WASHINGTON
LEGISLATIVE OFFICE

Sep. 22, 2015

The Honorable Frank J. Larkin
Office of the Sergeant at Arms and Doorkeeper of the Senate
U.S. Capitol
Room S-151
Washington, DC 20510

The Honorable Paul D. Irving
Office of the Sergeant at Arms of the House of Representatives
U.S. Capitol
Room H-124
Washington, DC 20515

Re: The Civil Liberties Implications of Insecure Congressional Communications and the Need for Encryption

Dear Messrs. Larkin and Irving,

We write to urge you to provide secure communications technology to members of Congress and staff, and to permit member offices to adopt secure technology on their own initiative. While the civil liberties implications of vulnerable government information technology may not be readily apparent, they are nonetheless, and increasingly, significant.

Our tripartite system of government works best when each branch of government is independent and functionally able to serve as an effective check on the other. Congress, for instance, oversees the president and the administrative state, and serves to identify and mitigate waste, fraud, abuse, or illegality through, among other things, the power of the purse, its investigative function, and, in extreme cases, the power to impeach. Congress' ability to exercise that oversight function, however, is only as robust as its independence from interference by other elements of the government, and its insulation from influence by bad actors outside government.

Nowhere was this as clear as in the controversy over the CIA's torture report. As explained by Senator Feinstein, the intelligence committee came to an agreement with the CIA to use agency-provided facilities, including computers and servers, to review documents that were ultimately the basis for the committee's report. Although the CIA purported to create a firewall

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

to give the committee the freedom to review these documents without interference, the CIA nonetheless searched the walled off committee drive, on the CIA-operated server.[1]

One key lesson is that secure communications facilities preserve effective checks and balances in constitutional government, and insecure facilities threaten them. Those checks and balances serve as safeguards of individual liberties and civil rights.[2] They also protect the civil liberties and privacy of the thousands of Congressional and government employees, who are themselves attractive targets of both foreign adversaries and, indeed, insider threats.[3] The recent, devastating breach of the U.S. Office of Personnel and Management's computer systems, which exposed the most sensitive details about up to 22 million federal employees to foreign hackers, made this starkly clear.

Ensuring the security of Congressional communications against all interception—whether by foreign governments, criminals, or even other branches of the U.S. government or rogue Congressional staffers — would promote both basic liberty interests and national security. Accordingly, we urge you to ensure that members of Congress and staff have the tools and training necessary to protect their communications.

I. U.S. Cellular Phone Networks are Insecure

In recent years, the American public has slowly learned what has been known to the computer security community for more than a decade: Security flaws in our telephone networks can be exploited by foreign governments and technologically sophisticated criminals to intercept our phone calls, text messages, and location data.[4] The world's most widely used cellular encryption algorithm,[5] known as A5/1, was designed in the 1980s,[6] broken by cryptographers in the 1990s,[7] and remains widely used today by U.S.

---

[1] Dustin Volz, *CIA Admits to Hacking Senate Computers,* Nat'l J. (JULY 13, 2014), http://www.nationaljournal.com/tech/cia-admits-it-improperly-hacking-senate-computers-20140731.

[2] The Federalist No. 51 (James Madison) ("Ambition must be made to counteract ambition. . . . [T]he private interest of every individual may be a sentinel over the public rights.").

[3] For instance, the Senate sergeant at arms launched an investigation in 2004 into revelations that staff on the Senate Judiciary Committee had repeatedly exploited a security vulnerability in the committee's systems to access restricted communications about judicial nominees without a password. Those files were then used to undercut the opposing party on nominees through leaks to the media. *See* Charlie Savage, *Infiltration of Files Seen as Extensive*, Boston Globe, Jan. 22, 2004, http://bit.ly/1HO9tNa.

[4] Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1 (2014), *available at* http://ssrn.com/abstract=2437678.

[5] Craig Timberg & Ashkan Soltani, *By Cracking Cellphone Code, NSA Has Ability To Decode Private Conversations*, Wash. Post (Dec. 13, 2013), http://www.washingtonpost.com/business/technology/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html.

[6] *See* Security Algorithms Group of Experts, *Report on the Specification and Evaluation of the GSM Cipher Algorithm A5/2*, ETSI (1996) , *available at* http://www.etsi.org/deliver/etsi_etr/200_299/278/01_60/etr_278e01p.pdf ("The algorithm A5/1 was designed and approved in 1988/9.").

[7] *See* Alex Biryukov et al., *Real Time Cryptanalysis of A5/1 on a PC* (2000), http://cryptome.org/a51-bsw.htm (updating a paper published in *Lecture Notes in Computer Science 1978*, at 1–18 (1999)).

cellular networks.[8] Moreover, although modern 3G and 4G networks use more secure encryption algorithms, widely available surveillance equipment[9] can force phones back to the older, less secure networks.[10]

Computer security experts have been warning about these vulnerabilities since the late 1990s.[11] Their warnings have largely been ignored. U.S. phone networks remain vulnerable,[12] and the Federal Communications Commission has not only taken no action to warn the public, but has resisted public disclosure of documents related to U.S. government agency exploitation of these same security flaws.[13]

In the two decades since these flaws were first discovered, surveillance technology companies, as part of the $5 billion dollar per year global market for surveillance technology,[14] have created numerous products designed to exploit them.[15] Such special purpose cellular surveillance products, which are sold by surveillance companies in Russia, China, and Israel to governments around the world, are now among the "bestselling items" at surveillance industry trade shows.[16]

---

[8] Security Research Labs, *GSM Security Country Report: USA* 4 (2013), http://gsmmap.org/assets/pdfs/gsmmap.org-country_report-United_States_of_America-2013-08.pdf.

[9] *See* 3G UMTS IMSI Catcher, PKI, http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/ (last visited Dec. 18, 2014) ("With our 3G UMTS IMSI Catcher you can redirect single UMTS mobile phones to specific GSM frequencies, in order to monitor the conversation with our active or passive cellular monitoring systems.").

[10] *See* Matthew Green, *On Cellular Encryption*, A Few Thoughts on Cryptographic Engineering (May 14, 2013), http://blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html ("[T]he biggest . . . concern for 3G/LTE is that you may not be using it. Most phones are programmed to gracefully 'fail over' to GSM when a 3G/4G connection seems unavailable. Active attackers exploit this feature to implement a rollback attack — jamming 3G/4G connections, and thus re- activating all of the GSM attacks . . . ").

[11] *See* Orr Dunkelman et al., *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*, Int'l Ass'n for Cryptographic Research (2010), http://eprint.iacr.org/2010/013.pdf (citing studies from late 1990s and noting "[t]he privacy of most GSM phone conversations is currently protected by the 20+ years old A5/1 and A5/2 stream ciphers, which were repeatedly shown to be cryptographically weak.").

[12] *See supra* note 1, Part V.B.3.

[13] *See* Letter from Julius P. Knapp, Chief, Office of Eng'g & Tech., FCC, to author (Feb. 29, 2012), *available at* http://files.cloudprivacy.net/FOIA/FCC/fcc-stingray-reply.pdf ("[W]e are withholding certain intra-agency and interagency e-mails and documents because they are classified or because taken together with other information they could endanger national and homeland security.").

[14] *See* Nicole Perlroth, *Software Meant To Fight Crime Is Used To Spy on Dissidents*, N.Y. Times (Aug. 30, 2012), http://www.nytimes.com/2012/08/31/technology/finspy- software-is-tracking-political-dissidents.html (" …[T]he market for such technologies has grown to $5 billion a year from 'nothing 10 years ago,' said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show…").

[15] *See supra* note 6, Part V.A.

[16] Stefan Krempl, *28C3: New Attacks on GSM Mobiles and Security Measures Shown*, H OPEN (Dec. 28, 2011), http://www.h-online.com/open/news/item/28C3-New-attacks-on-GSM-mobiles-and-security-measures-shown-1401668.html (noting that Karsten Nohl of Security Research Labs reported, after a trip to the ISS trade fair, "that the bestselling items in the espionage community at present are devices for monitoring mobile phones, such as IMSI catchers").

II. Foreign Governments are Monitoring Cell Phone Calls in Washington, D.C., Including, Possibly, Those of Members and Staff

As President Obama has noted, "We know that the intelligence services of other countries. . . are constantly probing our government and private sector networks and accelerating programs to listen to our conversations."[17] The director of the National Security Agency has echoed this point. At a public event earlier this year, we asked Admiral Mike Rogers whether foreign governments are spying on cell phones in Washington. Admiral Rogers responded by confirming that "nation states around the world are attempting to generate insights as to what we are doing as individuals" and that the cellphones of government employees and policy makers are attractive targets.[18]

In their 2012 book *Deep State*, national security reporters Marc Ambinder and D.B. Grady revealed that "[t]he FBI has quietly removed from several Washington, D.C.-area cell phone towers, transmitters that fed all data to . . . foreign embassies."[19] When asked about the allegation by the Washington Post, the FBI declined to comment.[20] However, a former FBI deputy director told Newsweek in 2014 that "[t]his type of technology has been used in the past by foreign intelligence agencies here and abroad to target Americans, both [in the] U.S. government and corporations. There's no doubt in my mind that they're using it."[21] Moreover, in the fall of 2014, a team of technical experts revealed that they had detected, with sophisticated equipment, telltale signs of cellular surveillance devices in eighteen locations in the Washington D.C. area, including near the White House, Congress, and several foreign embassies.[22]

Although the NSA takes steps to protect the communications of the President and other senior national security officials, those officials are the exceptions, not the norm.[23] Most policy makers in government, including members of Congress and their staff, are not provided with the tools necessary to protect their communications from interception.[24]

---

[17] Barack Obama, President of the United States, Speech on NSA Reforms (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[18] *Admiral Mike Rodgers on Cellular Surveillance in Washington, D.C.*, C-SPAN (May 7, 2015), http://www.c-span.org/video/?c4536888/admiral-mike-rogers-cellular-surveillance-washington-dc.

[19] Marc Ambinder & D.B. Grady, *Deep States: Inside the Government Secrecy Industry* 245 (2013).

[20] *See supra* note 5.

[21] Jeff Stein, *New Eavesdropping Equipment Sucks All Data off Your Phone*, Newsweek (June 22, 2014), http://www.newsweek.com/2014/07/04/your-phone-just-got- sucked-255790.html.

[22] 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.

[23] Michael S. Schmidt & Eric Schmitt, *Obama's Portable Zone of Secrecy (Some Assembly Required)*, N.Y. Times (Nov. 10, 2013), http://www.nytimes.com/2013/11/10/us/politics/obamas-portable-zone-of-secrecy-some- assembly-required.html ("Countermeasures are taken on American soil as well. When cabinet secretaries and top national security officials take up their new jobs, the government retrofits their homes with special secure rooms for top-secret conversations and computer use.").

[24] *See* Letter from Tom Wheeler, Chairman, Fed. Commc's Comm'n, to Rep. Alan M. Grayson (Aug. 1, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0822/ DOC-328995A1.pdf (responding to inquiry by Rep. Grayson as to how Congress can protect their cellular communications from interception by encouraging Rep. Grayson and his colleagues in Congress to "utilize

III. Widespread Congressional Adoption of Encryption Offers a Way Forward

It is possible to deliver secure communications over an insecure network. In much the same way that Bank of America and Google can deliver their websites securely to customers using insecure public Wi-Fi networks,[25] so too can smartphone apps protect the audio and text communications of their users—by using strong encryption that provides security even when the underlying cellular network remains vulnerable to interception.[26]

In recent years, technology companies have added strong encryption to their products, which can protect communications from interception. Smartphone apps that encrypt voice, video, and text messages are widely available, and some of them are used by hundreds of millions of existing users.[27] These apps do not rely on the weak encryption provided by cellular networks for their security, but instead use modern, strong encryption to protect their customers' communications.[28]

One of the most widely respected encrypted communication apps, Signal, from Open Whisper Systems,[29] has received significant financial support from the U.S. government,[30] has been audited by independent security experts,[31] and is now widely used by computer security professionals,[32] many of the top national security journalists,[33]

---

resources the Commission has made available to educate and inform regarding communications goods and services," including "several consumer publications aimed at increasing consumer awareness of [interception] risks").

[25] *See* Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. Times, (Feb. 17, 2011), http://www.nytimes.com/ 2011/02/17/technology/personaltech/17basics.html ("The only sites that are safe from snoopers are those that employ the cryptographic protocol Transport Layer Security.").

[26] *See* Kashmir Hill, *You Can Now Call or Text Anyone With End-to-End Encryption, For Free*, Fusion (Mar. 2, 2015), http://fusion.net/story/56778/signal-encrypted-texts-calls/.

[27] Mikey Campbell, *Apple Sees 2 Billion iMessages Sent Daily from Half a Billion iOS Devices*, Apple Insider (Jan. 23, 2013), http://appleinsider.com/articles/13/01/23/apple- sees-2b-imessages-sent-every-day-from-half-a-billion-ios-devices; Derek Snyder, *Skype Passes 100M Android Installs and Launches Redesigned 4.0*, Skype Big Blog (July 1, 2013), http://blogs.skype.com/2013/07/01/skype-passes-100m-android-installs-and- launches-redesigned-4-0/; Daisuke Wakabayashi, *Cook Raises, Dashes Hopes for Excitement at Apple Annual Meeting*, Wall St. J. (Feb. 28, 2014), http://blogs.wsj.com/digits/ 2014/02/28/cook-raises-dashes-hopes-for-excitement-at-apple-annual-meeting/ ("Apple said it sends 'several billion' messages on its iMessage service every day. Apple said users also send 15 million to 20 million FaceTime messages every day.").

[28] Micah Lee, *You Should Really Consider Installing Signal, an Encrypted Messaging App for iPhone*, The Intercept (Mar. 2, 2015), https://firstlook.org/theintercept/2015/03/02/signal-iphones-encrypted-messaging-app-now-supports-text/.

[29] *See Open Whisper Systems*, https://whispersystems.org/ (last visited June 29, 2015).

[30] *See Open Technology Fund*, https://www.opentechfund.org/project/open-whisper-systems (last visited June 29, 2015) (showing Radio Free Asia's Open Technology Fund has provided more than $1.3 million in support to Open Whisper Systems).

[31] *See Secure Messaging Scorecard*, Elec. Frontier Found. (Mar. 5, 2015), https://www.eff.org/secure-messaging-scorecard (listing that Signal's code is open to independent review and that there has been a recent code audit).

[32] *See* Note 28.

and public interest advocates. Indeed, members of the ACLU's own legal department regularly use Signal to make encrypted telephone calls.

There are no significant barriers to providing members of Congress with encrypted communications tools. Many members of Congress and their staff already have smartphones.[34] Encrypted communications apps like Signal and WhatsApp are free and can be easily downloaded from the major app stores.[35] Similarly, Apple's encrypted voice, video, and text communications apps—FaceTime and iMessage—are built into Apple's mobile operating system and thus are already available to every member or staffer with an iPhone.[36]

These encrypted apps would be a significant improvement over the insecure, easy-to-intercept cellular phones that members and their staff currently use, and would make surveillance by foreign governments and others significantly more difficult.

In sum, we urge you to empower House and Senate offices to adopt secure communications equipment on their own, or to facilitate the adoption of secure equipment Congress-wide under your own initiative. As more government communications flow through unencrypted and insecure networks, the threat from foreign and domestic interception alike grows apace. Congress could take easy and cheap steps today to ameliorate that threat.

Although the civil liberties implications of this issue may not be obvious, they are important. Congress must be able to conduct its business in a secure fashion in the knowledge that communications—with constituents, other branches of government, the media, and among staff—are themselves secure. The OPM hack, and the experience of the Senate intelligence committee with the CIA's facilities, lay bare the need to better protect Congress's oversight function by guaranteeing the integrity of its communications.

---

[33] *See* Patrick Howell O'Neill, *How National Security Reporter Barton Gellman Protects His Sources*, The Daily Dot (Mar. 10, 2015), http://www.dailydot.com/politics/barton-gellman-security-encryption-anonymity/ (noting that Gellman's "preferred voice/text channel is Signal").

[34] *iPhone a Clear Favorite Among House Members*, NBC News (Sept. 22, 2015), http://www.nbcnews.com/news/other/iphone-clear-favorite-among-house-members-f4B11225782 (reporting that 58% of House members use an iPhone, 23% a Blackberry and 4% an Android).

[35] *See* Andy Greenberg, *WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users*, Wired (Nov. 18, 2014), http://www.wired.com/2014/11/whatsapp-encrypted-messaging/ ("describing the implementation of WhatsApp's new encryption scheme as "totally frictionless . . . . The result is practically uncrackable encryption for hundreds of millions of phones and tablets that have Whats[A]pp installed — by some measures the world's largest-ever implementation of this standard of encryption in a messaging service.").

[36] For example, since 2011, Apple's iOS operating system has used its own iMessage service for all text messages sent between iOS devices. Such text messages are, without requiring any configuration or special action by the user, encrypted and sent over the internet using Apple's servers, rather than using the wireless carrier's text message servers. *See* Andy Greenberg, *Apple Claims It Encrypts iMessages and Facetime so That Even It Can't Decipher Them*, Forbes (June 17, 2013), http://www.forbes.com/sites/andygreenberg/2013/06/17/apple-claims-it-encrypts-imessages-and-facetime-so-that-even-it-cant-read-them/.

We would be eager to answer any questions you have and to discuss any of the issues we describe in this letter with your staff. Please do not hesitate to contact Legislative Counsel Gabe Rottman at 202-675-2325 or grottman@aclu.org, with any questions.

Sincerely,

Michael W. Macleod-Ball
Chief of Staff

Gabe Rottman
Legislative Counsel and Policy Advisor

/S/ Christopher Soghoian
Christopher Soghoian, Ph.D.
Principal Technologist
Speech, Privacy, and Technology Project