



February 29, 2016

The Honorable Bob Goodlatte
Chairman, House Judiciary Committee
2138 Rayburn House Office Bldg.
Washington, D.C. 20515

The Honorable John Conyers, Jr.
Ranking Member, House Judiciary Committee
2138 Rayburn House Office Bldg.
Washington, D.C. 20515

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

KARIN JOHANSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

**RE: House Judiciary Committee Hearing on “The Encryption Tighrope:
Balancing Americans’ Security and Privacy.”**

Dear Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee,

On behalf of the American Civil Liberties Union (“ACLU”¹), we submit this letter in connection with the March 1, 2016 hearing, “The Encryption Tighrope: Balancing Americans’ Security and Privacy.”

Over the last decade, the technology industry has made significant progress in protecting the security of Americans’ private data, including electronic communications, through enhanced security features and encryption technologies. This increased security has not only paved the way for advanced technological and economic development, but has been critical to ensuring free expression and an open Internet. Unfortunately, there have been calls by some to undermine— rather than support— these security advances. Specifically, the FBI is currently seeking to compel Apple to develop new software that would allow the FBI to hack into the work phone of one of the San Bernardino shooters.² One magistrate judge in New York has already ruled that such a request is not authorized by the law, noting that Congress has explicitly declined to provide this authority.³ Another case on this issue is pending.

¹ For nearly a century the ACLU has been our nation’s guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual’s rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

² 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, No. 15-0415M (C.D. Cal. Feb. 16, 2016).

³ Devlin Barrett, *Judge Sides With Apple in Drug Case Involving Locked Phone*, W.S.J. Feb. 29, 2016, <http://www.wsj.com/articles/judge-sides-with-apple-in-drug-case-involving-locked-phone-1456785910>; Memorandum and Order, *In Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2015 WL 5920207 (E.D.N.Y. 2016), available at <http://www.politico.com/f/?id=00000153-2f2b-d640-a7fb-7fbb72380001>.

The ACLU opposes the FBI efforts in the Apple case. They are unauthorized, unconstitutional, and unwise. We urge the Committee to reject any proposal that would grant the FBI the authority to conscript technology suppliers into hacking or building a backdoor into the devices of users.

I. Advancements in Encryption and Other Security Features

In recent years, Apple has added security features and enhanced encryption on its mobile devices. – responding to increased consumer demands for greater privacy and security. These features are designed to protect consumers from criminals, hackers, or even malicious foreign governments. The more recent versions of the Apple iOS operating system:

- Allow consumers to turn on a feature that makes the contents of the phone inaccessible in the event that a PIN code is incorrectly entered ten times;
- By default, create a time lag between incorrect PIN entries, to prevent a malicious actor from bombarding the phone with numerous PIN attempts in a row;
- Require the user's PIN to unlock and decrypt the data stored on the phone. In other words, without a user's PIN, no one, including Apple, can unlock an iPhone; and
- Expand the categories of data protected by industry-standard encryption to include photos, text messages, the address book, and several other forms of previously less-protected private data.⁴

Many of these changes mirror the industry trend of providing consumers enhanced security through encryption. Last September Google announced it would turn on disk encryption by default in the next version of its Android operating system, though this currently remains an opt-in feature due to reduction in speed suffered by many Android devices when encryption is used.⁵ In addition, encryption is being adopted to protect data as it is transmitted over the Internet. Major companies like Google, Facebook, and Twitter all use HTTPS and other transport encryption technologies to ensure that communication between their customers and their own servers are secure. The federal government has followed the technology industry's lead, and announced that all U.S. government websites will use HTTPS encryption within two years.⁶ Similarly, 76 members of Congress use HTTPS encryption by default on their official websites.⁷

⁴ Apple had for several years included such strong encryption technology in its mobile operating system; however, prior to last year, this method of encryption only protected a few categories of data stored on devices, such as email messages and data created by third party apps. Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot*, ARS TECHNICA (Sept. 18, 2014), <http://arstechnica.com/apple/2014/09/17/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/>.

⁵ Andrew Cunningham, *Google Quietly Backs Away from Encrypting New Lollipop Devices by Default*, ARS TECHNICA (Mar. 2, 2015), <http://arstechnica.com/gadgets/2015/03/02/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/>.

⁶ See *The HTTPS-Only Standard*, CHIEF INFORMATION OFFICER, <https://https.cio.gov/> (last visited Apr. 29, 2015) (“The American people expect government websites to be secure and their interactions with those websites to be private. Hypertext Transfer Protocol Secure (HTTPS) offers the strongest privacy protection available for public web connections with today's internet technology. The use of HTTPS reduces the risk of interception or modification of user interactions with government online services.”).

⁷ Eric Mill (@konklone), TWITTER (Apr. 18, 2015, 4:18PM), <https://twitter.com/konklone/status/589538454352097282>.

The adoption of these encryption technologies has yielded significant benefits to consumers, businesses, and government agencies, providing greater protection from the ever-increasing threat posed by cyber criminals and foreign governments.

II. The Apple Case

Currently, the FBI seeks to create legal precedent that would enable it to force private companies to develop software to hack into its customers' devices and access encrypted data. In the case at hand, the FBI argues that the 1789 All Writs Act grants it the authority to compel Apple to create a mechanism that allows the FBI to circumvent the existing security features in the iPhone to access to contents of the recovered phone. As a practical matter, to comply with this order, Apple will need to do three things:

- Create new software designed to circumvent security features, which create a time lag between incorrect PIN attempts or make the contents of the phone inaccessible following ten incorrect PIN entries;
- Cryptographically "sign" the software, which indicates that the software has been developed and validated by Apple. Such a signature is necessary to push the new software onto the target phone, since, as an added security feature, iPhones will not run software that has not been validated by Apple and
- Take steps to transmit the newly developed software onto the target phone.

If the FBI is successful, the legal precedent established by this case would apply to all companies, devices, or criminal investigations. Thus, it could be used to compel other companies to build mechanisms to hack into smart televisions, computers, or even medical devices. For example, law enforcement could require a company to remotely turn on a camera in a smart television to assist with a drug investigation, or require a car company to deliver malicious software to a car's GPS system to allow tracking as part of a tax evasion investigation.

III. The FBI Efforts to Compel Apple Would Place an Unconstitutional Burden on Private Companies

If successful, the FBI's efforts in this case would represent an unauthorized and unconstitutional expansion of the government's authority. While the government can demand the production of relevant evidence, the giving of truthful testimony, or the entry necessary to search for and seize evidence, law enforcement does not hold the general power to enlist private citizens or companies as its agents.

In this case, Apple manufactured the iPhone, but it does not possess or control the personal data stored on it or even have existing software or capabilities capable of accessing such data. Thus, in order to comply with the request, Apple's engineers would have to write new software specifically designed to subvert the security measures they built into the phone. Forcing Apple to take such action would violate the Fifth Amendment. The Fifth Amendment protects innocent third parties from being conscripted by law enforcement, except in narrow circumstances. The present case clearly extends beyond these limits, and raises troubling questions about the authority of law enforcement officials.

Proposals like the FBI's are also a dramatic expansion of a dangerous idea— that the private sector should be responsible for building the government's surveillance infrastructure. Such proposals

switch the burden for surveillance from the government to companies (and through them to their customers, the American people). Consumers would be forced to purchase fundamentally insecure products, with little ability to protect their communications and stored data from cybersecurity threats. Not only does this represent an improper government intrusion, but it threatens to eliminate one of the primary privacy protections that Americans have enjoyed for the last two centuries—namely, the sheer difficulty of mass surveillance. As a practical matter, the cost to law enforcement of surveillance has provided real privacy protection by forcing law enforcement to determine whether investigations merit the use of scarce resources. Shifting the costs and burdens of surveillance onto the private sector weakens this critical protection.

IV. The FBI Efforts to Compel Apple Threaten Free Expression and Human Rights

The FBI's actions in this case also pose a threat to free expression and global human rights. The legal precedent the FBI seeks to establish in this case would ensure that the government is able to demand access to virtually any electronic communication or piece of data, regardless of the device or software that an individual uses. Opening all electronic communication to the possibility of government scrutiny, or making such communication more easily subject to private hacking, could have a chilling effect on free speech, dissuading the public, journalists, or activists from engaging in protected speech. In the past, we have seen how the fear of outside scrutiny, whether by government or otherwise, has made it more difficult for prominent journalists to communicate with sources, leading to self-censoring and hindering reporting on critical issues, especially those related to national security where government secrecy and the potential for the abuse of civil liberties are at their highest.⁸

Indeed, U.S. foreign policy has also long supported efforts to ensure anonymous and secure communication, as a way of promoting free expression, human rights, and an open internet around the world. As part of this policy, the U.S. government has supported projects that provide secure communications to journalists and human rights activists who are often targeted by repressive regimes.⁹ For example, the U.S. government has helped to create tools that provide end-to-end encryption, which provide greater security to users.¹⁰ The FBI's attempts in this case are contrary to this policy, and open the door to repressive regimes demanding that American companies take the same burdensome actions to provide access to their citizens' devices in order

⁸ *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN AMERICA (Nov. 12, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; ACLU & Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy* 22–48 (2014), <https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf>; Jesse Holcomb & Amy Mitchell, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*, PEW RESEARCH CTR. (Feb. 5, 2015), <http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/>.

⁹ See, e.g., *About the Program*, OPEN TECH. FUND, <https://www.opentechfund.org/about> (noting creation of the Open Technology Fund (“OTF”) with U.S. government funding, and OTF’s goal of securing access to the Internet with “encryption tools”).

¹⁰ WhatsApp is adopting encryption mechanisms developed by Open Whisper Systems, which is funded by the Open Technology Fund. See *Projects*, OPEN TECH. FUND, <https://www.opentechfund.org/projects>; *Open Whisper Systems Partners with WhatsApp to Provide End-to-End Encryption*, OPEN WHISPER SYSTEMS BLOG (Nov. 18, 2014), <https://whispersystems.org/blog/whatsapp/>; see also White House, National Security Strategy 21 (Feb. 2015), http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf (“The United States is countering this trend by providing direct support for civil society and by advocating rollback of laws and regulations that undermine citizens’ rights. We are also supporting technologies that expand access to information, enable freedom of expression, and connect civil society groups in this fight around the world.”).

to target dissenters, suppress free expression, or commit other human rights violations

V. The FBI Efforts to Compel Apple Would Harm Cybersecurity

The FBI's efforts to compel Apple to undermine the security of its product will erode consumer confidence and put customers at risk. Forcing Apple to use its software update capability to undermine the security of one of its devices will make consumers wary of software updates, resulting in decreased cybersecurity. In recent years, there have been enormous strides in pushing software updates to consumers. In many cases, these updates help to patch or repair vulnerabilities in consumers' devices that leave them vulnerable to hackers. The viability of this software update apparatus depends, in part, on consumers having confidence that these updates are genuine, and not malicious code in disguise. Should consumers fear that these are not legitimate updates verified by companies, they may simply stop downloading them. In an age when data breaches and identity theft are increasingly common, such a shift in consumer behavior would have disastrous results for cybersecurity.

Moreover, simply by creating this software, Apple is putting its customers at risk. Should anyone be able to replicate or steal such software, it could leave all iPhones vulnerable. Such a risk is not theoretical – prominent technology companies are routinely targeted by malicious actors. In 2009, Google and Microsoft's law enforcement surveillance teams were compromised by Chinese hackers who gained access to a sensitive database with years' worth of information about the U.S. government's surveillance targets.¹¹ In 2014, Microsoft's surveillance team was compromised again, this time by the Syrian Electronic Army.¹² In 2012, a backdoor that was inserted into JuniperOS software in 2008 was compromised, opening customers' network traffic to an unknown adversary.¹³ This is, in part, why Apple's recent move toward strong device encryption is so critical – it ensures that consumers' information is secure even if Apple's own security systems are compromised.

At a time when cybersecurity threats are at the top of our national security agenda, the government should be encouraging companies to enhance security, not calling on companies to take actions that undermine the security and privacy of their users. Thus, we urge the committee to press the FBI to abandon these misguided efforts and instead invest in policies that encourage the adoption of strong encryption and other digital security technologies.

If you have any questions, please feel free to contact Legislative Counsel Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

Sincerely,

¹¹ Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, WASH. POST, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

¹² Tom Warren, *Microsoft Confirms Syrian Electronic Army Hacked into Employee Email Accounts*, THE VERGE, Jan. 15, 2014 <http://www.theverge.com/2014/1/15/5312798/microsoft-email-accounts-hacked-syrian-electronic-army>.

¹³ Dr. Matthew D. Green, Assistant Professor, Dept. of Computer Science, Johns Hopkins Univ., Keynote Address: "On Subverting Trust," at the Network and Distributed System Security Symposium (Feb. 22, 2016).

A handwritten signature in dark ink, appearing to read "Karin Johanson". The signature is fluid and cursive, with a long horizontal stroke at the end.

Karin Johanson

Director, Washington Legislative Office

A handwritten signature in dark ink, appearing to read "Neema Singh Guliani". The signature is cursive and somewhat stylized, with a long horizontal stroke at the end.

Neema Singh Guliani

Legislative Counsel