arnold Schoenberg and Lewis Carroll's Jabberwocky"); *Board of Trustees of Stanford University v. Sullivan*, 773 F. Supp. 472, 474 (D.D.C. 1991) ("[T]he First Amendment protects scientific expression and debate just as it protects political and artistic expression.").

Code retains its constitutional protection even if it is executable, and thus both expressive and functional "The fact that a medium of expression has a functional capacity should not preclude constitutional protection." *Junger*, 209 F.3d at 484–85. *See also Bernstein*, 922 F. Supp. at 1435–36 (recognizing that the functional nature of source code is "immaterial" in First Amendment analysis). Accordingly, the functional consequences of speech are not a bar to protection, though they may be relevant to whether a regulation burdening the speech is appropriately tailored. *Junger*, 209 F.3d at 485.

III. APPLIED HERE, THE COMPELLED SPEECH DOCTRINE RENDERS THIS COURT'S ORDER UNCONSTITUTIONAL BECAUSE IT FORCES APPLE INTO A POSITION OF HYPOCRISY BETWEEN ITS BELIEFS AND ITS COMPELLED STATEMENTS

A. The Order Compels Apple To Both Speak According To The Government's Specifications And Then Affirm A Belief In That Speech Despite Its Vehement Disagreement With Its Message

Applying the compelled speech doctrine, the Order's mandate that Apple create and sign code according to the government's specifications is unconstitutional.

As set forth in its Motion to Vacate, Apple has taken a strong public stance in

favor of strong encryption on its devices. As Judge Orenstein recently observed in a similar case: "Apple is clearly staking out the position that as a matter of protecting its customers' privacy and data security (and as a matter of securing the benefits it derives from doing so), it does not want the government or anyone else to have access to the information the government would compel it to use to provide the requested assistance at issue here." *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court,* Case No. 1:15-mc-01902-JO (Filed 2/29/16) at 40. The specific security features at issue here, as well as the requirement that all iOS code be signed as verified by Apple, are expressions of its beliefs.

The Order thus forces Apple into a position of hypocrisy which the compelled speech doctrine is meant to prevent. The government's message directly conflicts with both Apple's expressed statements and its assurances to its customers. Forcing Apple to carry that message hinders its ability to express its truly held beliefs in all contexts. Thus, "it is entirely appropriate to take into account the extent to which the compromise of privacy and data security that Apple promises its customers affects not only its financial bottom line, but also its decisions about the kind of corporation that it aspires to be." *Id.* at 39 n.34.

As with government demands that one include undesired participants in a parade, *Hurley*, 515 U.S. at 566, or display an objectionable motto on its vehicle, *Wooley*, 430 U.S. at 713, or assert its opposition to prostitution, *AID*, 133 S. Ct. at

2324–25, the Order here requires Apple to "confess by word or act" not its own position on the security that users require, but the government's.

Moreover, as in *PG&E*, 475 U.S. at 21, and *AID*, 133 S. Ct. at 2326, by being forced to carry the government's message, Apple's own message is irrevocably diminished. That Apple can elsewhere disclaim the position it is being forced to take in complying with the Order did not rectify the underlying problem in *AID*, 133 S. Ct. at 2331–32, and does not do so here.

The hypocrisy the FBI compels here is analogous to the government demanding that authors of books explaining how to improve your home security include flaws within those instructions that would enable the government to easily defeat that security.[11] Such an order would require the author to endorse the government's view of how security should work, and undermine their freedom to express a contrary view in a book with an otherwise contrary message. It would plainly be unconstitutional to compel an author to speak in such a manner. The result does not change because the "book" here is Apple's software and digital signature.

It makes no difference that the Apple's edited code and signature will be communicated only to the government or internally. The compelled loyalty oath struck down in *Speiser v. Randall*, 357 U.S. 513, 515 (1958), required those veterans

[11] *See, e.g.*, Stan Wasilik, *Essential Home Security: A Layman's Guide*, CreateSpace Independent Publishing Platform (2010), *available at* http://www.amazon.com/Essential-Home-Security-Laymans-Guide/dp/1453732039; Daniel Berg, *Build Your Own Secret Bookcase Door*, CreateSpace (2010), *available*

applying for benefits only to submit a form to the government. The loyalty was unconstitutional despite the fact that they were not required to make any type of public affirmation. *Id.* at 529.

Finally, by requiring Apple to use its own resources and communications channels in the form of rewriting iOS and endorsing it with a digital signature, a channel of communication Apple otherwise exclusively controls, the Order offends another of the basic precepts of the compelled speech doctrine. *See PG&E*, 475 U.S. at 21. Apple becomes the "mobile billboard" for the Government's message just as New Hampshire drivers were in *Wooley*, 430 U.S. at 713.[12]

As detailed in Apple's Motion to Vacate, the Order cannot satisfy strict scrutiny, as required by the compelled speech doctrine. It is therefore barred by the First Amendment.

B. The Order Burdens Apple's Ability To Participate In An Important Public Debate

The Order heavily burdens Apple's ability to participate in an active and heated ongoing national debate about digital security, exacerbating the constitutional harm. The discussion concerns the tradeoffs, between the public's increasingly

---

at http://www.amazon.com/Build-Your-Secret-Bookcase-Door/dp/1453760814.

[12] This differentiates this situation from the normal duties of a third party to provide relevant evidence in its possession. Apple is not merely providing purely factual records that it already has or disclosing what it already knows to the government. It must create new expression and then affirm a belief in that new expression, in support of the government's controversial policy position.

important need for technological security and privacy in the digital tools upon which it relies, and the government's desire for as broad as possible access to the data for surveillance and law enforcement purposes.

This debate is robust for good reason. In the past few years, as networks are increasingly exploited by criminals and foreign governments, the nation has become increasingly concerned about weaknesses in the security of digital devices. Successful attacks on the Office of Personnel Management,[13] Sony Pictures,[14] and the private photos and other material of celebrities and others[15] have led government and industry leaders to push for stronger security. Each day brings more news of such attacks and exploits. The situation is so serious that page one of the 2016 Department of Defense Threat Assessment states: "Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and

---

[13] Elizabeth Weise, "Second Hack At OPM May Have Been Worse Than First," USA Today (June 12, 2015), *available at:* http://www.usatoday.com/story/tech/2015/06/12/office-of-personnel-management-hack-china/71146452/

[14] Bruce W. Bennett, "Did North Korea Hack Sony?," Newsweek/The Rand Blog (Dec. 11, 2014) *available at:* http://www.rand.org/blog/2014/12/did-north-korea-hack-sony-pictures-entertainment.html

[15] Charles Riley and Jose Pagliery, "Apple To Beef Up Security Measures After Nude Photo Leak," CNN (Sept. 4, 2014), *available at:* http://money.cnn.com/2014/09/04/technology/security/apple-celebrity-photos/index.html

US Government systems."[16]

Government officials have weighed in of both sides of the debate.[17]

Government officials have drawn attention to the growing "cyber threat" posed by foreign governments, terrorists, criminals and malicious hackers. Indeed, the FBI itself has strongly recommended that Americans minimize the risks posed by these threats by encrypting data and protecting it with a strong password.[18] Similarly, the General Accounting Office, with agreement from the FCC, DHS and NIST, has recommended that device and network providers offer strong encryption to increase

---

[16] James Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," (Feb. 9, 2016) p. 1, *available at:* http://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1313-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-ic-before-the-senate-armed-services-committee-2016.

[17] *See* Brendan Sasso, "The Obama Administration's Encryption Views Are All Over the Map," DefenseOne (Jan. 27, 2016), *available at:* http://www.defenseone.com/technology/2016/01/obama-administrations-encryption-views-are-all-over-map/125463/ ("[A]nother top Obama appointee took the stage at the Newseum in Washington, D.C. to deliver almost the exact opposite message [as that of the Justice Department] . . . to the audience of tech-industry insiders: Encryption helps protect consumers from hackers, argued Terrell McSweeny, a Democratic member of the Federal Trade Commission.").

[18] Federal Bureau of Investigation, "Responding to the Cyber Threat - Speech by Shawn Henry, Executive Assistant Director" (Oct. 20, 2011), *available at:* https://www.fbi.gov/news/speeches/responding-to-the-cyber-threat; Federal Bureau of Investigation, "Smartphone Users Should be Aware of Malware Targeting Mobile Devices and the Safety Measures to Help Avoid Compromise," (Oct. 22, 2012), *available at:* https://www.fbi.gov/sandiego/press-releases/2012/smartphone-users-should-be-aware-of-malware-targeting-mobile-devices-and-the-safety-measures-to-help-avoid-compromise; The FBI is not alone. *See e.g.* Department of Defense iOS 9 Security Guide (Sept. 18, 2015), http://iasecontent.disa.mil/stigs/pdf/U_Apple_iOS_9_V1R0-1_Draft_Configuration_Tables.pdf.

security.[19] The current head of the NSA, Admiral Michael Rogers, has stated: "If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things."[20] Moreover, several prominent former government officials, including the former NSA Director and the Director of National Intelligence, Mike McConnell, the former Homeland Security Secretary Michael Chertoff and the former Deputy Defense Secretary William Lynn have all publicly embraced the position in favor of strong security and expressly rejected the FBI's position.[21]

However, key officials from the law enforcement communities have nevertheless urged a weakening of encrypted communication systems so as to facilitate law enforcement investigations.[22]

---

[19] GAO Report, "Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged," at 22 (September 2012), *available at:* http://www.gao.gov/assets/650/648519.pdf ("Mobile device manufacturers and wireless carriers can implement technical features, such as enabling passwords and encryption to limit or prevent attacks."). In a separate report, the GAO specifically noted the failure of the Census Bureau to do take full advantage of strong encryption in devices used by employees. GAO, "Information Security: Actions Needed by Census Bureau to Address Weaknesses," (January 2013), *available at:* http://www.gao.gov/assets/660/651448.pdf

[20] Atlantic Counsel, "US CYBERCOM AND THE NSA: A Strategic Look with ADM Michael S. Rogers," (January 21, 2016) *available at: http://www.youtube.com/watch?v=wnTGO6OFgCo*

[21] Mike McConnell, Michael Chertoff and William Lynn, "Why the Fear Over Ubiquitous Data Encryption is Overblown," Washington Post (July 28, 2015), *available at:* https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html

[22] For instance, FBI Director James Comey and others have argued that "[i]n a world where users have sole control over access to their devices," law enforcement's ability to obtain evidence from these devices in order to prosecute crime will be impaired. Department of Justice, "Statement of Sally Quillian Yates and James B. Comey"

Members of Congress are on all sides of the debate, with some advocating laws protecting encryption and strong security[23] and others calling for legislation allowing government access to encrypted devices and communications.[24] Importantly, despite consistent advocacy from the FBI for nearly 20 years, [25] Congress has yet to advance, much less pass, legislation that would require companies like Apple to ensure governmental access to data on the devices it sells to the public.[26]

(July 8, 2015), *available at:* http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Yates%20and%20Comey%20Joint%20Testimony1.pdf

[23] House Judiciary Committee Democrats, "Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption," (February 18, 2016), *available at:* http://democrats.judiciary.house.gov/press-release/senior-house-judiciary-committee-democrats-express-concern-over-government-attempts ("Properly understood, strong encryption is our best defense against online criminals—including terrorist organizations.").

[24] "President's Strategy To Defeat Isis," Speech to Congress by Sen. John Cornyn (R-TX) (Dec 15, 2015), *available at:* https://scout.sunlightfoundation.com/search/speeches/encryption. ("Another threat we are going to have to deal with that Director Comey and the Deputy Attorney General raised is the use of encryption as a challenge that hinders the FBI's counterintelligence efforts.")

[25] For instance, in 1992 the FBI's Advanced Telephony Unit warned that within three years Title III wiretaps would no longer work: at least 40% would be unintelligible and in the worst case all might be rendered useless (Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview, slide on Encryption Equipment," (1992), *available at:* https://www.cs.columbia.edu/~smb/Telecommunications_Overview_1992.pdf). Obviously, this has not occurred.

[26] To the contrary, in the case of telecommunications carriers, Congress has rejected such duties. "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a

IV. APPLYING THE COMPELLED SPEECH DOCTRINE HERE IS CONSISTENT WITH OTHER LIMITS ON DISCOVERY

Applying the Compelled Speech doctrine to the Order is consistent with other constitutional rights, common law principles, and state and federal laws that limit access to evidence in civil and criminal cases and protect many different types of speakers from forced testimony. *See generally* Fed. R. Ev. 501.

Although the Supreme Court has recognized the general principle that "the public . . . has a right to every man's evidence," *United States v. Bryan*, 339 U.S. 323, 331 (1950) (quoting 8 J. Wigmore, Evidence § 2192, p. 64 (3d ed. 1940)), parties, including the government, do not have absolute power to compel the production of evidence. Exceptions from this rule "may be justified, . . . by a public good transcending the normally predominant principle of utilizing all rational means for ascertaining the truth." *Trammel v. United States*, 445 U.S. 40, 50 (1980) (internal citations omitted).

Limitations on forced testimony and compelled evidence production that "serve[] public ends," *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981), include constitutional protections like the Fifth Amendment, which protects individuals from compelled self-incrimination;[27] and common law or statutory

---

subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." CALEA, 47 U.S.C. § 1002(b)(3).

[27] *See, e.g., Blau v. United States*, 340 U.S. 159, 161 (1950) (Fifth Amendment protected petitioner's refusal to testify regarding her employment by the Communist

privileges, which require a court to forgo valuable testimony to encourage frank communication between individuals and certain professionals to achieve some greater public good, such as sound legal[28] or medical advice,[29] robust investigative journalism,[30] or intimacy between spouses.[31]

The First Amendment is the source of several of these privileges, including the right to withhold the names of association members, *see NAACP v. Alabama*, 357 U.S. 449 (1958), and the reporter's privilege, *Shoen v. Shoen*, 5 F.3d 1289 (9th. Cir. 1289).

Here, the First Amendment interests are bolstered by the interests of all iPhone users in having secure devices, and the public's broader interest in digital security. Millions of Americans should be able to benefit from the security and personal safety fostered by encryption generally, and the robust encryption Apple provides on its

---

Party or knowledge of its workings).

[28] *See, e.g., Upjohn*, 449 U.S. at 389; *Swidler & Berlin v. United States*, 524 U.S. 399, 401 (1998). .

[29] S*ee, e.g., Jaffee v. Redmond*, 518 U.S. 1, 15 (1996) (psychotherapist-patient privilege).

[30] Forty-nine states and the District of Columbia have reporter "shield laws" embodied in statutes or judicial opinions that, to varying degrees, protect journalists from being forced to disclose sources and unpublished material. *See* Society of Professional Journalists, *Shield Law 101: Frequently Asked Questions*, http://www.spj.org/shieldlaw-faq.asp. California's "shield law," embodied in both the California constitution and in California's rules of evidence, provides reporters with absolute immunity from disclosure of sources and unpublished information and can only be outweighed by a competing constitutional right such as a defendant's right to a fair trial. *See Miller v. Super. Ct*, 21 Cal. 4th 883, 901 (1999).

[31] S*ee, e.g., Trammel v. United States*, 445 U.S. 40, 53 (1980) (spousal privilege).

iPhones specifically. Forcing Apple to rewrite and sign a new version of iOS would be counter to the public interest because it would undermine Apple's ability to ensure user trust in its software. And it would set a dangerous precedent for future weakening of the security of the digital environment. Users would no longer be able to trust Apple's updates to its devices, which are the only route available for eliminating security vulnerabilities after they are discovered, thereby undermining a complex trust ecosystem that is important for the security infrastructure underlying much of modern society.

V. THE ALL WRITS ACT IS LIMITED TO NONBURDENSOME, CONSTITUTIONAL ORDERS

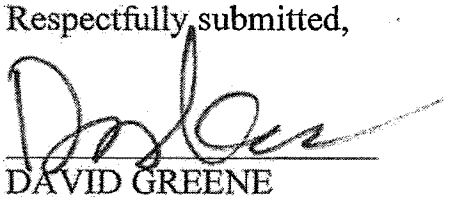
The government's reliance on the All Writs Act does not, and indeed cannot, alter this constitutional calculus. Court must consider whether an AWA order would violate the constitutional rights of third parties, because courts "may not use the All Writs Act to issue a subsequent order to effectuate the first order if the subsequent order is itself unconstitutional." *United States v. Perry*, 360 F.3d 519, 534 (6th Cir. 2004). *See also In re Application of the U.S.*, 849 F. Supp. 2d 526, 581 (D. Md. 2011) (holding that All Writs order cannot subvert the Fourth Amendment's probable cause requirement). The Supreme Court long ago recognized that "the power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed." *United States v. New York Tel. Co.*, 434 U.S. 159, 172 (1977).

CONCLUSION

For the foregoing reasons, Amicus respectfully requests that the Court grant Apple's Motion to Vacate the Order.

Dated: March 2, 2016

Respectfully submitted,



DAVID GREENE
CINDY COHN
LEE TIEN
KURT OPSAHL
JENNIFER LYNCH
NATE CARDOZO
SOPHIA COPE
ANDREW CROCKER
JAMIE WILLIAMS
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amici Curiae EFF and 46 Technologists, Researchers, and Cryptographers

APPENDIX – LIST OF AMICI CURIAE
(In alphabetical order)

Unless otherwise indicated, amici are signing this brief on their own individual behalf and not on behalf of the companies or organizations with whom they are affiliated. Those affiliations are only for identification.

1. **Josh Aas** founded Internet Security Research Group (ISRG), the non-profit entity behind the Let's Encrypt certificate authority, in 2013. He has been ISRG's Executive Director and chair of the corporate board since it was created. He worked on Gecko and Firefox as part of Mozilla's platform engineering group for many years and later worked as a senior strategist for Mozilla. He grew up in Duluth, MN, and graduated from Macalester College with majors in English Literature and Computer Science. He currently lives in Minneapolis, MN.

2. **Dr. Harold "Hal" Abelson** is a Professor of Electrical Engineering and Computer Science at MIT, a fellow of the IEEE, and a founding director of both Creative Commons and Public Knowledge. He directed the first implementation of the Logo computing language for the Apple II, which made the language widely available on personal computers beginning in 1981, and published a popular book on Logo in 1982. Abelson has won the Bose Award (MIT School of Engineering, 1992), the Taylor L. Booth Education Award (IEEE-CS, 1995), and the SIGCSE 2012 Outstanding Contribution to Computer Science Education (ACM, 2012). Abelson holds an A.B. from Princeton University and a Ph.D. in mathematics from MIT.

3. **Judy Anderson** received a B.A. in Philosophy and an M.S. in Computer Science from Stanford. She has been working in the computer industry ever since, with jobs both in research labs and in profit centers. She has worked for seven or so different companies. Her responsibilities have varied, including IT, build systems, porting software, and implementing new products, always as an individual contributor working as a member of a team. She has worked on a number of different types of products in several different languages.

4. **Andrew W. Appel** is Eugene Higgins Professor of Computer Science at Princeton University, where he has been on the faculty since 1986. His research is in software verification, computer security, programming languages and compilers, and technology policy. He received his A.B. summa cum laude in physics from Princeton in 1981, and his Ph.D. in computer science from Carnegie Mellon University in 1985. He has been Editor in

Chief of the Association for Computing Machinery's Transactions on Programming Languages and Systems and is a Fellow of ACM.

5. **Tom Ball** is a Staff Software Engineer at Google, working on Java-based developer tools. He was previously a Distinguished Engineer at Sun Microsystems, and a member of the JDK team that first released Java publicly. He wrote the first Java debugger (jdb), was a member of the AWT and Swing teams, and developed the Jackpot automated refactoring tool designed by James Gosling.

6. **Boaz Barak** is the Gordon McKay professor of Computer Science at Harvard University's John A. Paulson school of Engineering and Applied Sciences. His research interests include all areas of theoretical computer science and in particular cryptography and computational complexity. Barak has won the Packard and Sloan fellowships, and was also selected for Foreign Policy magazine's list of 100 leading global thinkers for 2014. He wrote with Sanjeev Arora the textbook "Computational Complexity: A Modern Approach."

7. **Brian Behlendorf** is a Managing Director at Mithril Capital Management. He is Chairman of the Board of Directors at the Electronic Frontier Foundation and also serves on the Boards of Directors of the Mozilla Foundation and Benetech. He has served as an advisor to the Office of Science and Technology Policy at the White House, as well as the Department of Health and Human Services; and as Chief Technology Office at the World Economic Forum. He was also a founding developer of the Apache Web Server, and served as the first President of the Apache Software Foundation.

8. **Rich Belgard** has been managing and designing the development of computer architectures for more than 40 years. He is co-inventor on 18 patents and sole inventor on 7 additional patents. Rich is the past Chairman and Vice-Chairman of the Association for Computing Machinery (ACM)'s Special Interest Group on Microarchitectures, and former Vice-Chair of the Institute of Electrical and Electronic Engineers (IEEE) Technical Committee on Microprogramming and Microarchitectures. Rich is currently Awards Chair and Industry Advisory Board Co-Chair for the IEEE Computer Society. Rich is an IEEE Fellow.

9. **Daniel J. Bernstein** is part-time Research Professor in the Department of Computer Science at the University of Illinois at Chicago and part-time

Professor in the Department of Mathematics and Computer Science at Technische Universiteit Eindhoven. Bernstein served as plaintiff in the landmark case of *Bernstein v. DOJ*, which established that code is speech protected by the First Amendment. He is the author of the software used by yahoo.com to receive mail, the software used by facebook.com to publish server addresses, the software used by OpenDNS to handle address requests from 50 million Internet users, the public-key system used by Apple to help protect files stored on iPhones, and the cipher used to encrypt Chrome's HTTPS connections to Google.

10. **Matt Bishop** is on the faculty at the Department of Computer Science at the University of California at Davis, where his main research area is the analysis of vulnerabilities in computer systems. His research includes modeling computer systems, building tools to detect vulnerabilities, and ameliorating or eliminating them. He was one of the two co-PIs on the California Top-to-Bottom Review of all electronic voting systems in California in 2007. Currently, he is examining data sanitization, modeling election processes, attribution, and the "insider" problem. His textbook, Computer Security: Art and Science, was published in December 2002 by Addison-Wesley Professional. He received his Ph.D. in computer science from Purdue University, where he specialized in computer security, in 1984.

11. **Joshua Bloch** is a Professor of the Practice at Carnegie Mellon University School of Computer Science. He is an expert on API design with over a quarter century of experience. He led the design and implementation of numerous Java APIs and language features, including the award-winning Java Collections Framework. He is the author of several books, including the bestselling, Jolt Award winning *Effective Java* (Addison-Wesley, 2001; Second Edition, 2008), the de facto standard guide to Java best practices. He holds a B.S. from Columbia and a Ph.D. in Computer Science from Carnegie Mellon University.

12. **Frederick P. Brooks, Jr.** is the Kenan Professor of Computer Science at UNC-Chapel Hill, Emeritus. While working at IBM in 1964, he switched the standard computer byte size from 6 to 8 bits. He was an architect of the Stretch and Harvest supercomputers, founded UNC's Computer Science Department, and researched computer architecture, software engineering, the design process, and graphics virtual environments. He wrote *The Mythical Man-Month*, *The Design of Design,* and, with G.A. Blaauw, *Computer Architecture*. Honors include the National Medal of Technology, the ACM

Turing Award, the National Academies of Engineering and Science, and British and Dutch academies.

13. **Dr. Mark Davis** co-founded the Unicode project and has been the president of the Unicode Consortium since its incorporation in 1991. He is one of the key technical contributors to the Unicode specifications, and one of the people responsible for Unicode emoji. Mark founded and was responsible for the overall architecture of ICU (the premier Unicode software internationalization library), and architected the core of the Java internationalization classes. Since 2006, Mark has been working on software internationalization at Google.

14. **Jeff Dean** joined Google in 1999 and is currently a Senior Fellow in Google's Knowledge Group. He has co-designed/implemented five generations of Google's crawling, indexing, and query serving systems, and co-designed/implemented major pieces of Google's initial advertising and AdSense for Content systems. Jeff has also worked for both the Centers for Disease Control and the World Health Organization, designing computer software for epidemiology and for statistical analysis of the HIV/AIDS pandemic. He is a Fellow of the ACM and the AAAS, a member of the U.S. National Academy of Engineering, and a recipient of the Mark Weiser Award and the ACM-Infosys Foundation Award in the Computing Sciences. Jeff holds a B.S., summa cum laude, in computer science and economics from the University of Minnesota, and a M.S. and Ph.D. in computer science from the University of Washington.

15. **Dr. L. Peter Deutsch** received a Ph.D. in Computer Science from U.C. Berkeley in 1973. At Xerox PARC, he helped develop programming systems that dramatically improved the performance of Java and JavaScript implementations. He is also the author of a number of RFCs and of the The Eight Fallacies of Distributed Computing, and originated the Deutsch limit adage about visual programming languages. Deutsch, dba Aladdin Enterprises, was the creator of Ghostscript, an Open Source implementation of the PostScript language. He later founded Artifex Software to license Ghostscript commercially while continuing its development and its release as Open Source. In 1993, he was a co-recipient of the ACM Software System Award, and was also named a Distinguished Alumnus of the U.C. Berkeley Computer Science program; he was named an ACM Fellow in 1994.

16. **David L. Dill** is the Donald E. Knuth Professor of Computer Science and, by courtesy, professor of Electrical Engineering at Stanford University. He was

named a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) in 2001 for his contributions to verification of circuits and systems, and a Fellow of the ACM in 2005 for contributions to system verification and for leadership in the development of verifiable voting systems. In 2008, he received the first "Computer-Aided Verification" award for fundamental contributions to the theory of real-time systems verification. In 2013, he was elected to the National Academy of Engineering and the American Academy of Arts and Sciences.

17. **Lester "Les" Earnest** is a widely-recognized computer scientist, best known for his deep involvement with the Advanced Research Project Agency Network (ARPAnet) startup committee, which led to his invention of the Finger protocol. He served as a US Navy Aviation Electronics Officer and Digital Computer Project Officer at the Naval Air Development Center, and later joined MIT to help design the Semi-Automatic Ground Environment air defense system. Later, he innovated numerous early features in the nascent field of word processing, including the first spell-checker.

18. **Brendan Eich** is the President and CEO of Brave Software, a start-up that aims to up-end the online ad ecosystem with more privacy and security for users. Eich previously served as CTO, then CEO, of the Mozilla Corporation. Prior to that, he co-founded the Mozilla project and foundation. While at Mozilla, Eich helped launch the award-winning Firefox Web browser and the Thunderbird e-mail client. Eich is also the inventor of JavaScript, the Internet's most widely used programming language, and is widely recognized for his enduring contributions to the Internet.

19. **David Farber** is Adjunct Professor of Internet Studies after his retirement as Distinguished Career Professor of Computer Science and Public Policy in the School of Computer Science at Carnegie Mellon University, holding a secondary appointment the Engineering Public Policy Group. He is a Member of the Markle Foundation Taskforce on National Security, and a Member of the Board of Trustees of EFF and the Electronic Privacy Information Center (EPIC). In 2003, he retired as the Alfred Fitler Moore Professor of Telecommunication Systems at the University of Pennsylvania where he held appointments as Professor of Business and Public Policy at the Wharton School of Business and as a Faculty Associate of the Annenberg School of Communications. In 2000, he was appointed to be Chief Technologist at the US Federal Communications Commission. He is a Fellow of both the ACM and the IEEE and was the recipient of the 1995 ACM Sigcomm Award for

life-long contributions to the computer communications field. He was awarded in 1997 the prestigious John Scott Award for Contributions to Humanity.

20. **Joan Feigenbaum** is Department Chair and Grace Murray Hopper Professor of Computer Science at Yale University. She received a B.A. in Mathematics from Harvard and a Ph.D. in Computer Science from Stanford. Professor Feigenbaum's research interests include security and privacy, computational complexity, Internet algorithms, and digital copyright. Her current and recent professional activities include service as the Program Chair of the 2013 ACM Symposium on Theory of Computing and membership on the Editorial Board of the ACM Transactions on Economics and Computation and the Steering Committee of the NetEcon Workshop. Professor Feigenbaum is a Fellow of the ACM, a Fellow of the AAAS, a Member of the Connecticut Academy of Science and Engineering, and a Connecticut Technology Council Woman of Innovation. In 1998, she was an invited speaker at the International Congress of Mathematicians.

21. **Professor Michael Fischer** received a B.S. in mathematics from the University of Michigan. He received an M.A. and Ph.D. in applied mathematics from Harvard University in the School of Engineering and Applied Sciences. Fischer's research interests include cryptographic protocols and security, theory of parallel and distributed systems, and discrete algorithms. Fischer is widely known for his work on the distributed consensus problem and for his "parallel prefix" algorithm that forms the basis of the "scan" operation fundamental to many parallel algorithms. Fischer directed one of the first Ph.D. dissertations on secure and verifiable e-voting and has developed information-theoretically secure cryptosystems based on random card deals. Fischer's recent work is focused on authentication and privacy. He is an ACM fellow and previously served as Editor-in-Chief of the Journal of the ACM. He has served on the Advisory Committee to the National Science Foundation and on the board of directors of the Computing Research Association, where he was a founding member of the CRA subcommittee on the Status of Women in Computer Science.

22. **Bryan Ford** leads the Decentralized/Distributed Systems (DeDiS) research group at Yale University. His work focuses broadly on building secure systems, touching on many particular topics including secure and certified OS kernels, parallel and distributed computing, privacy-preserving technologies, and Internet architecture. Prof. Ford earned his B.S. at the University of Utah

and his Ph.D. at MIT, while researching topics including mobile device naming and routing, virtualization, microkernel architectures, and touching on programming languages and formal methods.

23. **Matthew Keith "Matt" Franklin** is a professor of computer science at the University of California, Davis. Franklin is particularly known for the Boneh–Franklin scheme, a cryptography scheme he developed with Dan Boneh that uses the mathematics of elliptic curves to automatically generate public and private key pairs based on the identities of the communicating parties. In 2013, he and Boneh were winners of the Gödel Prize for their work on this system. Franklin graduated from Pomona College in 1983 with a degree in mathematics, was awarded a masters degree in mathematics in 1985 by U.C. Berkeley, and earned his Ph.D. in computer science from Columbia University in 1994. From 2009 to 2014, Franklin was editor-in-chief of the Journal of Cryptology.

24. **Dr. Matthew Green**, a respected cryptographer and security technologist, has over fifteen years of industry experience in computer security. Dr. Green is an Assistant Professor of Computer Science at the Johns Hopkins Information Security Institute. He specializes in applied cryptography, privacy-enhanced storage systems, and anonymous cryptocurrencies.

25. **J. Alex Halderman** is an Associate Professor of Computer Science and Engineering at the University of Michigan and Director of Michigan's Center for Computer Security and Society. His interests include computer and network security, Internet security measurement, censorship resistance, and electronic voting, as well as the interaction of technology with law and international affairs. Named one of Popular Science's "Brilliant 10" for 2015, his recent projects include ZMap, Let's Encrypt, and the Telex censorship resistance system.

26. **Martin E. Hellman** is a Professor Emeritus of Electrical Engineering at Stanford who, along with Whit Diffie, received the 2016 Turing Award for their pioneering invention of public key cryptography. The Turing Award is frequently likened to the Nobel Prize for the computing world. Hellman's co-invention of public key cryptography is significant because the technology, among other uses, forms the basis for secure transactions on the Internet. He has also been a long-time contributor to the computer security debate, starting with the issue of DES's key size in 1975, serving on the National Research Council's Committee to Study National Cryptographic Policy from 1994-96,

and currently serving on Verified Voting's Board of Advisors. Hellman received his B.E. from New York University in 1966, and his M.S. and Ph.D. from Stanford University in 1967 and 1969, all in Electrical Engineering.

27. **Nadia Heninger** is an assistant professor in the Computer and Information Science department at the University of Pennsylvania. Her research focuses on security, applied cryptography, and algorithms. Previously, she was an NSF Mathematical Sciences Postdoctoral Fellow at U.C. San Diego and a visiting researcher at Microsoft Research New England. She received her Ph.D. in computer science in 2011 from Princeton and a B.S. in electrical engineering and computer science in 2004 from U.C. Berkeley.

28. **Miguel de Icaza** was an early contributor to Linux projects and co-founded the GNOME with the goal to create a completely free desktop environment. In 2001, he co-founded and directed the Mono Project to implement Microsoft's .NET development platform on Linux. He has started two companies: Ximian, which focused on the Linux desktop and Xamarin, which builds development tools for mobile developers. Later this year, he will be joining Microsoft as a Distinguished Engineer, as part of the planned acquisition of Xamarin. He has received numerous awards and recognitions including: the Free Software Foundation Free Software Award, the MIT Technology Review Innovator of the Year Award, and was named one of Time Magazine's 100 innovators for the new century.

29. **Professor Tanja Lange** holds the chair for Cryptography at the Technische Universiteit Eindhoven, the Netherlands. She is an expert on curve-based crypto and post-quantum crypto. Her work brings together mathematics and cryptology to create more secure cryptographic implementations and protocols.

30. **Ed Lazowska** is the Bill & Melinda Gates Chair in Computer Science & Engineering at the University of Washington. His research concerns the design, implementation, and analysis of high performance computing and communication systems, and, more recently, the techniques and technologies of data-intensive discovery. He co-chaired (with Marc Benioff) the President's Information Technology Advisory Committee from 2003-05, and (with David E. Shaw) the Working Group of the President's Council of Advisors on Science and Technology to review the Federal Networking and Information Technology Research and Development Program in 2010. He is a Member of the National Academy of Engineering and a Fellow of the American Academy

of Arts and Sciences.

31. **George Ledin, Jr.** is a professor in the Computer Science Department at Sonoma State University and a former Visiting Fellow at SRI International. He has been working in the computer security field since 1975.

32. **Patrick McDaniel** is a Distinguished Professor in the School of Electrical Engineering and Computer at The Pennsylvania State University, co-director of the Systems and Internet Infrastructure Security Laboratory, and Fellow of IEEE and ACM. Dr. McDaniel is also the program manager and lead scientist for the Army Research Laboratory's Cyber-Security Collaborative Research Alliance. Patrick's research efforts centrally focus on a wide range of topics in security technical public policy. Patrick was awarded the National Science Foundation CAREER Award.

33. **David Patterson**, who joined U.C. Berkeley in 1976, was Chair of U.C. Berkeley's Computer Science Division, Chair of the Computing Research Association, and President of the Association for Computing Machinery. His most successful projects have been Reduced Instruction Set Computers (RISC), Redundant Arrays of Inexpensive Disks (RAID), and Network of Workstations, all of which helped lead to multibillion-dollar industries. This research led to his election to the National Academy of Engineering, the National Academy of Sciences, the Silicon Valley Engineering Hall of Fame, and Fellow of the Computer History Museum.

34. **Vern Paxson** is a Professor of Electrical Engineering and Computer Sciences at the University of California, Berkeley. He also leads the Networking and Security Group at the International Computer Science Institute in Berkeley, and has an appointment as a Staff Scientist at the Lawrence Berkeley National Laboratory. His research focuses heavily on measurement-based analysis of network activity and Internet attacks. He works extensively on high performance network monitoring, detection algorithms, cybercrime, and countering censorship. In 2006 he was inducted as a Fellow of the Association for Computing Machinery (ACM). In 2011 he received ACM's SIGCOMM Award, given for lifetime achievement and has also received ACM's Grace Murray Hopper Award and the 2015 IEEE Internet Award.

35. **Thomas Ristenpart** is an Associate Professor at Cornell Tech and a member of the Computer Science department at Cornell University. His research spans a wide range of computer security topics, with recent focuses on new threats

to, and improved opportunities for, cloud computing security, as well as topics in applied and theoretical cryptography. He completed his Ph.D. at U.C. San Diego in 2010.

36. **Professor Ron Rivest** is an MIT Institute Professor in the Department of Electrical Engineering and Computer Science. Professor Rivest is an inventor of the RSA public-key cryptosystem. He has extensive experience in cryptographic design and cryptanalysis, and has published numerous papers in these areas. Professor Rivest has current research interests in cryptography, computer and network security, voting systems, and algorithms. In the past he has also worked extensively in the area of machine learning. Professor Rivest is a co-author of the well-known text Introduction to Algorithms that has sold over 500,000 copies and has been translated into 12 languages. He is a founder of RSA Data Security and is also a co-founder of Verisign and of Peppercoin. He also serves on the Advisory Board of the Verified Voting Foundation. He is a member of a Scantegrity team developing and testing voting systems that are verifiable "end-to-end."

37. **Phillip Rogaway** is a professor in the Department of Computer Science at the University of California, Davis, USA whose research focuses on cryptography. He earned his Ph.D. at MIT's Theory of Computation group, worked at IBM as a security architect, then came to U.C. Davis, where he has spent most of the last 20 plus years. Rogaway's research has focused on obtaining provably-good solutions to protocol problems of genuine utility. He is also interested in social and ethical issues connected to technology.

38. **Greg Rose** was a Senior VP in the office of the Chief Scientist for QUALCOMM Incorporated, where he worked on cryptographic security and authentication for third-generation mobile phones and other technologies and managed other diverse research groups. He holds a number of patents for cryptographic methods and has successfully cryptanalyzed widely deployed ciphers. Greg was program chair of the 1996 and 2000 USENIX Security Symposia, and General Chair of Crypto 2003.

39. **Guido van Rossum** created the open-source programming language Python, and is its lead developer and thought leader. Python is widely used in industry, and is the most popular introductory programming language taught at top US universities. Guido developed the Python language while at CWI in Amsterdam. After moving to the US he worked as a guest researcher at NIST, at CNRI, and at several start-up companies. He became a Senior Staff

Engineer at Google, and currently works for Dropbox. Guido is an ACM Distinguished Engineer and a recipient of several awards including the USENIX STUG Award, the NLUUG Award, the Free Software Foundation Award, and the Dr. Dobb's Journal 1999 Excellence in Programming Award. In 2013, Python was awarded the Dutch National ICT COMMIT/Award. Guido holds an M.S. in Mathematics and Computer Science from the University of Amsterdam.

40. **Tom Shrimpton** is an associate professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. His research is in cryptography, with an emphasis the needs of real-world cryptographic practice. Much of his work has focused upon the theory and practice of hash functions, authenticated encryption schemes, and other symmetric-key primitives. Recently, he has worked more broadly in applied cryptography. He earned a Ph.D. in 2004 from U.C. Davis. In 2009, Professor Shrimpton was the recipient of a National Science Foundation CAREER award.

41. **Barbara Simons** is a former President of the Association for Computing Machinery (ACM), the nation's largest educational and scientific computing society. She is the only woman to have received the Distinguished Engineering Alumni Award from the College of Engineering of U.C. Berkeley, where she earned her Ph.D. in computer science. A fellow of ACM and of the American Association for the Advancement of Science, she also received the Computing Research Association Distinguished Service Award and the Electronic Frontier Foundation Pioneer Award. An expert on electronic voting, she published Broken Ballots: Will Your Vote Count?, a book on voting machines co-authored with Douglas Jones. She has been on the Board of Advisors of the U.S. Election Assistance Commission since 2008, and she co-authored the report that led to the cancellation of Department of Defense's Internet voting project (SERVE) in 2004 because of security concerns. She co-authored the July 2015 report of the U.S. Vote Foundation entitled The Future of Voting: End-to-End Verifiable Internet Voting. She is Board Chair of Verified Voting.

42. **Eugene H. Spafford** is a professor of Computer Sciences at Purdue University. He is also the founder and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). Some of his work is at the foundation of current security practice, including intrusion detection, firewalls, and whitelisting. His most recent work has been

in cyber security policy, forensics, and future threats. Professor Spafford is a Fellow of the AAAS, ACM, IEEE, (ISC)2, a Distinguished Fellow of the ISSA, recipient of the NIST/NSA Computer Systems Security Award, and a member of the Cyber Security Hall of Fame — the only person to ever hold all these distinctions. In 2012 he was named as one of Purdue's inaugural Morrill Professors — the university's highest award for the combination of scholarship, teaching, and service.

43. **Dan S. Wallach** is a Professor in the Department of Computer Science and a Rice Scholar in the Baker Institute for Public Policy at Rice University. His research considers a variety of issues in computer systems security. Wallach has also served on the Air Force Science Advisory Board and the USENIX Association Board of Directors.

44. **Nickolai Zeldovich** is an Associate Professor at MIT's department of Electrical Engineering and Computer Science, and a member of the Computer Science and Artificial Intelligence Laboratory. His research interests are in building practical secure systems, from operating systems and hardware to programming languages and security analysis tools. He received his Ph.D. from Stanford University, where he developed HiStar, an operating system designed to minimize the amount of trusted code by controlling information flow. He co-founded MokaFive, a company focused on improving desktop management and mobility using x86 virtualization. Prof. Zeldovich has received a Sloan fellowship, an NSF CAREER award, the MIT EECS Spira teaching award, and the MIT Edgerton faculty achievement award.

45. **Yan Zhu** is a senior software engineer at Brave Software, where she focuses on privacy and security matters. She joined Brave from the Yahoo security team and is a technology fellow at the Electronic Frontier Foundation. She previously worked on the Tor project and SecureDrop at the Freedom of the Press Foundation. Zhu received her Bachelor in Physics from MIT, and was a PhD candidate in Physics at Stanford University.

46. **Philip R. Zimmermann** is the creator of Pretty Good Privacy (PGP), an email encryption software package. Zimmermann originally designed PGP as a human rights tool and published it for free on the Internet. PGP is the most widely used email encryption software in the world. Zimmermann has received numerous technical and humanitarian awards for his pioneering work in cryptography, including the US Privacy Champion Award from the Electronic Privacy Information Center. He has been inducted into the Cyber

Security Hall of Fame, the Internet Society Internet Hall of Fame, the Heinz Nixdorf MuseumsForum Wall of Fame, and the CRN Industry Hall of Fame. He is a member of the International Association of Cryptologic Research, and the League for Programming Freedom. He has also founded several companies, most recently Silent Circle.

DAVID GREENE (SBN 160107)
davidg@eff.org
CINDY COHN (SBN 145997)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JENNIFER LYNCH (SBN 240701)
NATE CARDOZO (SBN 259097)
SOPHIA COPE (SBN 233428)
ANDREW CROCKER (SBN 291596)
JAMIE WILLIAMS (SBN 279046)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amici Curiae Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	Case No: 16-cm-00010-SP **PROOF OF SERVICE**

I am a citizen of the United States and employed in San Francisco, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is 815 Eddy Street, San Francisco, CA 94109. On this date, I served the following:

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND 46 TECHNOLOGISTS, RESEARCHERS, AND CRYPTOGRAPHERS

and caused to be served by U.S. Mail, postage thereon fully prepaid, true and correct copies of the foregoing on:

Theodore B Olson
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 20036-5306
202-955-8668
Fax: 202-530-9575
Email: tolson@gibsondunn.com

Theodore J Boutrous , Jr
Eric David Vandevelde
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
213-229-7000
Fax: 213-229-7520
Email: tboutrous@gibsondunn.com
Email: evandevelde@gibsondunn.com

Nicola T Hanna
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 92612-4412
949-451-3800
Fax: 949-451-4220
Email: nhanna@gibsondunn.com

Marc J Zwillinger
Jeffrey G Landis
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
202-296-3585
Fax: 202-706-5298
Email: marc@zwillgen.com
Email: jeff@zwillgen.com

Counsel for Respondent

Allen W Chiu
AUSA - Office of US Attorney
National Security Section
312 North Spring Street Suite 1300
Los Angeles, CA 90012
213-894-2435
Fax: 213-894-6436
Email: allen.chiu@usdoj.gov

Tracy L Wilkison
AUSA Office of US Attorney
Chief, Cyber and Intellectual Property
Crimes Section
312 North Spring Street 11th Floor
Los Angeles, CA 90012-4700
213-894-0622
Fax: 213-894-0141
Email: tracy.wilkison@usdoj.gov

Counsel for Plaintiff

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed this March 3, 2016 in San Francisco, California

Cynthia Dominguez