

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

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.

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.

Sincerely,



ALAN GRAYSON
Member of Congress