WASHINGTON
LEGISLATIVE OFFICE

July 7, 2015

RE: Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"

Dear Chairman Grassley, Ranking Member Leahy, and Members of the Committee,

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter in connection with the July 8, 2015 hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

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

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, the 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 proposal has yet been made public, the ACLU will oppose any proposal to (1) remove the protections for strong, backdoor-free encryption in CALEA; (2) require, request, or incentivize technology companies or communication providers to weaken encryption to enable greater government surveillance; or (3) incentivize, request, or mandate that technology companies retain information or metadata to circumvent encryption efforts.

Such proposals threaten privacy and place an improper burden on private entities to build the government's surveillance infrastructure, decrease cyber and national security, and are 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.

I. Recent encryption advances

In recent years, there have been several encryption advancements, enhancing security and privacy for millions of Americans. Such enhancements have provided increased protection for data that is stored on devices (such as smartphones), as well as data that is transmitted over the Internet.

For example, last year, Apple and Google announced advancements to provide greater protection for information stored on mobile devices. Both companies announced that their smartphone operating systems would, by default, protect data stored on devices with encryption.[1] 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. Last year, Apple 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] Similarly, last September Google announced that it would turn on disk encryption by default in the next version of its Android operating system. Subsequently, however, the company 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]

Enhanced 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 communication between their customers and their own servers are secure. The Washington Post also now encrypts parts of its website to provide greater protection to readers who visit the newspaper's website.[4] Additionally, in just the past several 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.[5] Similarly, 76 members of Congress use HTTPS encryption by default on their official websites.[6]

The adoption of these encryption technologies has yielded significant benefits to consumers,

---

[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] Andrea Peterson, *Washington Post starts to automatically encrypt part of Web site for visitors*, WASH. POST (June 20, 2015), https://www.washingtonpost.com/blogs/the-switch/wp/2015/06/30/washington-post-starts-to-automatically-encrypt-part-of-web-site-for-visitors/.

[5] *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.").

[6] *Tweet from Eric Mill*, TWITTER (Apr. 18, 2015), https://twitter.com/konklone/status/589538454352097282.

businesses, and government agencies, providing enhanced protection from the ever-increasing threat posed by cyber criminals and foreign governments.

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

When Congress passed CALEA in 1994, it disturbingly mandated that telephone companies rework their networks to be wiretap ready – expanding the government's surveillance capabilities in unnecessary and unprecedented ways. Notwithstanding this, however, Congress explicitly limited the scope of CALEA to include specific language that explicitly protects companies that wish to deliver strong encryption without a backdoor for law enforcement to their customers.[7] The legislative history of the act makes clear that it was the intent of Congress to protect the right to use encryption to safeguard information. Notwithstanding this, however, some government officials have sought changes that would remove the strong existing legal protections for encryption and grant the government the ability to compel that companies provide a surveillance backdoor into every electronic communication service, product, or app.

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, and a mandate of this type would be contrary to the protections in our constitution. Requiring a backdoor into any encrypted device is essentially the same; it guarantees that law enforcement has a view of the information of all Americans stored on mobile devices, regardless of whether there is cause to believe they have committed a crime.

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—a government surveillance tax. Consumers would be forced to purchase fundamentally insecure products, with no option to allow them to protect their communications and stored data from cybersecurity 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 expansion of the surveillance obligations mandated by CALEA would weaken this critical protection, and open the Internet to easy and pervasive government scrutiny.

Such pervasive government scrutiny also represents a threat to free expression and an open internet by eliminating the ability of individuals to communicate anonymously without fear of interception by the government. Opening all electronic communication to the possible government scrutiny would create a chilling effect on free speech, dissuading the public, journalists, or activists from engaging in protected, anonymous speech. Indeed, prominent journalists have reported that fear of government scrutiny and surveillance has made it more difficult 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

[7] 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."

potential for the abuse of civil liberties are at their highest.[8]

Many of America's founders recognized this connection between the notion of free expression, anonymity, and cryptography. James Madison, for example, relied on ciphers both in a political capacity as Secretary of State and in his personal correspondence with Thomas Jefferson.[9] Archives of Madison's encrypted letters show him discussing topics ranging from his unsuccessful courtships, to his personal political rivals, to his views on the need to raise taxes.[10] James Lovell, a member of the Continental Congress, designed codes and ciphers that were used widely by members of the congress and their families. John and Abigail Adams famously used Lovell's ciphers to encrypt their personal correspondence.[11] Other early encryptors included George Washington, James Monroe, Alexander Hamilton, Aaron Burr, and John Jay, the first Chief Justice of the U.S. Supreme Court.[12]

U.S. foreign policy has also long supported the notion of anonymity and encryption, as a way of promoting free expression and an open internet around the world. As part of this policy, the U.S. government has supported encryption projects that provide secure communications to journalists and human rights activists who are often targeted by repressive regimes.[13] For example, the U.S. government has helped to create tools that provide end-to-end encryption, which provide greater security to users.[14] Director Comey's proposal is contrary this policy, and opens the door to repressive regimes demanding the same access to the technology products of their citizens, in order to target dissenters and suppress free expression.

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

---

[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] The James Madison Papers, *James Madison's Ciphers*, LIBRARY OF CONGRESS, http://memory.loc.gov/ammem/collections/madison_papers/mjmciphers.html (last visited Feb. 9, 2015).

[10] Ralph E. Weber, *Masked Dispatches: Cryptograms and Cryptology in American History, 1775–1900* 83 (2011).

[11] David Kahn, *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* 181 (1996); The James Madison Papers, supra note 9; Weber, supra note 11, at 83

[12] John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications Is an 'Ancient Liberty' Protected by the United States Constitution*, 2 Va. J.L. & Tech 2 (1997), available at http://www.vjolt.net/vol2/issue/vol2_art2.html. In the century following the invention of the telegraph in 1844, forty-four new commercial ciphers were patented by Americans for both commercial and private uses. See Simon Singh, The Code Book 61, 79 (1999); Kahn, supra note 12, at 191.

[13] 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").

[14] 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.").

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.[15]

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.[16]

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… **This means that when 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**.[17] (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.[18] 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'

---

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

[16] 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.

[17] 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.

[18] Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE SPECTRUM (June 29, 2007), http://spectrum.ieee.org/telecom/security/the-athens-affair.

worth of information about the U.S. government's surveillance targets.[19] In 2014, Microsoft's surveillance team was compromised again, this time by the Syrian Electronic Army.[20]

If major technology companies like Microsoft and Google have not been able to secure their systems, smaller, less well-resourced companies likely remain even more vulnerable. These examples highlight that proposed expansions to CALEA 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.[21]" While technology promises to secure the content of our communications, it, disturbingly, 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.[22] 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, which in many cases themselves raise significant privacy concerns.

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 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. Thus, existing 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.[23] The FBI has for more than a decade had the capability to hack into the computers

---

[19] 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.

[20] 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.

[21] 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/.

[22] *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.").

[23] 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/.

and mobile devices of targets, allowing agents to capture data that might otherwise be protected by encryption and potentially raising additional privacy concerns.[24]

Furthermore, there is little evidence that encryption has been a significant impediment in existing law enforcement investigations. For example, in 2014, the federal government only encountered three federal wiretaps as being encrypted. In only two of these cases were federal agencies unable to access the information sought.[25] Given existing investigative 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-U.S. government officials, these vulnerabilities are being exploited by foreign intelligence services here in the Washington, D.C.[26] Similarly, numerous government systems, including the recently hacked Office of Personnel Management (OPM) systems, which exposed the sensitive information of millions of federal employees, reportedly do not use encryption to protect sensitive data.[27] [28]

At a time when cybersecurity 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,

---

[24] *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.

[25] UNITED STATES COURTS, WIRETAP REPORT 2014 (2014), *available at* http://www.uscourts.gov/statistics-reports/wiretap-report-2014.

[26] 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.

[27] Tal Kopan and David Perera, *Oversight Chairman: Fire Leaders of Hacked Agency*, POLITICO (June 16, 2015), http://www.politico.com/story/2015/06/katherine-archuleta-opm-computer-hack-house-119067.html

[28] Prior to the hack, the OPM Office of Inspector General had noted that several OPM systems lacked appropriate encryption. *See* Office of the Inspector General United States Office of Personnel Management Statement (June 24, 2015), *available at* https://oversight.house.gov/wp-content/uploads/2015/06/McFarland-OPM-OIG-Statement-6-24-Data-Breach-II.pdf.

Michael W. 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