

United States Senate

WASHINGTON, DC 20510

October 6, 2016

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

Dear Chairman Wheeler:

We write regarding recent reports about state and local law enforcement's use of "cell site simulators"—portable surveillance devices that collect cell phone identification and location information by mimicking cellphone towers. We are particularly concerned about allegations that cell site simulators—commonly referred to as "Stingrays"—disrupt cellular service and may interfere with calls for emergency assistance, and that the manner in which cell site simulators are used may disproportionately impact communities of color. While we appreciate law enforcement's need to locate and track dangerous suspects, the use of Stingray devices should not come at the expense of innocent Americans' privacy and safety, nor should law enforcement's use of the devices disrupt ordinary consumers' ability to communicate.

Recent complaints filed with the Federal Communications Commission (FCC) have alleged that state and local law enforcement agencies' use of Stingray devices violate the Communications Act.¹ Specifically, the complaints allege that cell site simulators' disruption of cell phones' ability to make and receive calls, possibly including calls to 911 and other emergency responders, constitutes "willful" interference with a communications network, which is prohibited by Section 333 of the Communications Act. The complaints further assert that state and local enforcement agencies do not possess the requisite licenses to operate Stingray devices over wireless spectrum—licenses required by Section 301 of the Communications Act. Reliable access to telecommunications services is vital to Americans' ability to communicate and successfully engage in today's economy, and it is the FCC's responsibility to ensure that communications services are available to Americans of all backgrounds.

We are also concerned by the complaints' assertion that cell site simulators are more frequently used in minority neighborhoods. Section 151 of the Communications Act tasks the FCC with the duty to ensure that people of the United States are able to access communications "without discrimination on the basis of race, color, religion, national origin, or sex." We have long been concerned that underlying inequities within our criminal justice system have a disproportionate impact on minority communities. Law enforcement practices that excessively subject communities of color to heightened and potentially unlawful government surveillance only exacerbate this concern. In this instance, there is also a possibility that the surveillance

¹ Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications, *In re Baltimore City Police Dep't, Baltimore, Md* (filed Aug. 16, 2016), <https://ecfsapi.fcc.gov/file/10816659216934/CS%20Simulators%20Complaint%20FINAL.pdf>; Memorandum in Support of Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications and Petition for an Enforcement Advisory on Use of Cell Site Simulators by State and Local Government Agencies, *In re Baltimore City Police Dep't, Baltimore, Md* (filed Sept. 1, 2016), https://www.aclu.org/sites/default/files/field_document/aclu-eff_fcc_cell_site_simulator_filing.pdf.

technology may more frequently interfere, however inadvertently, with the ability of minority communities to use wireless communications and emergency services. Such interference raises additional questions where federal funding appears to have supported the acquisition of this technology by state and local law enforcement.² We urge the FCC to investigate and, if necessary, address the charges in the referenced complaints. In addition, we urge that the findings of such an investigation be made public.

Finally, we write to request additional information about the FCC's role in overseeing the use of cell site simulators. The *Washington Post* recently reported some confusion within the agency regarding how the devices operate. According to the *Post* article, an FCC official indicated that cell site simulators do not transmit signals on the wireless spectrum—a statement directly at odds with Department of Justice documentation on the devices.³ In an effort to gain a better understanding of how Stingrays may be interfering with consumers' ability to communicate, we respectfully request that you respond to the following questions:

1. Do cell site simulators, including but not limited to the Stingray and HailStorm models, transmit over frequencies licensed to cellular phone carriers? What is the power and range of these devices' transmissions?
2. Does the Communications Act require that law enforcement agencies obtain licenses from the FCC to transmit over licensed spectrum, and refrain from causing harmful interference? Please provide any examples of devices for which law enforcement has acquired a license in order to transmit over licensed spectrum. Are such agencies required to coordinate with the spectrum holder in any way?
3. For devices that do require a license in order to transmit over licensed spectrum, what steps can the FCC take to hold users accountable for operating the devices without the appropriate license? What procedures are currently in place to verify that users have acquired the appropriate license prior to using a device? If the FCC does not currently

² See Memorandum from Detective Jeffrey Shipp, Tacoma Police Department to Kathy Katterhagen, Procurement and Payables Manager, City of Tacoma (Mar. 3, 2013), <https://www.documentcloud.org/documents/1280700-unredacted-purchmemo-hailstorm.html> (explaining that the Tacoma Police Department acquired cell site simulator technology in 2007 using a DOJ Law Enforcement Grant award, and that in 2013 the Department received a Department of Homeland Security Port Security Grant in order to update its existing cell site simulator technology); Letter from William J. Quinlan, General Counsel, Office of the Illinois Governor, to Larry G. Trent, Director, Illinois State Police (Mar. 18, 2008), https://muckrock.s3.amazonaws.com/foia_files/14-0754_Docs.pdf at 7 (stating that funding for Illinois State Police's purchase of cell site simulator technology "is provided by the Homeland Security Grant").

³ Ellen Nakashima, *Civil Liberties Groups Ask FCC to Probe Baltimore Police Use of Cellphone Tracking Devices*, WASH. POST (Aug. 16, 2016), https://www.washingtonpost.com/world/national-security/civil-liberties-groups-ask-fcc-to-probe-baltimore-police-use-of-cell-phone-tracking-devices/2016/08/16/37002b76-6336-11e6-96c0-37533479f3f5_story.html ("The official, who spoke on the condition of anonymity because she was not authorized to talk on the record, said at one point that the devices do not transmit on the wireless spectrum—which experts dispute."); *contra* U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY, <https://www.justice.gov/opa/file/767321/download> ("Cell-site simulators, as governed by this policy, function by transmitting as a cell tower.").

have such procedures in place, when will the agency develop oversight procedures and what will these procedures consist of?

4. Are cell site simulators capable of disrupting cellular communications in their vicinity? To the extent that the answer is yes, how large is the area of interference, and does the interference extend to 911 calls, or calls to police, hospitals, or public safety hotlines?
5. As part of the equipment authorization process for cell site simulators, has the FCC determined that cell site simulators do not cause harmful interference? When was the last time a cell site simulator went through the equipment authorization process?
6. Including any testing that may have been conducted in the equipment authorization process, has the FCC ever tested cell site simulators in a real world setting to determine whether the devices disrupt a cell phone's ability to make or receive calls? If so, when?
7. Does the FCC maintain a record of which state and local law enforcement agencies possess cell site simulators, how many each department has, and when, where, and for how long the devices are used?
8. Does the FCC have any knowledge of whether state and local police departments take steps to ensure cell site simulators are used in a way that minimizes network interference, protects emergency calling, and does not disproportionately harm communities of color?
9. What is the current status of the task force that the FCC established in 2014 to study reported misuse of surveillance technology?⁴ How often has this task force met? Please provide us with the results of any studies it has undertaken as well as a description of its actions to combat misuse of surveillance technologies.
10. The equipment authorization granted to the manufacturer of Stingrays requires states and localities to "advance coordinate" with the FBI before acquiring or using cell site simulator equipment.⁵ Publicly available documents indicate that the FBI implements this coordination requirement by requiring state and local agencies to sign a non-disclosure agreement with the FBI. For example, one letter from the FBI to a local law enforcement agency states, "[c]onsistent with the conditions of the equipment authorization granted to

⁴ Letter from Chairman Wheeler, FCC to U.S. Rep. Alan Grayson (Aug. 1, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-328995A1.pdf ("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.").

⁵ See, e.g., FCC, Grant of Equipment Authorization, Harris Corporation, FCC Identifier NK73166210 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=S02SFOCotzKlbdYCDPFIIA%3D%3D&fcc_id=NK73166210; FCC, Grant of Equipment Authorization, Harris Corporation, FCC Identifier NK73092523 (Apr. 19, 2011), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=9nDFvP9N200RJUhSYM6ASQ%3D%3D&fcc_id=NK73092523.

[the manufacturer] by the [FCC], state and local law enforcement agencies must coordinate with the [FBI] to complete [a] non-disclosure agreement.”⁶

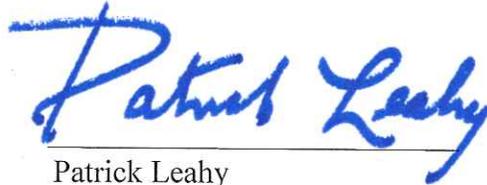
- a. Did the FCC intend for its equipment authorizations for cell site simulators to require that state and local law enforcement officials sign non-disclosure agreements? If so, please explain why the grant of an equipment authorization is conditioned on compliance with a non-disclosure agreement.
- b. Has the FCC communicated with the FBI about the terms of non-disclosure agreements as they relate to equipment authorizations? Has the FCC communicated with the FBI or any other law enforcement agency about taking steps to minimize network interference and protect calls to emergency services while operating cell site simulators?

As always, thank you for your consideration of our request, and we look forward to working with you to protect Americans’ privacy and safety.

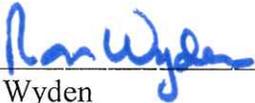
Sincerely,



Al Franken
United States Senator



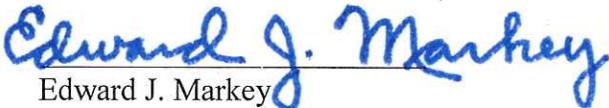
Patrick Leahy
United States Senator



Ron Wyden
United States Senator



Sherrod Brown
United States Senator



Edward J. Markey
United States Senator



Elizabeth Warren
United States Senator

⁶ FBI Non-Disclosure Agreement (June 29, 2012), available at <http://www.nyclu.org/files/releases/Non-Disclosure-Agreement.pdf>.



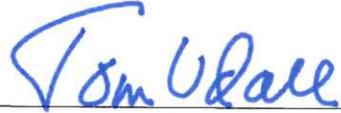
Jeffrey A. Merkley
United States Senator



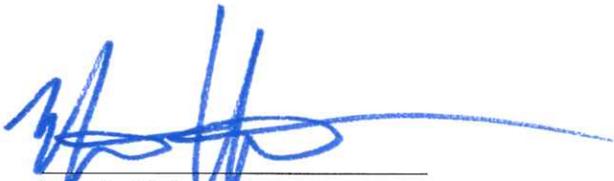
Tammy Baldwin
United States Senator



Bernard Sanders
United States Senator



Tom Udall
United States Senator



Martin Heinrich
United States Senator



Christopher A. Coons
United States Senator