epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 27, 2018

The Honorable Ralph Abraham, Chairman
The Honorable Don Beyer, Ranking Member
House Committee on Science, Space, and Technology
Subcommittee on Oversight
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Abraham and Ranking Member Beyer:

We write to you before the hearing "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats."[1] In a landmark ruling last week, the U.S. Supreme Court held that the Fourth Amendment protects location records generated by mobile phones.[2] As a consequence, Congress should update privacy law to address the challenges of devices such as Stingrays. StingRays, with their ability to discretely collect vast troves of non-target, non-pertinent data should clearly be subject to the heightened Title III warrant requirement for communications interception.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC has a particular interest in the impact of new surveillance technologies with the capacity to enable warrantless, pervasive mass surveillance of the public by law enforcement agents. EPIC has long promoted oversight of IMSI Catchers, or "StingRays," by law enforcement agencies. An EPIC FOIA lawsuit in 2012 revealed that the FBI was using StingRays without a warrant, and that the FBI provided StingRays to other law enforcement agencies.[4] EPIC has also filed amicus briefs in federal and states courts arguing that cell phone location data is protected by the Fourth Amendment.[5]

A StingRay is a device that can triangulate the source of a cellular signal by acting "like a fake cell phone tower" and measuring the signal strength of an identified device from several locations. With StingRays and other similar "cell site simulator" technologies, Government

---

[1] *Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats*, 115th Cong. (2018), H. Comm. on Science, Space, & Technology, Subcomm. on Oversight (June 27, 2018), https://science.house.gov/legislation/hearings/subcommittee-oversight-hearing-bolstering-data-privacy-and-mobile-security.
[2] *Carpenter v. United States*, 585 US _ (2018).
[3] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *EPIC v. FBI,* No. 12-667 (D.D.C. Mar. 28, 2013); *See generally* https://epic.org/foia/fbi/stingray/.
[5] *See e.g.* Brief of Amici Curiae EPIC et. al,, *Carpenter v. United States*, 585 US _ (2018) (arguing that the Fourth Amendment protects the right against warrantless seizure and search of location data), *available at* https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.

investigators and private individuals can locate, interfere with, and even intercept communications from cell phones and other wireless devices. the use of cell site simulator technology implicates not only the privacy of the targets of investigation, it also affects other innocent users near the technology. And their abilities go far beyond location tracking, including the ability to intercept, redirect, spoof, otherwise modify the content of calls.

After EPIC's 2012 FOIA lawsuit, the Justice Department released new guidelines that require the Department's law enforcement components to obtain a warrant before using Stingrays.[7] The policy prohibits officers from using Stingrays to intercept communications, and requires that all non-target data be deleted after use. And last year, a federal court ruled that warrantless use of a stingray violates the Fourth Amendment.[8]

Because StingRays can (1) collect data about all devices in an area, (2) enable ongoing monitoring and massive data collection absent clear limits, and (3) potentially interfere with legitimate signals, including emergency calls, the use of these devices by law enforcement should be subject to the same heightened "super warrant" requirement placed on Wiretap Orders since Congress passed Title III in 1968.

We ask that this Statement from EPIC be entered in the hearing record. We look forward to working with you on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Alan Butler*
Alan Butler
EPIC Senior Counsel

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

[7] *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, Dept. of Justice (2015), *available at* https://www.justice.gov/opa/file/767321/download.
[8] *Jones v. U.S.*, 168 A.3d 703 (D.C. App. 2017).