



April 29, 2015

Dear Member of Congress,

On behalf of the American Civil Liberties Union (“ACLU”), we submit this letter to the House of Representatives Committee on Oversight hearing on April 29, 2015: “Encryption Technology and Potential U.S. Policy Responses.”

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.

Over the last decade, the technology industry has made significant progress in protecting the security of Americans’ private data, including electronic communications, through the expanded use of encryption technologies. This increased security has not only paved the way for enhanced technological and economic development, it has been critical to ensuring free expression and an open internet.

Unfortunately, there have been calls by some to weaken – rather than strengthen – these encryption technologies. Specifically, Director of the FBI, James Comey, has proposed modifications to the Communication Assistance to Law Enforcement Act (CALEA) that would gut strong protections for encryption technology passed by Congress in the 1990s.

While no formal legislative proposal exists, the ACLU would oppose any efforts to remove the protections for strong, backdoor-free encryption in CALEA, or an expansion of the technological surveillance obligations imposed on communications service providers and technology companies.

Such a proposal (1) threatens privacy and places an improper burden on private entities to build the government’s surveillance infrastructure, (2) decreases cyber and national security, and (3) is unnecessary given current law enforcement access to electronic information. Rather than weakening encryption, the ACLU urges Congress and the executive branch to take steps to expand the use of strong encryption, thereby protecting America’s technology infrastructure from increasingly sophisticated cyber threats.

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

MICHAEL W. MACLEOD-BALL
ACTING 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

I. Recent encryption advances

In recent years, there have been several encryption advancements. Last year, Apple and Google announced that their popular smartphone operating systems would, by default, protect data stored on iOS and Android devices with encryption.¹ Although Apple had for several years included such strong encryption technology in its mobile operating system, 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. Apple last year expanded 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.² In contrast, although Google announced in September that it would turn on disk encryption by default in the next version of its Android operating system, the company subsequently reversed course and announced that encryption would remain an opt-in feature due to reduction in speed suffered by many Android devices when encryption is used.³

In addition to protecting stored data, encryption has also been used to protect data as it is transmitted over the Internet. Over the past five years, this method of encryption has increasingly become an industry best practice. Major companies like Google, Facebook, and Twitter all use HTTPS and other transport encryption technologies to ensure that communications between their customers and their own servers is secure. In just the past few months, the federal government has followed the technology industry's lead, and announced that all US government websites will use HTTPS encryption within two years.⁴ Similarly, 76 members of Congress use HTTPS encryption by default on their official websites.⁵

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

II. Requiring companies to build backdoors into their products threatens privacy and places an improper burden on private entities

When Congress passed CALEA in 1994, it included specific language that explicitly protects companies that wish to deliver strong encryption without law enforcement backdoor to their

¹ Craig Timberg, *Apple will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html; Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/>.

² 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/>.

³ 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/>.

⁴ 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.").

⁵ *Tweet from Eric Mill*, TWITTER (Apr. 18, 2015), <https://twitter.com/konklone/status/589538454352097282>.

customers.

47 USC § 1002(b)(3) states:

A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

The legislative history for CALEA makes it clear that it was the intent of congress to "protect the right to use encryption":

Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. This obligation is consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4). Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access

...

Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. **To the contrary, section 2602 protects the right to use encryption.**⁶ (emphasis added)

Now, twenty years later, some are seeking legislative changes which would remove the strong legal protections for encryption created by Congress and instead give the government the ability to compel the manufacture of a surveillance back door into every electronic communication service, product or app.

A real world analogy helps to explain why this is so problematic. Imagine if the government required every home to be built with government-issued, internet-connected cameras and microphones pre-installed. It would provide little reassurance to know that the government would have to get a search warrant to turn those cameras on. We understand intuitively that government surveillance of private activities would be much too easy.

At the same time, proposals like Director Comey's are 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). Every customer would be paying to have surveillance capability pre-installed and ready to go at a moment's notice. And consumers would be forced to purchase fundamentally insecure products, with no option to allow them to protect their communications and stored data from cyber-security threats. Not only does this represent an improper government intrusion, but, as a practical matter, the cost to law enforcement of surveillance has provided real privacy protection by forcing law enforcement to determine if investigations are practical and appropriate uses of resources. An

⁶ H.R. Rept. No. 103-827 (1984), *available at* https://epic.org/privacy/wiretap/calea/H_Rpt_103_827.txt

expansion of the surveillance obligations mandated by CALEA would weaken this critical protection, and open the Internet to easy and pervasive government scrutiny.

III. *Weakening encryption harms cyber and national security*

Absent encryption, all networked communications are fundamentally insecure. Anyone with access to the servers that store our data or the networks that transmit it would be able to intercept any communication, tamper with it, or delete it altogether. This not only jeopardizes freedom of expression and an open internet, it also poses a threat to national and cybersecurity. Modern encryption is an answer to this threat. Properly implemented, it helps to protect against the increasingly frequent and costly cyberattacks waged by malicious hackers and oppressive regimes.

Technical experts, independent oversight boards, and governments have long acknowledged the value of encryption. For example, nearly two decades ago, the Internet Architecture Board (“IAB”) and the Internet Engineering Steering Group (“IESG”) wrote:

The IAB and IESG would like to encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries. . . . The Internet is becoming the predominant vehicle for electronic commerce and information exchange. It is essential that the support structure for these activities can be trusted.⁷

More recently, a review group hand-selected by President Obama echoed that view, recommending that the U.S. government take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.⁸

A proposal that would require companies to weaken existing technologies to facilitate law enforcement access is contrary to this sage advice. As prior efforts have shown, it is virtually impossible to build law enforcement access into products that cannot also be exploited by criminals, hackers, and malicious foreign government. As Stephanie Pell, a Professor at the Army Cyber Institute at West Point has observed:

Back doors create additional “attack surfaces,” that is, code must be written to create the back door and the code must have unfettered access to communications content. The additional code creates the potential for more bugs (more code, more bugs) that could be exploited to allow improper access to the system. Moreover, for a back door in an encrypted communications service to offer interception functionality, the service provider must have momentary access to the unencrypted communications data. As a result, if and when security flaws in the system are discovered and exploited, the worst-case scenario will be unauthorized access to users’ communications. **This means that when**

⁷ IAB and IESG Statement on Cryptographic Tech. & the Internet (Aug. 1996), *available at* <https://tools.ietf.org/html/rfc1984>.

⁸ President’s Review Grp. on Intelligence & Commc’ns Techs., *Liberty and Security in a Changing World* 22 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

compromised, an encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users.⁹
(emphasis added)

There are ample real-world examples that demonstrate the weaknesses inherent in “lawful interception” systems. For example, in 2004 and 2005, the mobile phones of dozens of members of the Greek government were spied upon by an unknown adversary who exploited a backdoor intended for law enforcement. And, 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.¹⁰ In 2014, Microsoft’s surveillance team was compromised again, this time by the Syrian Electronic Army.¹¹

If major technology companies like Microsoft and Google have not been able to secure their law enforcement surveillance databases, what hope is there for smaller, less well-resourced companies? These examples highlight that proposed expansions to CALEA to force companies to build vulnerabilities into their encryption would come at an unacceptable cost to our national and cyber security.

IV. An expansion to CALEA is unnecessary given the unprecedented access law enforcement has to information stored on electronic devices

In many respects, law-enforcement authorities are now operating in a “golden age of surveillance.”¹² While technology promises to secure the content of our communications, it has at the same time made our lives more transparent to law enforcement than ever before. With little effort, law enforcement agencies can now determine a suspect’s exact location over a period of months, access records of all of his calls and electronic communications, and obtain every other digital fingerprint he leaves when interacting with technology.¹³ The increased use of encryption, whether to protect data transmitted over the Internet or in storage on mobile devices, leaves intact many of these existing investigative avenues.

Additionally, as a practical matter, some of the information protected by disk encryption may still be accessible to law enforcement via alternative means. Much of the information stored on

⁹ Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix—Doctrine to Follow*, 14 N.C. J. L. & Tech. 489 (2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262397.

¹⁰ 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.

¹¹ Tom Warrner, *Microsoft Confirms Syrian Electronic Army Hacked into Employee Email Accounts*, THE VERGE (Jan. 15, 2014, 4:35 PM) <http://www.theverge.com/2014/1/15/5312798/microsoft-email-accounts-hacked-syrian-electronic-army>.

¹² Peter Swire, *‘Going Dark’ Versus a ‘Golden Age for Surveillance,’* CTR. FOR DEM. & TECH. (Nov. 28, 2011), <https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99%E2%80%99/>.

¹³ See *United States v. Pineda-Moreno*, No. 08-30385, at 11 (9th Cir. 2010) (denial for rehearing en banc), available at <http://cdn.ca9.uscourts.gov/datastore/opinions/2010/08/12/08-30385.pdf> (“When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that ‘such dragnet-type law enforcement practices’ are already in use.”).

cell phones and other electronic devices are often backed up on the cloud. For example, Apple provides users with free cloud storage as a backup for photos, music, emails, text messages, and other information stored on cell phones, and such backups are enabled by default. Similarly, companies are increasingly relying on cloud computing services to store and backup information, as a way of enhancing security and efficiency. The encryption technologies delivered to consumers by companies like Apple would not interfere with the law enforcement access to information stored in the cloud through appropriate administrative or judicial process.

Moreover, for those who do pose serious threats, governments often have other tools at their disposal. For example, where the NSA cannot crack the encryption used by its targets, it circumvents it in other ways.¹⁴ The FBI has for more than a decade had the capability to hack into the computers and mobile devices of targets, allowing agents to capture data that might otherwise be protected by encryption.¹⁵ Given these other surveillance methods, as well as the plethora of electronic information readily available to law enforcement, expanding CALEA to further facilitate government surveillance is unnecessary and unwise.

V. *Congress and the executive branch should seek to expand the use of encryption technologies and secure our communications systems*

Instead of weakening encryption efforts, Congress and the executive branch should work to patch and remove the many existing vulnerabilities in our communications networks that can be exploited by nation states and cyber criminals. For example, our cellular communications networks use weak, decades-old encryption algorithms, and as a result, Americans calls and text messages can be intercepted by criminals and foreign governments. Indeed, according to ex-US government officials, these vulnerabilities are being exploited by foreign intelligence services here in the Washington DC.¹⁶

At a time when cyber security threats are at the top of our national security agenda, the government should be promoting the use of strong encryption, not calling on companies to weaken their systems and leave them vulnerable to hackers. The expanded use of strong encryption would be much more effective at addressing threats to cyber security than an expansion to CALEA or the creation of new surveillance authorizes under the guise of enhancing cyber information sharing.

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

Sincerely,

¹⁴ Tom Simonite, *NSA Leak Leaves Crypto-Math Intact but Highlights Known Workarounds*, MIT TECH. REV. (Sept. 9, 2013), <http://www.technologyreview.com/news/519171/nsa-leak-leaves-crypto-math-intact-but-highlights-known-workarounds/>.

¹⁵ FBI Sheds Light on 'Magic Lantern' PC Virus, USA TODAY (Dec. 13, 2001), <http://usatoday30.usatoday.com/tech/news/2001/12/13/magic-lantern.htm>.

¹⁶ Jeff Stein, *New Eavesdropping Equipment Sucks All Data Off Your Phone*, NEWSWEEK (June 22, 2014, 8:27 AM), www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html; Ashkan Soltani & Craig Timberg, *Tech Firm Tries to Pull Back Curtain on Surveillance Efforts in Washington*, WASH. POST (Sept. 17, 2014), http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html.



Wes Macleod-Ball

Acting Director

American Civil Liberties Union

915 15th St., NW, Washington, DC 20005



Neema Singh Guliani

Legislative Counsel

American Civil Liberties Union

915 15th St., NW, Washington, DC 20005

202.675.2322

nguliani@aclu.org