



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

**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu