March 16, 2016

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

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Chairman & Ms. Brown Lee:

The undersigned 45 civil rights, public policy, and public interest organizations write to express our shared concerns about International Mobile Subscriber Identity (IMSI) catchers, also referred to as Cell-Site Simulators or "Stingray" devices ("Stingrays").[1] Reports surfaced last month that the New York Police Department has used Stingrays extensively–without warrants and without policies in place guiding how police can use the devices.[2] This news follows on the heels of numerous allegations over the past several months that law enforcement agencies have improperly used Stingrays to spy on lawful protesters; routinely deployed Stingrays without a warrant and in violation of the Fourth Amendment; and failed to adopt adequate procedures to protect privacy and civil liberties.[3]

In light of these developments, we urge you to investigate the continued and largely unregulated use of Stingrays by law enforcement officials, to remedy the lack of data and transparency about these devices, and to act swiftly to prevent the disproportionate harms that the use of these devices by law enforcement officials can pose to historically disadvantaged communities.

Stingrays are powerful surveillance technologies that mimic cell towers in order to indiscriminately intercept all cellular signals in an area, thus enabling users to gather serial

[1] Widespread sale and operation of IMSI devices are reflected in the number of manufacturers producing the product and the numerous trade names for these companies' product offerings. Cell-tower simulation technologies from Harris Corporation are marketed and sold as TriggerFish, Stingray, Stingray II, AmberJack, HailStorm, Kingfish, and Loggerhead. Martone Radio Technology offers similar products under the following trade names: Max-G, Max-W, Spartacus, and Spartacus-II products. And Cellxion offers similar products under the following trade names: Optima, Quadra, UGX-300, GX-200, GX-Duo, and GX-Solo. *See, e.g., American Civil Liberties Union of Northern California on the Request for Inspection of Records*, Memorandum Opinion and Order, 29 FCC Rcd 9724, n. 3 (2014) ("*ACLU MO&O*"), *available at* http://bit.ly/1RqBmlw.

[2] Ciara McCarthy, *NYPD tracked citizens' cellphones 1,000 times since 2008 without warrants*, The Guardian (Feb. 11, 2016), *available at* http://bit.ly/23ZQPR3.

[3] Mike Krauser, *Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests*, CBS Chicago (Dec. 6, 2014), *available at* http://cbsloc.al/1Byvth4; *see also* The Free Press Thought Project, *Chicago Cops Used Stingray to Intercept Protester's Conversations* (Dec. 7, 2014), *available at* http://bit.ly/1vsJILZ; Daniel Rivero, *Florida Cops Have Tracked Protesters, Suicidal People, and Robbers with Stingray Devices*, Fusion (Feb. 25, 2015), *available at* http://fus.in/1KFQb4D.

numbers and location information, as well as to identify individual phones.[4] Information about Stingray devices' use and functions has been routinely withheld from courts and the public,[5] and the numerous privacy and legal concerns raised by these devices have already received significant attention in national media and other outlets.

We wish to highlight another serious concern: when used by law enforcement, Stingrays and other surveillance technologies do not affect all Americans equally.

Stingrays Have a Disproportionate Impact on Historically Disadvantaged Communities

Law enforcement agencies have long exercised their power disproportionately in communities of color, and this imbalance persists today. People of color are much more likely to be stopped and searched, with 95% of police departments across the country reporting that they are likely to stop African-Americans at a higher rate than others, even though officers are equally likely to identify something as being of interest regardless of race.[6] A *USA Today* study found that at least 70 police departments across the country arrested African-Americans at a rate ten times higher than other racial groups.[7] And more than 60 percent of the people in prison are now racial and ethnic minorities. Among African-American men in their thirties, one in ten is in prison or jail.[8]

New technological tools that amplify police power can amplify existing biases in policing. Lack of effective oversight and supervision by the regulatory authorities in the use of this technology may lead to even greater invasions of privacy and subversions of rights in communities of color that are already the targets of biased policing.[9] Given these documented biases, the use of a

---

[4] Craig Timberg, *Feds to Study Illegal Use of Spy Gear*, Wash. Post (Aug. 11, 2014), *available at* http://wapo.st/1K08eeK; *see also* Cyrus Farivar, *FCC to Examine "Unauthorized" Cell Snooping Devices,* Ars Technica (Aug. 12, 2014), *available at* http://bit.ly/1l8bKhS. Some models also have the capability to eavesdrop on calls and send malicious software.

[5] Non-disclosure agreements between law enforcement agencies and manufacturers has led to the withholding of information about Stingray devices to judges and defendants, including for the purposes of obtaining a warrant. *See* Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, Wired (Mar. 4, 2014), *available at* http://bit.ly/1ToqHvF. Numerous other cases have revealed information about the devices withheld from defendants, prosecutors, and judges, despite widespread use. *See* Jennifer Valentino-Devries, *Judge Questions Tools That Grab Cellphone Data on Innocent People, Wall Street Journal*, Wall Street Journal (Oct. 12, 2012), *available at* http://on.wsj.com/1mFHPP9; *see also* Justin Fenton, *Baltimore Police used secret technology to track cellphones in thousands of cases,* The Baltimore Sun (Apr. 9, 2015), *available at* http://bsun.md/1GS5MJO.

[6] Matthew R. Durose, *et al.*, U.S. Department of Justice, *Recidivism of Prisoners Released in 30 States in 2005: Patterns from 2005 to 2010* (April 2014), *available at* http://1.usa.gov/1lvWsR7.

[7] Brad Heath, *Racial Gap in U.S. Arrest Rates: 'Staggering Disparity'*, USA Today (Nov. 19, 2014), *available at* http://usat.ly/1u8ETXA.

[8] The Sentencing Project, *Racial Disparity, available at* http://bit.ly/1jERtxX (last visited Oct. 16, 2015).

[9] For example, a few years ago the New York Police Department admitted that it had installed surveillance cameras and used unmarked cars outfitted with electronic license plate readers to target Muslims near mosques. Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012), *available at* http://bit.ly/TPeUdp. Other police technologies also have reportedly been used disproportionately in communities of color. *See, e.g.,* Jeremy Gillula & Dave Maass, EFF, *What You Can Learn from Oakland's Raw ALPR Data* (Jan. 21, 2015), http://bit.ly/1BIowul.

powerful surveillance technology like Stingrays—particularly in secret and with little oversight—threatens African Americans, Latinos, Asians and other persons of color with disproportionate harm to their privacy, security, and basic civil rights as Americans.

And as grave as the privacy and civil rights concerns about the indiscriminate use of these data-collection devices are, Stingrays can pose an even more immediate threat: the devices have been known to disrupt and disable lawful mobile communications, including the ability of bystanders to communicate with police, fire and medical service personnel in an emergency.[10]

The FCC and DOJ Should Be Committed to Improving Stingray Oversight

With people's lives and liberties at risk, the FCC established a task force in 2014 to focus on the use of Stingray devices by "criminals" and "foreign intelligence services."[11] But an inquiry into curbing the misuse of Stingrays must not stop there. Rather, the task force must address their broad use by federal, state, and local law enforcement agencies, recognizing that law enforcement use of Stingrays, like other police tactics and surveillance technologies, may well have a disparate impact on already marginalized groups.

In addition, last year the Department of Justice released new guidance for federal agencies wishing to deploy Stingray devices. While this guidance includes important protections like a warrant requirement for Stingrays and minimization procedures to prevent unlawful retention of data on innocent bystanders, it only applies to DOJ components and federal, state, and local agencies when they partner with the DOJ.[12] In addition to New York City, Stingrays have been used in Sacramento, California; Tacoma, Washington; Baltimore, Chicago, and likely many other localities that citizens still don't know about.[13] Therefore, the DOJ must take further steps to ensure that all states and localities that deploy Stingrays do so in a way that is transparent, accountable, and consistent with the constitution, and encourage other agencies to put policies in place to minimize harm to historically disadvantaged communities. They could do this by ending the FBI's practice of requiring state and local law enforcement agencies to sign nondisclosure agreements for Stingrays and could link the agency's technology funding to a mandate that state and local agencies comply with the DOJ's Stingray guidance.

---

[10] Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, Wired (Mar. 1, 2014), *available at* http://wrd.cm/1K5Aa76.

[11] The task force was created in response to Rep. Alan Grayson's (D-FL) letter on stingrays. See letter from the Chairman Tom Wheeler to Congressman Grayson (Aug. 1, 2014), Federal Communicatons Commission, *available at* http://bit.ly/1XzWIQN.

[12] This federal guidance notably fails to address the lack of notice given the individuals affected by Stingray surveillance. *See* ACLU, *Letter for the Record to the House Committee On Oversight Subcommittee On Information Technology, Hearing On "Examining Law Enforcement Use Of Cell Phone Tracking Devices"* (Oct. 20, 2015), *available at* http://bit.ly/1Wi05KE.

[13] See ACLU, *Stingray Tracking Devices: Who's Got Them?* (last visited Feb. 16, 2016), *available at* http://bit.ly/1OxKmWG.

FCC and DOJ Stingray Inquiries Must Consider and Address Impact on Historically Disadvantaged Communities

The use of Stingrays and similar surveillance technologies could have a disproportionate and negative impact on communities of color. As the FCC and DOJ work to ensure the lawful and targeted use of Stingray technology, and consistent with your agencies' authorities and our shared interest in ensuring that police technologies are used to promote justice without unduly infringing on civil rights, we urge you to explore ways to ways to curb disparate impact on historically disadvantaged communities. We also urge your agencies to follow their respective missions in these regards, to denounce racial profiling in police technology, to restrict all law enforcement uses of Stingrays to cases where a warrant is obtained,[14] and to promote policies that ensure Stingrays are adopted and deployed if at all in a way that is transparent and accountable to the public.

Sincerely,

18MillionRising.org
Allied Media Projects
Alvaro Bedoya, Center on Privacy & Technology at Georgetown Law
Appleshop
Black Alliance for Just Immigration
Black Lives Matter Bay Area
Black Movement Law Project
Center for Community Change Action
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Champaign-Urbana Citizens for Peace and Justice
ColorOfChange
Common Frequency
Concerned Citizens for Justice
Courage Campaign
CREDO
Deep Dish TV
Demand Progress
Electronic Frontier Foundation
Ella Baker Center for Human Rights

[14] Although the Department of Justice now has a policy of requesting a warrant before using an IMSI catcher, this policy has exceptions, in addition to applying only to the FBI and other Justice Department agencies. Ellen Nakashima, *Justice Department: Agencies Need Warrants to Use Cellphone Trackers*, Wash. Post (Sept. 3, 2015), *available at* http://wapo.st/1LYiAmc.

Fight for the Future
Free Press
Generation Justice
Instituto de Educacion Popular del Sur de California
Media Action Grassroots Network
Media Alliance
Media Mobilizing Project
Million Hoodies Movement for Justice
Moms Rising
Move Food
Movement Strategy Center
NAACP
National Council of La Raza
National Hispanic Media Coalition
New America's Open Technology Institute
Presente.org
Public Knowledge
Restaurant Opportunity Center
Silicon Valley De-Bug
St. Paul Neighborhood Network
The Ruckus Society
Urbana-Champaign Independent Media Center
Voices for Racial Justice
Working Narratives