

JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
RIANA PFEFFERKORN (SBN 266817)
riana@law.stanford.edu
STANFORD LAW SCHOOL
CENTER FOR INTERNET AND SOCIETY
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 736-8675
Facsimile: (650) 725-4086



Attorneys for [Proposed] *Amici Curiae*
iPhone Security and Applied Cryptography
Experts

LOGGED

2016 MAR -3 PM 3:19
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE
BY

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

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

ED No. CM 16-10 (SP)

~~[PROPOSED]~~
**ORDER GRANTING
APPLICATION OF [PROPOSED]
AMICI CURIAE IPHONE
SECURITY AND APPLIED
CRYPTOGRAPHY EXPERTS FOR
LEAVE TO FILE BRIEF IN
SUPPORT OF MOVANT APPLE
INC.**

Hearing:

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

1 The Court has received the Application of [Proposed] *Amici Curiae* iPhone
2 Security and Applied Cryptography Experts for Leave to File Brief in Support of
3 Movant Apple Inc. in the above-captioned matter. Having reviewed the
4 Application, the proposed *amici curiae* brief attached thereto, and related papers
5 filed therewith, and good cause appearing, the Application is hereby GRANTED.
6 The Clerk is respectfully directed to file the *amici curiae* brief and related papers
7 and add *amici curiae* to the ECF docket for this action.

8
9 SO ORDERED.

10
11
12 Dated: March 4, 2016



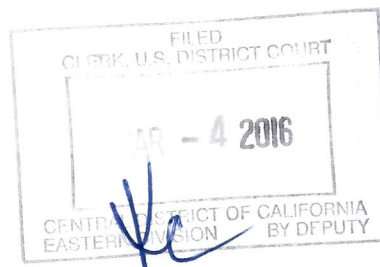
13 THE HONORABLE SHERI PYM
14 UNITED STATES MAGISTRATE JUDGE

LODGED

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

JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
STANFORD LAW SCHOOL
CENTER FOR INTERNET AND SOCIETY
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 736-8675
Facsimile: (650) 725-4086

2016 MAR -3 PM 3:19
CENTRAL DIST. OF CALIF.
RIVERSIDE



UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

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

ED No. CM 16-10 (SP)

**NOTICE OF APPEARANCE OF
COUNSEL**

Hearing:

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

1 **SECTION I - IDENTIFYING INFORMATION:**

2 Name: Jennifer Stisa Granick CA Bar Number: 168423

3 Firm or Agency: Stanford Law School, Center for Internet and Society

4 Address: 559 Nathan Abbott Way, Stanford CA 94305

5 Telephone Number: 650-736-8675 Fax Number: 650-725-4086

6 Email: Jennifer@law.stanford.edu

7 Counsel of record for [Proposed] *Amici Curiae*: iPhone Security and Applied
8 Cryptography Experts

9
10 **SECTION II – TO ADD AN ATTORNEY TO THE DOCKET**

11 *Please select one of the following options:*

12 The filing of this form constitutes the first appearance in this case of the
13 attorney listed above. No other members of this attorney’s firm or agency have
14 previously appeared in the case

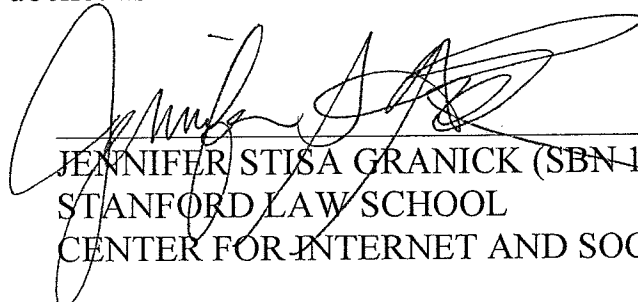
15 *In addition, if this is a criminal case, please check the applicable box below. The*
16 *attorney listed above is:*

17 USAO FPDO CJA Appointment Pro Bono Retained

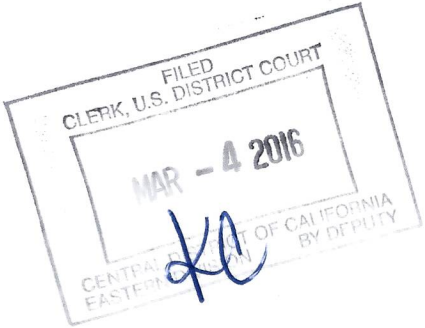
18
19 **SECTION IV – SIGNATURE**

20 I request that the Clerk update the docket as indicated above.

21
22 Dated: March 2, 2016


JENNIFER STISA GRANICK (SBN 168423)
STANFORD LAW SCHOOL
CENTER FOR INTERNET AND SOCIETY

25 Attorney for [Proposed] *Amici Curiae*
26 iPhone Security and Applied Cryptography
27 Experts
28



JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
RIANA PFEFFERKORN (SBN 266817)
riana@law.stanford.edu
STANFORD LAW SCHOOL
CENTER FOR INTERNET AND SOCIETY
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 736-8675
Facsimile: (650) 725-4086

Attorneys for *Amici Curiae*
iPhone Security and Applied Cryptography
Experts

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION**

LOGGED

2016 MAR - 3 PM 3:18

U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

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

ED No. CM 16-10 (SP)

**BRIEF OF *AMICI CURIAE*
IPHONE SECURITY AND
APPLIED CRYPTOGRAPHY
EXPERTS IN SUPPORT OF
APPLE INC.'S MOTION TO
VACATE ORDER COMPELLING
APPLE INC. TO ASSIST AGENTS
IN SEARCH, AND OPPOSITION
TO GOVERNMENT'S MOTION
TO COMPEL ASSISTANCE**

Hearing:

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

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

TABLE OF CONTENTS

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

INTERESTS OF *AMICI CURIAE*..... 1

SUMMARY OF ARGUMENT..... 3

FACTUAL BACKGROUND..... 4

ARGUMENT..... 9

 I. Forcing Device Manufacturers to Create Forensic Capabilities
 For U.S. Investigators Creates Security Risks 10

 A. The Court’s Order Will Most Likely Force Apple To
 Create An Insecure Version of iOS Capable of
 Bypassing Passcode Functionality On Any iPhone..... 10

 B. Apple Will Likely Lose Control Of the Code, Due Either
 to Legal Compulsion or Theft 13

 C. The Court’s Order Would Set A Precedent For Forcing
 Vendors to Turn Their TVs and Other Consumer Goods
 Into FBI Surveillance Tools..... 17

 D. The Court’s Order Risks Undermining Critical Public
 Trust in Automatic Software Security Updates 18

 II. Security Breaches Are All But Certain When Law Mandates
 Government Access 22

CONCLUSION 23

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

TABLE OF AUTHORITIES

Statutes

All Writs Act (“AWA”), 28 U.S.C. § 1651 *passim*

Cases

In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 15-mc-1902-JO (E.D.N.Y. Feb. 29, 2016) 10

Other Authorities

Harold Abelson, *et al.*, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications* (2015), <https://dspace.mit.edu/handle/1721.1/97690> 22

James Bamford, *A Death in Athens: Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee?*, *The Intercept* (Sept. 28, 2015), <https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/> 22

Killian Bell, *President Obama Answers Questions on Cool iPad Setup*, *iPhoneHacks.com* (July 3, 2015), <http://www.iphonhacks.com/2015/07/president-obama-answers-healthcare-questions-on-cool-ipad-setup.html> 15

Katie Benner, *Apple Moves to Shift Battle Over Unlocking iPhone to Capitol Hill*, *N.Y. Times* (Feb. 22, 2016), <http://www.nytimes.com/2016/02/23/technology/apple-unlock-iphone-san-bernardino.html>..... 12

Brute Force Attack, https://en.wikipedia.org/wiki/Brute-force_attack 6

Lorrie Faith Cranor *et al.*, *Supporting Privacy-Conscious App Update Decisions with User Reviews*, in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices* (2015), <http://mews.sv.cmu.edu/papers/spsm-15.pdf>..... 20

1 *Does the FBI Need a Back Door to Your Data?*, KCRW
 2 (Feb. 23, 2016), [http://www.kcrw.com/news-culture/shows/to-the-](http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone-unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data)
 3 [point/apple-v-fbis-iphone-unlock-battle#seg-does-the-fbi-need-a-](http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone-unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data)
[back-door-to-your-data](http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone-unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data) 21

4 Brad Haynes, *Facebook Executive Jailed in Brazil as Court Seeks*
 5 *WhatsApp Data*, Reuters (Mar. 1, 2016),
 6 [http://www.reuters.com/article/us-facebook-brazil-](http://www.reuters.com/article/us-facebook-brazil-idUSKCN0W34WF)
[idUSKCN0W34WF](http://www.reuters.com/article/us-facebook-brazil-idUSKCN0W34WF) 16

7 iPad in Business, <https://www.apple.com/ipad/business/profiles/> 15

8 Legal Process Guidelines: U.S. Law Enforcement,
 9 [https://www.apple.com/privacy/docs/legal-process-guidelines-](https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf)
 10 [us.pdf](https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf) 7

11 Ewen MacAskill, *Yahoo Forced to Apologise to Chinese Dissidents*
 12 *over Crackdown on Journalists*, The Guardian (Nov. 14, 2007),
 13 <http://www.theguardian.com/technology/2007/nov/14/news.yahoo> 16

14 Sarah Perez, *You Can Now Jailbreak Your iOS 9 Devices (But You*
 15 *Probably Shouldn't)*, TechCrunch (Oct. 14, 2015),
 16 [http://techcrunch.com/2015/10/14/you-can-now-jailbreak-your-ios-](http://techcrunch.com/2015/10/14/you-can-now-jailbreak-your-ios-9-devices-but-you-probably-shouldnt/)
 17 [9-devices-but-you-probably-shouldnt/](http://techcrunch.com/2015/10/14/you-can-now-jailbreak-your-ios-9-devices-but-you-probably-shouldnt/) 11

18 Samsung Smart TVs Do Not Monitor Living Room Conversations,
 19 [https://news.samsung.com/global/samsung-smart-tvs-do-not-](https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations)
 20 [monitor-living-room-conversations](https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations) 17

21 Greg Sandoval and Declan McCullagh, *Apple Loses Another*
 22 *Unreleased iPhone (Exclusive)*, CNET (Aug. 31, 2011),
 23 [http://www.cnet.com/news/apple-loses-another-unreleased-iphone-](http://www.cnet.com/news/apple-loses-another-unreleased-iphone-exclusive/)
 24 [exclusive/](http://www.cnet.com/news/apple-loses-another-unreleased-iphone-exclusive/) 15

25 Greg Sandoval and Declan McCullagh, *Lost iPhone Prototype Spurs*
 26 *Police Probe*, CNET (Apr. 23, 2010),
 27 [http://www.cnet.com/news/lost-iphone-prototype-spurs-police-](http://www.cnet.com/news/lost-iphone-prototype-spurs-police-probe/)
 28 [probe/](http://www.cnet.com/news/lost-iphone-prototype-spurs-police-probe/) 15

Avie Schneider, *Amazon Wants To Put A Listening Speaker In Your*
 Home, National Public Radio (Nov. 6, 2014),
[http://www.npr.org/sections/alltechconsidered/2014/11/06/362088](http://www.npr.org/sections/alltechconsidered/2014/11/06/362088269/amazon-wants-to-put-a-listening-speaker-in-your-home)
[269/amazon-wants-to-put-a-listening-speaker-in-your-home](http://www.npr.org/sections/alltechconsidered/2014/11/06/362088269/amazon-wants-to-put-a-listening-speaker-in-your-home) 17

1 Bruce Schneier, *Attacking Tor: How the NSA Targets Users' Online*
2 *Anonymity*, The Intercept (Oct. 4, 2013),
3 [http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-](http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity)
4 [users-online-anonymity](http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity) 20

5 TaiG9beta, <http://taig9.com> 11

6 Ben Thompson, *UAE Blackberry update was spyware*, BBC News
7 (July 21, 2009), <http://news.bbc.co.uk/2/hi/8161190.stm> 21

8 Update the iOS Software on Your iPhone, iPad, or iPod Touch,
9 <https://support.apple.com/en-us/HT204204> 19

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

INTERESTS OF *AMICI CURIAE*

1
2 *Amici curiae* are computer security experts who research and publish on the
3 topic of mobile device security and encryption. Independent experts in iPhone
4 security and applied cryptography, *amici* work to analyze, understand, and
5 encourage the security of Apple products. *Amici* are strongly opposed to the
6 Court's enforcing its order. In *amici's* expert opinion, to do so would endanger
7 public safety.

8 *Amicus* Dino Dai Zovi is an expert in Apple iOS security. He has over 15
9 years' experience in the information security field, including penetration testing,
10 software security, information security management, and cybersecurity research
11 and development. In 2008, eWEEK named him one of the 15 Most Influential
12 People in Security. A regular speaker at information security conferences around
13 the world, Mr. Dai Zovi is the co-author of several books: *The iOS Hacker's*
14 *Handbook* (Wiley, 2012), *The Mac Hacker's Handbook* (Wiley, 2009), and *The*
15 *Art of Software Security Testing* (Addison-Wesley, 2006).

16 *Amicus* Dan Boneh is a Professor of Computer Science at Stanford
17 University, where he heads the applied cryptography group and co-directs the
18 computer security lab. Dr. Boneh's research focuses on applications of
19 cryptography to computer security. His work includes cryptosystems with novel
20 properties, security for mobile devices, web security, and cryptanalysis. He is the
21 author of over 150 publications in the field and is a recipient of the 2014 Infosys
22 award, the 2013 Gödel Prize, the Packard Award, the Alfred P. Sloan Award, and
23 the RSA Conference Award in mathematics. In 2016, Dr. Boneh was elected to the
24 National Academy of Engineering.

25 *Amicus* Charlie Miller is an independent security researcher who focuses on
26 mobile devices and embedded technology. Mr. Miller, who spent five years
27 working for the National Security Agency, was the first to discover a remote
28 exploit against the iPhone when it came out in 2007 as well as the first to discover

1 a remote exploit against any commercial Android device. Dr. Miller holds a Ph.D.
2 in Mathematics from the University of Notre Dame and has authored or co-
3 authored several books, including, with Mr. Dai Zovi, *The iOS Hacker's*
4 *Handbook*. He has found vulnerabilities in iPhone web browsers as well as the
5 code responsible for processing SMS text messages. This latter flaw would have
6 allowed an attacker to completely compromise any iPhone just by sending text
7 messages. Dr. Miller has also found multiple code signing bypasses against iOS
8 devices, which would allow for the installation of malicious, unsigned code on the
9 devices. He has worked with Apple each time to get these flaws fixed.

10 *Amicus* Dr. Hovav Shacham has been a professor in the University of
11 California at San Diego's Department of Computer Science and Engineering since
12 2007. Dr. Shacham received his Ph.D. in computer science in 2005 from Stanford
13 University. In 2006 and 2007, he was a Koshland Scholars Program postdoctoral
14 fellow at the Weizmann Institute of Science, hosted by Moni Naor. Dr. Shacham's
15 research interests are in applied cryptography, systems security, privacy-enhancing
16 technologies, and technology policy.

17 *Amicus* Bruce Schneier is an internationally renowned security technologist.
18 Called a "security guru" by *The Economist*, Mr. Schneier is a fellow at the
19 Berkman Center for Internet and Society at Harvard University, a board member of
20 the Electronic Frontier Foundation, and an Advisory Board member of the
21 Electronic Privacy Information Center. He is also the Chief Technology Officer of
22 Resilient Systems, Inc. Mr. Schneier designed the popular Blowfish encryption
23 algorithm, and his Twofish encryption algorithm was a finalist for the new Federal
24 Advanced Encryption Standard (AES).

25 *Amicus* Dan S. Wallach is a Professor in the Department of Computer
26 Science and a Rice Scholar in the Baker Institute for Public Policy at Rice
27 University. His research considers a variety of issues in computer systems security.
28

1 Wallach has also served on the Air Force Science Advisory Board and the
2 USENIX Association Board of Directors.

3 *Amicus* Jonathan Zdziarski is an independent forensics researcher considered
4 to be among the foremost experts in iOS-related digital forensics and security. Mr.
5 Zdziarski's research into the iPhone has pioneered modern forensic methodologies
6 used today for iOS devices, of which his were the first to be validated by the
7 United States National Institute of Justice (NIJ) and National Institute of Standards
8 and Technology (NIST). Mr. Zdziarski has extensive experience in the roles of
9 forensic scientist and security researcher, specializing in reverse engineering,
10 research and development, and penetration testing. He has consulted with law
11 enforcement and military agencies on numerous high profile cases, assisted on
12 local, state, federal, and international cases, and testified numerous times as an
13 expert in cases he has assisted with. Mr. Zdziarski trains law enforcement and
14 intelligence agencies worldwide specifically in iOS forensics and penetration. He
15 has written several books pertaining to the iPhone, including *iPhone Forensics*,
16 *iPhone SDK Application Development*, *iPhone Open Application Development*,
17 and *Hacking and Securing iOS Applications*.

18 SUMMARY OF ARGUMENT

19 This Court's Order seeks to address law enforcement's legitimate interest in
20 conducting investigations. However, in commanding Apple to create forensic
21 software that would bypass iPhone security features, the Order endangers public
22 safety. *Amici*, independent experts in iPhone security and encryption with
23 backgrounds in government, industry, and academia, write to inform the Court of
24 these real dangers. As experts, it is *amici's* opinion that the dangers of forcing
25 companies to denigrate the security of their products and of allowing law
26 enforcement to commandeer consumer devices for surveillance purposes are too
27 great.

28

1 For practical reasons, the security bypass this Court would order Apple to
2 create almost certainly will be used on other iPhones in the future. This spread
3 increases the risk that the forensic software will escape Apple's control either
4 through theft, embezzlement, or order of another court, including a foreign
5 government. If that happens, the custom code could be used by criminals and
6 governments to extract sensitive personal and business data from seized, lost, or
7 stolen iPhones, or it could be reverse engineered, giving attackers a stepping stone
8 on the path towards their goal of defeating Apple's passcode security. Compelling
9 Apple to create forensic software for the government is also dangerous due to any
10 bugs the software might contain.

11 Further, the Court here threatens to set a legal precedent that law
12 enforcement will use to force companies to craft other security bypasses for
13 forensic purposes. There is nothing in the All Writs Act or the Court's Order that
14 would put off-limits software "updates" that turn on a smart TV's microphone for
15 eavesdropping purposes, or activate a laptop camera for video surveillance. These
16 other bypasses will pose their own, potentially even worse, privacy, cybersecurity,
17 and personal safety risks to the public. As risky as the Court's Order in this case is,
18 the precedent it would set poses even greater danger.

19 Finally, the Court's Order could undermine public trust in automatic
20 software updates. Regular, silent, automatic updates are crucial for software
21 security. The belief that such an update could be spyware that a company was
22 forced by the government to sign and distribute might lead people to turn off
23 automatic updates. This would render software patches less effective and the
24 general public less secure.

25 Accordingly, *amici* respectfully urge the Court to vacate its order.

26 **FACTUAL BACKGROUND**

27 Syed Rizwan Farook and his wife, Tashfeen Malik, went on a deadly
28 shooting rampage at Farook's San Bernardino workplace in December 2015. The

1 FBI wants access to the data stored on Farook's work-issued iPhone (the "Subject
2 iPhone"), made by Apple.

3 Farook's iCloud stored data, including some data from the Subject iPhone, is
4 now in the FBI's possession. So far, however, investigators have been unable to
5 access all the data from the Subject iPhone. That is because the iPhone stopped
6 backing up to Apple's iCloud servers about six weeks before the attack. With
7 Farook's iCloud account password, the FBI could have forced the Subject iPhone
8 to back up the last six weeks of data to iCloud, and then access it. Instead, Farook's
9 employer, at the request of FBI agents, changed the password, and that is no longer
10 an option.¹ At this point, it appears that the last few weeks' worth of data cannot be
11 obtained other than from the Subject iPhone itself.

12 To access the data on the iPhone, the FBI must guess the passcode. That is
13 because the data is encrypted with a key that is partially calculated with the
14 passcode. Without knowing the passcode, you cannot generate the key, and
15 without the key, you cannot decrypt the data.

16 *Apple's passcode limitation features protect the privacy, digital security,*
17 *and physical safety of iPhone owners.* For most people, the biggest risk to the data
18 on their iPhones is when their device ends up in the wrong hands. An abusive
19 partner might want to search the phone to keep tabs on its owner. An economic
20 competitor might want to steal trade secrets. An identity thief might want to find
21 the owner's credit card numbers, PINs, or social security number. An agent of an
22 autocratic government might be looking to persecute journalists or human rights
23 workers who use iPhones to communicate. To protect unauthorized outsiders from
24 accessing or altering the sensitive personal data people store on iPhones, Apple

25
26 ¹ See Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents
27 in Search, and Opposition to Government's Motion to Compel Assistance, D.I. 16
28 (hereafter "Motion to Vacate") at 7 n.11.

1 must make it difficult or infeasible for an attacker to use a computer to automate or
2 “brute force” guess the passcode—rapidly attempting all possible combinations
3 until the guess is right.² Apple limits passcode guesses in at least two ways in order
4 to accomplish this goal: (1) a passcode guess delay, which after enough
5 consecutive incorrect attempts is set to an infinite value, such that the device will
6 refuse to accept any further passcode entries; and (2) an optional data deletion
7 feature.

8 Apple implements the passcode guess delay by default. The iOS software
9 imposes an increasing lag to discourage brute force attacks against the passcode.
10 After five incorrect guesses, the attacker must wait one minute, after the sixth, five
11 minutes, and so on. This delay slows down the attacker, but will not permanently
12 disable the device or erase the data unless the latter, optional “erase after ten failed
13 guesses” feature is enabled. After approximately ten or eleven wrong guesses, the
14 attacker will not be allowed to enter any more guesses. The passcode guess delay
15 makes it extremely difficult if not impossible to brute force the passcode.

16 Apple has also given consumers an optional “erase after ten failed guesses”
17 feature. If the phone user enables this feature, and an attacker tries to guess the
18 passcode, this feature will wipe the data, ensuring that confidential and/or valuable
19 data will not be exposed. The increasing delays for incorrect guesses also prevent a
20 malicious user with brief physical possession of the phone from entering enough
21 incorrect passcode guesses to force the device to erase itself.

22 The passcode guess delay and data destruction feature (passcode limitations)
23 serve an important security and privacy function. These security features stop
24 attackers from being able to access the extremely personal, sensitive, and extensive
25

26 ² A brute force attack consists of systematically checking all possible keys or
27 passwords until the correct one is found. *See* Brute Force Attack,
28 https://en.wikipedia.org/wiki/Brute-force_attack.

1 data people store on their iOS devices. Additionally, these security features
2 disincentivize would-be attackers from iPhone thefts, robberies, and burglaries.

3 *The Order Requires Apple To Do More Than Past Requests Did.* In the
4 past, Apple has performed data extractions from passcode locked devices for law
5 enforcement.³ The company did this extraction for the government on devices
6 running versions of Apple's iOS software prior to 8.0. For these earlier versions,
7 Apple was able to extract certain categories of data from the device because that
8 data was not encrypted with a key generated from the user's passcode. *Id.*
9 However, with version 8.0 and higher, Apple's data extraction tools no longer
10 work, as "[t]he files to be extracted are protected by an encryption key that is tied
11 to the user's passcode, which Apple does not possess." *Id.*

12 The Subject iPhone runs iOS 9.0.⁴ Since Apple does not have the passcode,
13 the only recourse to decrypt and access data stored exclusively on the Subject
14 iPhone is to guess the passcode. The government is concerned that, as a result of
15 these passcode security features, it will take too long to guess the passcode, and
16 that if it makes too many wrong guesses, it could cause the Subject iPhone to
17 automatically delete the data on it.

18 Consequently, the government asked for and received a technical assistance
19 order from this Court to Apple pursuant to the All Writs Act ("AWA"), 28 U.S.C.
20 § 1651.⁵ The Order requires Apple to write software that will accomplish three

21 _____
22 ³ Legal Process Guidelines: U.S. Law Enforcement,
23 <https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf> (see section
24 "Extracting Data from Passcode Locked iOS Devices").

25 ⁴ Government's *Ex Parte* Application For Order Compelling Apple Inc. To Assist
26 Agents In Search; Memorandum Of Points And Authorities; Declaration of
27 Christopher Pluhar; Exhibit, Crim. No. 15-mj-451, D.I. 18 (hereafter
28 "Application") at 4.

⁵ Order Compelling Apple, Inc. To Assist Agents in Search, Crim. No. 15-mj-451,
(Footnote Continued on Next Page.)

1 things on the Subject iPhone: “(1) it will bypass or disable the auto-erase function
2 whether or not it has been enabled; (2) it will enable the FBI to submit passcodes
3 to the Subject Device for testing electronically via the physical device port,
4 Bluetooth, Wi-Fi, or other protocol available on the Subject Device; and (3) it will
5 ensure that when the FBI submits passcodes to the Subject Device, software
6 running on the device will not purposefully introduce any additional delay between
7 the passcode attempts beyond what is incurred by Apple hardware.”⁶ Order at 2.
8 For the purposes of this brief, we refer to the forensic software the government
9 would force Apple to create in this case as the “Custom Code.”

10 In other words, the Court Order compels Apple to create a type of forensic
11 software for the government—a version of its iOS that lacks the passcode
12 limitation features. The Order would compel Apple to create new software that
13 does not currently exist, to carry out a capability Apple does not presently have.
14 This is the first time any Court has ever publicly ordered a vendor to do something
15 like this.

16 *The Court Order Would Compel Apple to Sign, Or Validate, the Custom*
17 *Code.* Once the Custom Code is created, complying with the Order requires Apple
18 to authenticate the new code by cryptographically signing it. Apple’s hardware is
19 designed to only run software that has been cryptographically “signed” by Apple
20 or by another entity that has been authorized by Apple to also sign software to run
21
22
23

24 _____
(Footnote Continued from Previous Page.)

25 D.I. 19 (hereafter “Order”) at 1.

26 ⁶ There is an 80-millisecond delay per guess that is required for the hardware to
27 perform the cryptography necessary to verify a passcode guess attempt. This is a
28 limitation of the hardware.

1 on an iPhone or iPhones.⁷ The fact that software must be signed to run on an iOS
2 device is one way that Apple protects its customers from computer viruses and
3 malicious software (malware). By creating a security architecture that only runs
4 Apple signed code, Apple protects its iPhone customers from the attacks that
5 plague desktop computer users. iPhone users know that the software they run is
6 approved by Apple and that to the best of Apple's knowledge, it will not steal their
7 data, transmit viruses or worms to other Internet users, surreptitiously turn on their
8 phone's camera or microphone and spy on them, or otherwise compromise the
9 security of their device or the privacy of their data. Apple's cryptographic
10 signature is essentially an attestation that as far as Apple knows, the signed
11 software is safe to run.

12 Again, no public U.S. court has ever compelled a private party to
13 cryptographically sign code.

14 ARGUMENT

15 *Amici* have dedicated their careers to studying and improving iPhone and
16 cryptographic security. Despite the Court's efforts, this Order endangers the
17 privacy and safety of iPhone users and those who come into digital contact with
18 them. Worse, it sets a precedent for other such orders that would create even
19 greater risks.

20 The All Writs Act (AWA) was originally enacted as part of the Judiciary Act
21 of 1789. Needless to say, there were no computer networks or mobile phones at the
22 time. Congress could not have considered the privacy and security risks that efforts
23 to build forensic capabilities into hardware or software can cause. Nevertheless,
24 those public security risks can be significant. This is but one reason, alongside
25

26 ⁷ Apple delegates the ability to authorize software to run to some app developers
27 during coding and testing, and to some large organizations. But system software
28 such as that which this Court has ordered Apple to create must be signed by Apple.

1 those set forth in Apple’s Motion to Vacate and Eastern District of New York
2 Magistrate Judge James Orenstein’s February 29, 2016 opinion,⁸ why the AWA is
3 an inappropriate legal vehicle for compelling companies to alter their security
4 architectures.

5 **I. Forcing Device Manufacturers to Create Forensic Capabilities For U.S.**
6 **Investigators Creates Security Risks**

7 **A. The Court’s Order Will Most Likely Force Apple To Create An**
8 **Insecure Version of iOS Capable of Bypassing Passcode**
9 **Functionality On Any iPhone**

10 Apparently aware that its Order could put iPhone users at risk of public
11 exposure of private photos, identity or intellectual property theft, physical attacks,
12 real-time surveillance, or worse, this Court devised some safeguards to
13 theoretically reduce the risk of harm. Order at 2. First, Apple is supposed to
14 engineer the Custom Code to only work on the Subject iPhone. *Id.* Second, Apple
15 need not transfer the Custom Code to the FBI, but may install and use it itself and
16 then turn any responsive data over. *Id.*

17 These rules are not meaningful barriers to misuse and abuse of the forensic
18 capabilities this Court is ordering Apple to create. First, the Order assumes that
19 Apple will create the Custom Code without any vulnerabilities in its
20 implementation. Vulnerabilities are common in software code, including Apple’s
21 iOS, and despite Apple’s best efforts. The government dismissively downplays the
22 effort required to develop and update the Custom Code, stating that Apple “writes
23 software code as part of its regular business,” including “routinely patch[ing]
24 security or functionality issues” in iOS and “releas[ing] new versions of [iOS] to
25 address issues.” Application at 15. But creating software (especially secure
26 software) is complex, and software development requires rigorous testing.

27 ⁸ *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant*
28 *Issued by This Court*, No. 15-mc-1902-JO (E.D.N.Y. Feb. 29, 2016).

1 Vulnerabilities are common in software code, despite vendors' best efforts.
2 To address this problem, vendors employ extensive pre-release testing; after-the-
3 fact audits, including by independent security researchers; and regular updates. Yet
4 none of these practices, alone or in concert, can ensure that software will not be
5 vulnerable and subject to misuse. Yet, given the circumstances of this case, this
6 code is unlikely to go through this lifecycle, increasing the risk that it will
7 introduce vulnerabilities into the iPhone ecosystem.

8 For example, since first introducing the earliest iPhone, Apple has waged a
9 cat-and-mouse battle with "jailbreakers," software developers who identified and
10 exploited vulnerabilities in the devices in order to run software other than that
11 signed by Apple and to defeat carrier locks that tied handsets to particular cellular
12 providers. Apple warns its users against jailbreaking and the practice is contrary to
13 Apple's terms of service. Jailbreaking involves modifying the iPhone firmware so
14 that it will run software code without checking to see if the code has been signed
15 by Apple. When Apple releases a new iOS, scores of independent programmers
16 study the code, successfully finding ways to circumvent Apple's imposed
17 restrictions. In response, Apple issues software updates to defeat these jailbreaks.
18 Eventually, the jailbreaking community finds new ways to circumvent controls
19 built into Apple's increasingly secure iOSes. Today, all iOS versions through 9.2
20 are jailbroken, even though doing so is increasingly harder due to Apple's efforts.⁹

21 In other words, vulnerabilities in Apple's software have persisted for years
22 even though Apple very much does not want them to. This is a lesson for this case.

23
24
25 ⁹ See Sarah Perez, *You Can Now Jailbreak Your iOS 9 Devices (But You Probably*
26 *Shouldn't)*, TechCrunch (Oct. 14, 2015), [http://techcrunch.com/2015/10/14/you-](http://techcrunch.com/2015/10/14/you-can-now-jailbreak-your-ios-9-devices-but-you-probably-shouldnt/)
27 [can-now-jailbreak-your-ios-9-devices-but-you-probably-shouldnt/](http://techcrunch.com/2015/10/14/you-can-now-jailbreak-your-ios-9-devices-but-you-probably-shouldnt/); *see also*
28 *TaiG9beta*, <http://taig9.com> (offering software to jailbreak iOS 9.0-9.2 and beta-
release version to jailbreak iOS 9.2.1 and 9.3).

1 Apple can try its very hardest to create this Custom Code as the Court directs.
2 Nevertheless, it may well fail, as it has acknowledged to the Court. *See* Motion to
3 Vacate at 13-14. Even with time and extensive testing, which the government's
4 sense of urgency seems designed to deny Apple, it is extremely difficult to write
5 bug-free code. Software bugs can interact with existing code in complex ways,
6 creating unanticipated new paths for bypassing iPhone security and exploiting the
7 phone.

8 Importantly, the most probable outcome of this Order is that Apple will be
9 forced to create forensic software that bypasses the passcode but is *not* limited to
10 the Subject iPhone. U.S. law enforcement agencies have a large number of locked
11 devices from which they would like to acquire forensic data in order to assist in
12 prosecuting the cases in association with which the devices had been seized.¹⁰
13 Ordering Apple to build the Custom Code for U.S. law enforcement will prompt
14 requests from other governments as well. Should the Court's Order stand, other
15 governments will take a keen interest in the Custom Code functionality this Court
16 compels Apple to create. Governments of other countries where Apple sells its
17 devices will want the same treatment Apple will have given to the FBI.

18
19
20
21 ¹⁰ For example, a recent *New York Times* article quoted a statement by Apple that
22 "Law enforcement agents around the country have already said they have hundreds
23 of iPhones they want Apple to unlock if the F.B.I. wins this case." In New York
24 City alone, according to the article, law enforcement "currently possessed 175
25 iPhones that they could not unlock." The piece quotes Manhattan District Attorney
26 Cyrus Vance, Jr., who, when asked, "If there is access to [the Subject iPhone], you
27 want access to all those phones that you think are crucial in a criminal
28 proceeding?," responded, "Absolutely right." Katie Benner, *Apple Moves to Shift
Battle Over Unlocking iPhone to Capitol Hill*, N.Y. Times (Feb. 22, 2016),
<http://www.nytimes.com/2016/02/23/technology/apple-unlock-iphone-san-bernardino.html>.

1 Apple is not likely to delete the Custom Code. *See* Motion to Vacate at 14,
2 24-25. It is expensive and difficult to build the Custom Code, but once built, it is
3 trivial for Apple to change it to work on any other iPhone. Given the demand,
4 Apple would keep the code and then either modify it code for each of the many
5 devices covered by future court orders, or more likely, remove the few lines of
6 code that tie the forensic software to one particular device in order to comply with
7 these demands. In sum, the Custom Code will neither be tied to the Subject iPhone
8 nor will it be deleted.

9 **B. Apple Will Likely Lose Control Of the Code, Due Either to Legal**
10 **Compulsion or Theft**

11 This Court also allowed the Custom Code to stay with Apple, rather than go
12 to the FBI. Simply put, if no one else has the Custom Code, no one else should be
13 able to use it, at least not without Apple's knowledge. However, once created, this
14 software is going to be *very valuable* to law enforcement, intelligence agencies,
15 corporate spies, identity thieves, hackers, and other attackers who will want to steal
16 or buy the Custom Code. Keeping the Custom Code secret is essential to ensuring
17 that this forensic software not pose a broader security threat to iOS users. But the
18 high demand poses a serious risk that the Custom Code will leak outside of
19 Apple's facilities.

20 Other governments, or ours, may eventually compel Apple to turn the
21 Custom Code over so that law enforcement officials can unlock phones without
22 delay or Apple oversight. Authoritarian governments will likely be the most
23 enthusiastic customers for the Custom Code this Court is contemplating ordering
24 Apple to create and sign. The software will be used in China, Russia, Turkey, the
25 United Arab Emirates, and other governments with poor human-rights records
26 where iPhones are sold.

27 Inadequate security practices by those governments increase the risk that
28 attackers will acquire and use the Custom Code. Given the Custom Code's value,

1 unscrupulous government officials in corruption-plagued jurisdictions could
2 foreseeably sell the Custom Code to third parties. For example, if the Russian
3 government compelled Apple to hand over the Custom Code, it could end up being
4 sold by a corrupt agent to a Russian identity-theft ring. Even without selling it,
5 corrupt officials could also use the code for their own agendas, such as to target
6 political or personal enemies who had broken no law. Journalists, human-rights
7 advocates, religious and sexual minorities, and others in those countries are at
8 much greater risk if software that can bypass passcode limitations exists.

9 There is also a danger that the Custom Code will be lost or stolen. The more
10 often Apple must use the forensic capability this Court is ordering it to create, the
11 more people have to have access to it. The more people who have access to the
12 Custom Code, the more likely it will leak. The software will be valuable to anyone
13 eager to bypass security measures on one of the most secure smartphones on the
14 market. The incentive to steal the Custom Code is huge. The Custom Code would
15 be invaluable to identity thieves, blackmailers, and those engaged in corporate
16 espionage and intellectual property theft, to name a few.

17 Those technicians responsible for using the Custom Code to comply with
18 access demands will likely be targeted by phishing attacks—emails carefully
19 designed to seem legitimate but which contain malware—that seek to steal the
20 Custom Code. The same technicians will be approached with offers to buy the
21 software. The price offered could be irresistibly high, as the Custom Code will be
22 worth a lot to foreign national security officials and organized crime syndicates,
23 and can be sold to multiple customers. Or Apple technicians may be blackmailed
24 to the same end. In short, the Custom Code will be exceedingly valuable and in
25 danger of leaking or being stolen.
26
27
28

1 International demand further exacerbates the risk that the Custom Code will
2 fall into the wrong hands. Even if Apple can reliably secure its own headquarters in
3 Cupertino¹¹ (to which the Order contemplates the code would be confined in the
4 current case), Apple could be required by future courts in future cases to provide
5 the Custom Code (not merely the data extracted from a device) to U.S. or other
6 governments' agents, whose physical security practices are beyond Apple's
7 control.

8 If the Custom Code is signed by Apple, and capable of being used on any
9 device, that is the worst-case scenario. If that leaks, the public danger is apparent
10 and could be catastrophic.¹² But even if Apple writes the Custom Code such that it
11 must input an iPhone device identifier and then sign the software, leak or theft
12

13 ¹¹ Mistakes happen. Apple has had leaks of internal non-public iPhones in the past,
14 albeit from locations outside the Apple main campus. *E.g.*, Greg Sandoval and
15 Declan McCullagh, *Lost iPhone Prototype Spurs Police Probe*, CNET (Apr. 23,
16 2010), <http://www.cnet.com/news/lost-iphone-prototype-spurs-police-probe/> (pre-
17 release iPhone 4G accidentally left in a bar by an Apple software engineer); Greg
18 Sandoval and Declan McCullagh, *Apple Loses Another Unreleased iPhone*
19 *(Exclusive)*, CNET (Aug. 31, 2011), <http://www.cnet.com/news/apple-loses-another-unreleased-iphone-exclusive/> (another pre-release iPhone model went missing from a different bar).

20 ¹² iPhones and iPad tablet devices (which also run iOS) are in use not just by
21 members of the general public, but by airline pilots, surgeons, police, and President
22 Obama. *See generally* iPad in Business,
23 <https://www.apple.com/ipad/business/profiles/> (linking to Apple business-customer
24 use cases for iPads and iPhones, including United Airlines, the Mayo Clinic, and
25 the Redlands (California) Police Department); *see also* Killian Bell, *President*
26 *Obama Answers Questions on Cool iPad Setup*, iPhoneHacks.com (July 3, 2015),
27 <http://www.iphonhacks.com/2015/07/president-obama-answers-healthcare-questions-on-cool-ipad-setup.html> (noting that “[a]lthough Obama isn’t allowed to
28 use an iPhone for security reasons, his administration has long been using other Apple devices,” including iPads, and that Apple sends new iPad models to the President).

1 poses a security risk. Having access to the Custom Code is a dangerous stepping
2 stone towards a successful attack. The Custom Code helps attackers understand the
3 passcode limitations bypass. Knowledge is half the battle. It brings attackers one
4 step closer to defeating this important iPhone security measure.

5 If the Court's Order stands, Apple's market and office presence in
6 authoritarian jurisdictions will inevitably subject it to government demands to
7 install Custom Code on devices they wish to target for purposes inconsistent with
8 liberty and human rights.¹³ Should Apple refuse, a foreign government can use the
9 threat of jailing in-country Apple employees (as Brazil did earlier this week to a
10 Facebook vice president),¹⁴ seizing inventory, or shutting down the business, as
11 leverage to induce Apple to relent. In sum, once the capability of bypassing the
12 passcode limitations exists, the United States will have thrown away both a moral
13 and a practical argument against authoritarian abuse of iPhone customers.

14 The Court's Order does not and cannot account for these eventualities.

15
16
17 ¹³ See Ewen MacAskill, *Yahoo Forced to Apologise to Chinese Dissidents over*
18 *Crackdown on Journalists*, The Guardian (Nov. 14, 2007),
19 <http://www.theguardian.com/technology/2007/nov/14/news.yahoo> (reporting on
20 settlement of lawsuit brought against Yahoo by families of two dissidents whom
21 China prosecuted and imprisoned; Yahoo had helped the Chinese government
22 identify them by handing over their email records, claiming "it had no choice other
23 than to comply with a request from Beijing to share information about the online
24 activities of the journalists").

25 ¹⁴ Facebook owns popular encrypted messaging service WhatsApp. This week,
26 after the company did not comply with a court order to produce WhatsApp user
27 data to investigators in a drug case, Brazilian federal police arrested Facebook's
28 vice president for Latin America. He was freed the following day. Brazil had
previously blocked WhatsApp briefly in December for similar reasons. Brad
Haynes, *Facebook Executive Jailed in Brazil as Court Seeks WhatsApp Data*,
Reuters (Mar. 1, 2016), [http://www.reuters.com/article/us-facebook-brazil-
idUSKCN0W34WF](http://www.reuters.com/article/us-facebook-brazil-idUSKCN0W34WF).

1 **C. The Court’s Order Would Set A Precedent For Forcing Vendors**
2 **to Turn Their TVs and Other Consumer Goods Into FBI**
3 **Surveillance Tools**

4 If this Order stands, the FBI might demand next that Apple assist law
5 enforcement by surreptitiously turning on an iPhone microphone or camera, for
6 example. Mobile devices are among the most intimate devices in existence. Many
7 Americans sleep with their mobile phones by their beds. Front and rear facing
8 cameras are capable of seeing users and their surroundings at any time. There is a
9 microphone capable of recording the user, and an accelerometer sensitive enough
10 to identify users by their gait. Forced software “updates” could convert these
11 consumer friendly features into government surveillance tools to be deployed
12 against a target or a community.

13 iPhones and other mobile phones are not the only common consumer
14 appliances that this Order sets a precedent for converting to surveillance devices.
15 Amazon distributes an appliance called the Echo that captures spoken voice.¹⁵
16 While Amazon designed the Echo only to send voice data to Amazon if it “hears”
17 the word “Alexa,” that limitation, like the iPhone passcode limitations, is encoded
18 in software. Similarly, smart TVs, like those sold by Samsung, capture and
19 transmit owners’ voices in an effort to identify natural language commands and
20 search requests. In responding to consumer privacy concerns, Samsung assured the
21 public that TV owners’ voice data would only be collected if the TV user clicks the
22 activation button and speaks into the microphone on the remote control.¹⁶ Again,

23 ¹⁵ Avie Schneider, *Amazon Wants To Put A Listening Speaker In Your Home*,
24 National Public Radio (Nov. 6, 2014),
25 [http://www.npr.org/sections/alltechconsidered/2014/11/06/362088269/amazon-](http://www.npr.org/sections/alltechconsidered/2014/11/06/362088269/amazon-wants-to-put-a-listening-speaker-in-your-home)
[wants-to-put-a-listening-speaker-in-your-home](http://www.npr.org/sections/alltechconsidered/2014/11/06/362088269/amazon-wants-to-put-a-listening-speaker-in-your-home).

26 ¹⁶ Samsung Smart TVs Do Not Monitor Living Room Conversations,
27 [https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-](https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations)
28 [conversations](https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations).

1 like the iPhone passcode limitations, this privacy safeguard is a function of
2 software. If the government is allowed compel Apple to change its software to
3 enable decryption and forensic access here, will it also be allowed to compel
4 Amazon to update the Echo, or Samsung to update its Smart TVs, to always collect
5 some customers' conversations?

6 Converting the tools of modern living into eavesdropping bugs could be
7 something law enforcement is eager to do. These future forensic capabilities will
8 not just raise serious privacy questions. They also pose *security* risks, and not just
9 to the owners of the particular iPhones, Echos, and smart TVs, but, because these
10 consumer devices interact with each other and the public Internet, to the public at
11 large.

12 Each of these workarounds could pose its own unique security risks to the
13 public. Without question and in every case, creating a security bypass is risky.
14 Assessing how risky is a case-by-case, fact dependent job, which even experienced
15 security designers can get wrong. Fully-remote forensic tools are more dangerous
16 than ones that can only be used locally, as they are hard for the target to detect and
17 thus more susceptible to illegitimate use. Likewise, tools that must be designed for
18 a class of products are more dangerous than those that can theoretically be limited
19 to a particular device. A signed firmware update that is not truly limited to a single
20 device, even one created for legitimate forensic purposes, becomes like a “skeleton
21 key” for the entire class of devices. A “skeleton key” that can be used remotely
22 against numerous devices is thus a formidable cybersecurity threat should it fall
23 into the wrong hands. On its face, the Court's Order does not call for such a tool—
24 but it opens the Pandora's box that contains it.

25 **D. The Court's Order Risks Undermining Critical Public Trust in**
26 **Automatic Software Security Updates**

27 The biggest consequence from forced code signing like that ordered in this
28 case could be a general erosion of public trust in software updates. When iPhone

1 users know that Apple can be forced to create, sign, and deliver software updates
2 that decrease, rather than increase, user security, they will not want to install the
3 updates. The Court's Order in this high-profile case threatens to undermine an
4 important trust relationship not just between Apple and its customers, but also
5 between software vendors and the general public. This loss of trust would lead to a
6 decrease in the overall level of security of mobile devices and computers.

7 Apple periodically transmits software updates to its customers' iPhones in
8 order to fix vulnerabilities in iOS.¹⁷ Microsoft does the same with Windows
9 updates. Vendors also may automatically update applications. These updates,
10 which typically are cryptographically signed, fix newly discovered vulnerabilities
11 that attackers can use to steal private data. A signed update is designed to improve
12 software functionality and/or to patch security vulnerabilities. The vendor's
13 cryptographic signature verifies to a mobile device, desktop, or laptop computer
14 (and its user) that a software update is legitimate and safe to install.

15 Automatic updates are an important way that software companies ensure
16 their users are as protected as possible from attackers, without inconvenience,
17 significant effort, or technical savvy on the part of the user (who is more likely to
18 install security updates when there is little or nothing she needs to do). These auto-
19 updates are one of the reasons why the millions of iPhones currently in use
20 worldwide are very secure.

21 Consumers (and their devices) trust these auto-updates because they are
22 signed by the vendor. A cryptographic signature from Microsoft or Apple assures
23 the user that the software she is about to install legitimately comes from the
24

25
26 ¹⁷ See generally Update the iOS Software on Your iPhone, iPad, or iPod Touch,
27 <https://support.apple.com/en-us/HT204204> (instructing users how to install updates
28 when notified that an update is available).

1 company she trusts. It is akin to Apple saying, “This is Apple, and we stand behind
2 this software.” Here, however, the Court is contemplating ordering Apple to sign
3 software it does not stand behind and in fact considers “too dangerous to build.”
4 Motion to Vacate at 2. And the next logical step if this Court enforces its Order is
5 for the FBI to ask to compel other vendors, in addition to Apple, to sign other
6 software that bypasses other customer security measures, creating new and
7 different risks.

8 This is why compelling cryptographic signatures is extremely risky.
9 Automatic software updates are a crucial vehicle for maintaining the security of
10 iOS devices and other computers, but they can be effective only so long as users
11 continue to trust them. If the Court compels Apple to create and sign the Custom
12 Code in this high-profile case, then all computer users, especially those for whom
13 smartphone privacy may already be a concern,¹⁸ could become suspicious of all
14 software updates going forward. That is because a member of the public could
15 reasonably fear that in the future, even a signed software update from a trusted
16 vendor will bypass passcode limitations, convert her iPhone into an audio or video
17 recording device, or otherwise interfere with her property, privacy, or security
18 interests.¹⁹ Users will know that these updates could be software designed to

19
20 ¹⁸ See Lorrie Faith Cranor *et al.*, *Supporting Privacy-Conscious App Update*
21 *Decisions with User Reviews*, in *Proceedings of the 5th Annual ACM CCS*
22 *Workshop on Security and Privacy in Smartphones and Mobile Devices* (2015),
23 <http://mews.sv.cmu.edu/papers/spsm-15.pdf> (study of Android smartphone users’
reasons for choosing whether or not to update installed apps automatically; privacy
invasiveness found to be a top reported reason for not updating apps).

24 ¹⁹ Governments, including our own, are very interested in developing the ability to
25 install spyware on users’ machines for intelligence and other purposes. The U.S.
26 National Security Agency already has found ways its spyware can masquerade as a
27 legitimate software installation. See Bruce Schneier, *Attacking Tor: How the NSA*
28 *Targets Users’ Online Anonymity*, *The Intercept* (Oct. 4, 2013),
<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online->

(Footnote Continued on Next Page.)

1 extract private data from the user's machine, but which a company was forced to
2 sign at the behest of some court, law enforcement, or other government official.
3 The code would be indistinguishable from a genuine update created, signed, and
4 transmitted of the vendor's own free will.

5 This distrust would have serious ramifications for computer security at large.
6 In response, some users would likely stop accepting iOS updates (which users must
7 choose to install), in which case their machines will remain unprotected against
8 vulnerabilities that legitimate automatic updates would have patched. Importantly,
9 the impact of unpatched devices is not limited to those devices. Vulnerable
10 software that has not been updated can become a vector for spreading malware,
11 potentially compromising other machines on the network. The more users who turn
12 off automatic updates, the more devices, the more information, the more people put
13 at risk. Just as herd immunity to a disease is lost if enough members of the group
14 are not vaccinated against the disease, if enough users stop auto-updating their
15 devices, it will weaken the entire device security ecosystem. Indeed, one computer
16 security expert has likened automatic updates to "a public health system for the
17 Internet."²⁰ It is this whole system which the Court ultimately threatens to put at
18 risk should it enforce its Order to Apple.

19
20 _____
(Footnote Continued from Previous Page.)

21 anonymity. So has the United Arab Emirates. Ben Thompson, *UAE Blackberry*
22 *update was spyware*, BBC News (July 21, 2009),
23 <http://news.bbc.co.uk/2/hi/8161190.stm>.

24 ²⁰ *Does the FBI Need a Back Door to Your Data?*, KCRW (Feb. 23, 2016),
25 [http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone-](http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone-unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data)
26 [unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data](http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone-unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data) (Chris Soghoian,
27 Principal Technologist and Senior Policy Analyst with the American Civil
28 Liberties Union's Speech, Privacy and Technology Project, interviewed for radio
show about the instant case).

1 **II. Security Breaches Are All But Certain When Law Mandates**
2 **Government Access**

3 The threat to public security is an important reason why this Court should
4 not set a precedent of using the All Writs Act to force companies to bypass
5 cybersecurity measures in the name of investigations. The AWA's authority to
6 issue writs to non-parties simply does not account for the public-security dangers
7 this Court's Order creates, nor the future risks that future orders will also pose. The
8 plain language of the statute creates no obligations and gives no guidance to courts
9 considering the very important and technologically nuanced underlying security
10 risks associated with mandating forensic access to private data.

11 In the past, lawful access mechanisms that private parties were forced to
12 build have been exploited by attackers. In 2004 and 2005, unknown persons
13 (recently revealed to be the National Security Agency²¹) exploited the law
14 enforcement backdoors built into Greece's communications system to spy on more
15 than 100 Greek officials (including the prime minister and the mayor of Athens), in
16 what has been called Greece's Watergate. In 2010, an IBM researcher observed
17 that a Cisco architecture for enabling lawful interception in IP networks was
18 insecure. Security experts have identified other examples, and explained why
19 successful attacks on lawful access mechanisms are to be expected.²²

20 The Court's Order opens the door to a host of privacy and security problems.
21 As experts, *amici* know that secure coding is very hard, even when there is just one

22
23 ²¹ James Bamford, *A Death in Athens: Did a Rogue NSA Operation Cause the*
24 *Death of a Greek Telecom Employee?*, The Intercept (Sept. 28, 2015),
25 <https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/> (meticulous
26 investigatory reporting on the so-called "Athens Affair," whose perpetrators had
27 remained unknown for a decade).

28 ²² Harold Abelson, *et al.*, *Keys Under Doormats: Mandating Insecurity by*
Requiring Government Access to All Data and Communications (2015),
<https://dspace.mit.edu/handle/1721.1/97690>.

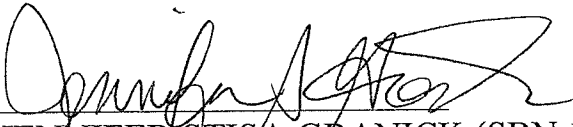
1 clear goal—protect the user’s data. Here, the Court seeks to require Apple to also
 2 fulfill a competing goal—assist law enforcement with this (and eventually other)
 3 investigation(s). Accommodating competing goals of security and access is not
 4 something that even state of the art software coders do well. Experience and
 5 history lead to the conclusion that forcing a company to undermine its own product
 6 security will thereby imperil not just the cybersecurity but also the physical
 7 security of its worldwide users.

8 CONCLUSION

9 Compelling a company to create and run a piece of custom forensic software
 10 for a target’s phone is unprecedented. So is compelling a company to digitally sign
 11 a piece of code. As experts experienced in both analyzing and building security
 12 functionality on iOS-based devices, *amici* believe that any such Order poses a
 13 public-safety risk. These are highly technical and complex computer security
 14 issues in a field that evolves much more quickly than the law. Given the difficulty
 15 of building security systems correctly and the crucial public importance of doing
 16 so, *amici* believe that the courts, Congress, and law enforcement alike should
 17 refrain from dictating to companies that they must weaken or bypass security
 18 features or build forensic capabilities into their products like the one at issue here.

19 For the foregoing reasons, *amici* believe the government’s Application
 20 should be rejected and the Order vacated.

21
 22 Dated: March 2, 2016


 23 JENNIFER STISA GRANICK (SBN 168423)
 24 RIANA PFEFFERKORN (SBN 266817)
 25 STANFORD LAW SCHOOL
 26 CENTER FOR INTERNET AND SOCIETY

27 Attorneys for [Proposed] *Amici Curiae*
 28 iPhone Security and Applied Cryptography
 Experts

LODGED

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

JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
RIANA PFEFFERKORN (SBN 266817) 2016 MAR 3 PM 3:19
riana@law.stanford.edu
STANFORD LAW SCHOOL
CENTER FOR INTERNET AND SOCIETY
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 736-8675
Facsimile: (650) 725-4086

CLEARING U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
BY: _____

FILED
CLERK, U.S. DISTRICT COURT
3/4/2016
CENTRAL DISTRICT OF CALIFORNIA
BY: _____ DEPUTY

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION**

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

ED No. CM 16-10 (SP)
CERTIFICATE OF SERVICE

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

CERTIFICATE OF SERVICE

I, AMANDA AVILA, declare:

That I am a citizen of the United States and resident or employed in Santa Clara County, California; that my business address is Stanford Law School, Center for Internet and Society, 559 Nathan Abbott Way, Stanford, CA 94305; that I am over the age of eighteen years, and not a party to the above-entitled action; that I am employed by Jennifer Stisa Granick who is a member of the Bar of the United States District Court for the Central District of California, at whose direction I served a copy of the following:

1. **APPLICATION OF [PROPOSED] *AMICI CURIAE* IPHONE SECURITY AND APPLIED CRYPTOGRAPHY EXPERTS FOR LEAVE TO FILE BRIEF IN SUPPORT OF MOVANT APPLE INC.**
2. **BRIEF OF *AMICI CURIAE* IPHONE SECURITY AND APPLIED CRYPTOGRAPHY EXPERTS IN SUPPORT OF APPLE INC.'S MOTION TO VACATE ORDER COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH, AND OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE**
3. **[PROPOSED] ORDER GRANTING APPLICATION OF [PROPOSED] *AMICI CURIAE* IPHONE SECURITY AND APPLIED CRYPTOGRAPHY EXPERTS FOR LEAVE TO FILE BRIEF IN SUPPORT OF MOVANT APPLE INC.**
4. **NOTICE OF APPEARANCE OF COUNSEL**

By overnight delivery as follows:

Allen W. Chiu
AUSA – Office of US Attorney
National Security Section
312 North Spring Street, Suite 1300
Los Angeles, CA 90012

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
Counsel for Plaintiff United States of America

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

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

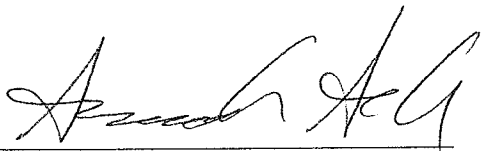
Marc J Zwillinger
Jeffrey G Landis
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036

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

Theodore B Olson
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 20036-5306
Counsel for Respondent Apple Inc.

This Certificate is executed on March 2, 2016, in Stanford, California. I certify under penalty of perjury that the foregoing is true and correct.

Dated: March 2, 2016


AMANDA AVILA