ALAN GRAYSON
9TH DISTRICT, FLORIDA

COMMITTEE ON FOREIGN AFFAIRS
SUBCOMMITTEE ON WESTERN HEMISPHERE
SUBCOMMITTEE ON MIDDLE EAST AND NORTH AFRICA

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON ENERGY
SUBCOMMITTEE ON ENVIRONMENT
REGIONAL DEMOCRATIC WHIP

Congress of the United States
House of Representatives
Washington, DC 20515–0909

430 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225–9889

ORLANDO DISTRICT OFFICE
5842 SOUTH SEMORAN BOULEVARD
ORLANDO, FL 32822
(407) 615–8889

KISSIMMEE DISTRICT OFFICE
101 NORTH CHURCH STREET
SUITE 550
KISSIMMEE, FL 34731
(407) 518–4983

grayson.house.gov

July 2, 2014

673

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairman Wheeler,

I write to you today because I recently learned that the telephone calls of many Americans can be intercepted by criminals and foreign governments with widely available technology, which can be purchased for as little as $1800 from online retailers or built at home by hobbyists, and I want your information and views on this subject.

On June 22, Newsweek revealed the existence of "IMSI catcher" technology.[1] These devices impersonate a cell phone tower. They can be used to locate and identify nearby phones, as well as to intercept calls and text messages covertly. IMSI catchers can apparently "be bought openly"[2] from online retailers for as little as $1800.[3] According to a forthcoming article in the *Harvard Journal of Law and Technology*, referenced by Newsweek, hackers and hobbyists can make these devices themselves, using open source software.[4] According to the Newsweek article, a graduate student even demonstrated to some Congressional staffers in 2012 the ease with which phone calls can be intercepted with home-made technology.

Newsweek quotes former FBI deputy director Tim Murphy as stating that "This type of technology has been used in the past by foreign intelligence agencies here and abroad to target Americans, both U.S. government and corporations . . . . There's no doubt in my mind that they're using it." The article also quotes Mike Janke, a former Navy SEAL and covert communications expert, as stating that: "Defense firms in the Washington, D.C. area have found IMSI catchers attached to the light poles in their parking lots."

---

1 *See* Jeff Stein, New Eavesdropping Equipment Sucks All Data Off Your Phone, Newsweek, June 22, 2014, http://www.newsweek.com/your-phone-just-got-sucked-255790.

2 See Tom Brady, Bugging device linked to ombudsman inquiry 'can be bought openly,' The Independent (Ireland), June 10, 2014, http://www.independent.ie/irish-news/news/bugging-device-linked-to-ombudsman-inquiry-can-be-bought-openly-30340966.html

3 *See* Listing for IMSI Catcher at Alibaba.com, shipped from a company in Guangdong, China. http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html.

4 *See* Stephanie K. Pell and 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, Harvard Journal of Law and Technology, Forthcoming, draft available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678.

PRINTED ON RECYCLED PAPER

Apparently, experts have been warning about the weak security of US phone networks for some time. Last December, the *Washington Post* reported that "Encryption experts have complained for years that the most commonly used [cellular encryption algorithm], known as A5/1, is vulnerable and have urged providers to upgrade to newer systems that are much harder to crack."[5] According to the Harvard article referenced above, this encryption algorithm was created in the 1980s, was broken by Berkeley researchers in the 1990s, and is still widely used by US wireless carriers today.[6] Indeed, a working group within the FCC's Technological Advisory Council raised this very issue in a public presentation at the FCC in 2012, stating that the encryption used in "2G" networks is "widely broken," and that it is a "key threat to end user security."[7]

Americans have a reasonable expectation of privacy in their communications, and in information about where they go and with whom they communicate. It is extremely troubling to learn that cellular communications are so poorly secured, and that it is so easy to intercept calls and track people's phones.

Your predecessors Mignon Clyburn and Julius Genachowski both spoke in public about the FCC's role in protecting the privacy and security of Americans' communications. In 2013, then-FCC Acting Chair Clyburn stated that "protecting consumer privacy is a key component of [the FCC's] mission to serve the public interest."[8] Similarly, during Congressional testimony in 2010, Chairman Genachowski observed that the FCC had been directed by Congress to "protect the privacy of consumers who rely on our Nation's communications infrastructure."[9]

Given those statements, I am disturbed by reports which suggest that the FCC has long known about the vulnerabilities in our cellular communications networks exploited by IMSI catchers and other surveillance technologies. According to the Associated Press, the FCC issues licenses to American companies that manufacture such interception technology.[10]

I trust that your office will take my inquiry into this matter seriously, and that you will provide me with complete responses to all of my questions by July 15th, 2014.

Questions:

1. Does the FCC have any evidence that IMSI catchers and similar cellular interception technology have been used by private entities or foreign governments to spy on the public, companies, policy

---

5 *See* Craig Timberg and Ashkan Soltani, By cracking cellphone code, NSA has ability to decode private conversations, Washington Post, December 13, 2013, http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html.

6 *See* Pell and Soghoian at 49 ("Today, the A5/1 algorithm, created in 1988 and thoroughly broken a decade ago, remains the most widely deployed cellular encryption algorithm in the world. Indeed, wireless carriers AT&T and T-Mobile still use the A5/1 algorithm for their older '2G' networks in the United States.") (internal citations omitted)

7 Wireless Security and Privacy WG, Report to the TAC, Sept. 24, 2012, at 6, http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92412/TAC-9-24-12-Presentations.pdf.

8 *See* Statement of Acting Chairwoman Mignon Clyburn, Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0627/FCC-13-89A2.pdf.

9 *See* Statement of FCC Chairman Julius Genachowski, Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Science and Transportation, 111th Cong. (2010), available at http://www.gpo.gov/fdsys/pkg/CHRG-111shrg67686/html/CHRG-111shrg67686.htm.

10 *See* Jack Gillum and Eileen Sullivan, US Pushing Local Cops to Stay Mum on Surveillance, Associated Press, June 12, 2014, http://bigstory.ap.org/article/us-pushing-local-cops-stay-mum-surveillance

makers or Members of Congress?

2. Do the FCC's existing legal authority permit it to force the wireless carriers to upgrade the security of their networks in order to secure their subscribers' conversations from criminals, private parties or foreign governments using commercially available interception technology?

3. What steps, if any, has the FCC taken to require that wireless carriers upgrade their networks and the phones they sell to the American public to use up-to-date, secure encryption algorithms?

4. What steps, if any, has the FCC taken to inform the American public that its cellular communications can be intercepted by criminals, private parties, and foreign governments? If the FCC has not attempted to inform the public about these risks, why has it not done so?

5. What steps can Members of Congress and the American public take today to protect their cellular telephone calls and text messages from interception by criminals, private parties and foreign governments?

Thank you for your attention to this matter. If you have any questions or concerns, please contact my Senior Policy Advisor, Matt Stoller, at matt.stoller@mail.house.gov.

Sincerely,

Alan Grayson

ALAN GRAYSON
Member of Congress

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

August 1, 2014

The Honorable Alan M. Grayson
U.S. House of Representatives
430 Cannon House Office Building
Washington, D.C. 20515

Dear Congressman Grayson:

Thank you for your letter regarding the vulnerability of telephone calls to unlawful intercepts conducted by criminals and foreign governments. In your letter, you posed several questions about the vulnerabilities the illicit and unauthorized use of "IMSI catchers" and other surveillance technologies pose to the security of our cellular communications networks, as well as consumers' expectation of privacy. I appreciate your inquiry and welcome this opportunity to address your specific questions.

1. Does the FCC have any evidence that IMSI catchers and similar cellular interception technology have been used by private entities or foreign governments to spy on the public, companies, policy makers or Members of Congress?

Media reports of private, non-U.S. law enforcement entities or foreign governments using devices such as IMSI catchers to spy on law-abiding American citizens are of grave concern to me. Such uses are clearly illegal. We are not aware of any specific instances of private entities or foreign governments using these devices to intercept telephone calls. Because the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) serve as the expert agencies regarding federal criminal investigations and counterintelligence and possess the necessary enforcement authority and experience with IMSI catchers, I defer to their expertise on the extent to which private entities and foreign governments may be using IMSI catchers for espionage purposes.

2. Do the FCC's existing legal authority permit it to force the wireless carriers to upgrade the security of their networks in order to secure their subscribers' conversations from criminals, private parties or foreign governments using commercially available interception technology?

The FCC's responsibility to protect national security and to promote public safety and network security is fundamental, and our mandate is codified in the Communications Act. In particular, Title III of the Act charges the Commission with the responsibility to "maintain the control for the United States over all the channels of radio transmission" and to regulate the use and operation of any device that transmits signals by radio. In short, the FCC has the statutory authority to address the threat posed by illicit IMSI catchers and to work closely with industry on

mechanisms to secure our nation's wireless networks and to ensure the privacy of consumers' conversations. So long as I am Chairman, we will work diligently and strategically with all stakeholders to leverage the agency's expertise and fulfill these responsibilities.

Along these lines, I have recently established a task force to initiate immediate steps to combat the illicit and unauthorized use of IMSI catchers. The mission of this task force is to develop concrete solutions to protect the cellular network systemically from similar unlawful intrusions and interceptions. The task force can also leverage the agency's risk responsibility with our federal partners at DOJ, FBI, and DHS in order to clamp down on the unauthorized use of these devices and promote consumer privacy.

3. What steps, if any, has the FCC taken to require that wireless carriers upgrade their networks and the phones they sell to the American public to use up-to-date, secure encryption algorithms?

The Commission has worked closely with the National Institute of Standards and Technology (NIST) and industry bodies to develop cryptographic standards. We have further charged the Communications Security, Reliability, and Interoperability Council (CSRIC), an FCC federal advisory committee, with developing measurable, accountable, marketplace-driven cybersecurity risk management processes based on the NIST Cybersecurity Framework. This will include, as one of its elements, ensuring the security of data in transit. We also have been working to mitigate cyber threats through the industry's Cyber Security Working Group (CSWG). Through this collaborative partnership, consumers have been advised to keep their mobile devices' operating system (OS) and applications updated to the latest version. These updates often fix problems and possible cyber vulnerabilities associated with outdated technologies and security software.

4. What steps, if any, has the FCC taken to inform the American public that its cellular communications can be intercepted by criminals, private parties, and foreign governments? If the FCC has not attempted to inform the public about these risks, why has it not done so?

Through its ongoing mission to educate and inform consumers, the FCC has released several consumer publications aimed at increasing consumer awareness of the risks that may arise in using those goods and services, including a collection of consumer guides and publications addressing the issue of privacy and online security. For example, our guide on Mobile Wallet Services Protection provides helpful tips on how to safeguard smartphones, mobile wallet applications, associated data, and mobile wallet services. In addition, we have a guide on Interception and Divulgence of Radio Communications, which discusses provisions of the Communications Act that affect the manufacture of equipment used for listening to or receiving radio transmissions. The guide further notes that persons with concerns regarding the interception and divulgence of radio communications can file a complaint with the FCC. Lastly,

FCC staff frequently addresses privacy and cybersecurity issues regarding communications goods and services in its outreach and consumer education events.

5. What steps can Members of Congress and the American public take today to protect their cellular telephone calls and text messages from interception by criminals, private parties and foreign governments?

I would encourage you and your colleagues in Congress to utilize resources the Commission has made available to educate and inform regarding communications goods and services, as outlined above. Because the integrity of our nation's infrastructure and the privacy of consumers are under constant threat, the Commission remains vigilant in its efforts to update our consumer publications and take the necessary steps to safeguard our nation's communications in coordination with other federal agencies and the industry at large.

I appreciate your bringing these important public safety matters to my attention. Please let me know if I can be of any further assistance.

Sincerely,

Tom Wheeler