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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Cases

Other Authorities

INTERESTS OF *AMICI CURIAE*

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

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

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

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

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

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

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

Amicus 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.

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

SUMMARY OF ARGUMENT

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

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

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

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

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

FACTUAL BACKGROUND

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

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

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

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

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

---

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

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

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

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

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

---

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

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

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

The Subject iPhone runs iOS 9.0.[4] Since Apple does not have the passcode, the only recourse to decrypt and access data stored exclusively on the Subject iPhone is to guess the passcode. The government is concerned that, as a result of these passcode security features, it will take too long to guess the passcode, and that if it makes too many wrong guesses, it could cause the Subject iPhone to automatically delete the data on it.

Consequently, the government asked for and received a technical assistance order from this Court to Apple pursuant to the All Writs Act ("AWA"), 28 U.S.C. § 1651.[5] The Order requires Apple to write software that will accomplish three

---

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

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

[5] Order Compelling Apple, Inc. To Assist Agents in Search, Crim. No. 15-mj-451,

(Footnote Continued on Next Page.)

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

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

The Court Order Would Compel Apple to Sign, Or Validate, the Custom Code. Once the Custom Code is created, complying with the Order requires Apple to authenticate the new code by cryptographically signing it. Apple's hardware is designed to only run software that has been cryptographically "signed" by Apple or by another entity that has been authorized by Apple to also sign software to run

---

(Footnote Continued from Previous Page.)

D.I. 19 (hereafter "Order") at 1.

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

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

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

ARGUMENT

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

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

---

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

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

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

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

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

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

---

[8] *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).

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

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

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

---

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

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

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

---

[10] For example, a recent *New York Times* article quoted a statement by Apple that "Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the F.B.I. wins this case." In New York City alone, according to the article, law enforcement "currently possessed 175 iPhones that they could not unlock." The piece quotes Manhattan District Attorney Cyrus Vance, Jr., who, when asked, "If there is access to [the Subject iPhone], you want access to all those phones that you think are crucial in a criminal 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.

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

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

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

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

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

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

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

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

International demand further exacerbates the risk that the Custom Code will fall into the wrong hands. Even if Apple can reliably secure its own headquarters in Cupertino[11] (to which the Order contemplates the code would be confined in the current case), Apple could be required by future courts in future cases to provide the Custom Code (not merely the data extracted from a device) to U.S. or other governments' agents, whose physical security practices are beyond Apple's control.

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

---

[11] Mistakes happen. Apple has had leaks of internal non-public iPhones in the past, albeit from locations outside the Apple main campus. *E.g.*, Greg Sandoval and Declan McCullagh, *Lost iPhone Prototype Spurs Police Probe*, CNET (Apr. 23, 2010), http://www.cnet.com/news/lost-iphone-prototype-spurs-police-probe/ (pre-release iPhone 4G accidentally left in a bar by an Apple software engineer); Greg Sandoval and Declan McCullagh, *Apple Loses Another Unreleased iPhone (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).

[12] iPhones and iPad tablet devices (which also run iOS) are in use not just by members of the general public, but by airline pilots, surgeons, police, and President Obama. *See generally* iPad in Business, https://www.apple.com/ipad/business/profiles/ (linking to Apple business-customer use cases for iPads and iPhones, including United Airlines, the Mayo Clinic, and the Redlands (California) Police Department); *see also* Killian Bell, *President Obama Answers Questions on Cool iPad Setup*, iPhoneHacks.com (July 3, 2015), http://www.iphonehacks.com/2015/07/president-obama-answers-healthcare-questions-on-cool-ipad-setup.html (noting that "[a]lthough Obama isn't allowed to 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).

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

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

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

---

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

[14] Facebook owns popular encrypted messaging service WhatsApp. This week, after the company did not comply with a court order to produce WhatsApp user data to investigators in a drug case, Brazilian federal police arrested Facebook's 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.

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

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

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

---

[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/2014/11/06/362088269/amazon-wants-to-put-a-listening-speaker-in-your-home.

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

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

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

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

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

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

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

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

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

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

---

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

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

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

---

[18] *See* 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 (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).

[19] Governments, including our own, are very interested in developing the ability to install spyware on users' machines for intelligence and other purposes. The U.S. National Security Agency already has found ways its spyware can masquerade as a legitimate software installation. *See* Bruce Schneier, *Attacking Tor: How the NSA 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.)

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

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

(Footnote Continued from Previous Page.)

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

[20] *Does the FBI Need a Back Door to Your Data?*, KCRW (Feb. 23, 2016), 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, Principal Technologist and Senior Policy Analyst with the American Civil Liberties Union's Speech, Privacy and Technology Project, interviewed for radio show about the instant case).

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

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

In the past, lawful access mechanisms that private parties were forced to build have been exploited by attackers. In 2004 and 2005, unknown persons (recently revealed to be the National Security Agency[21]) exploited the law enforcement backdoors built into Greece's communications system to spy on more than 100 Greek officials (including the prime minister and the mayor of Athens), in what has been called Greece's Watergate. In 2010, an IBM researcher observed that a Cisco architecture for enabling lawful interception in IP networks was insecure. Security experts have identified other examples, and explained why successful attacks on lawful access mechanisms are to be expected.[22]

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

---

[21] 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/ (meticulous investigatory reporting on the so-called "Athens Affair," whose perpetrators had remained unknown for a decade).

[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.

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

CONCLUSION

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

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

Dated: March 2, 2016

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

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