Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of

Baltimore City Police Department
Baltimore, Maryland

Complaint for Relief Against
Unauthorized Radio Operation and
Willful Interference with Cellular
Communications

Petition for an Enforcement Advisory
on Use of Cell Site Simulators by State
and Local Government Agencies

COMPLAINT FOR RELIEF AGAINST UNAUTHORIZED RADIO OPERATION AND WILLFUL INTERFERENCE WITH CELLULAR COMMUNICATIONS

PETITION FOR AN ENFORCEMENT ADVISORY ON USE OF CELL SITE SIMULATORS BY STATE AND LOCAL GOVERNMENT AGENCIES

Submitted by

Center for Media Justice

Color Of Change

New America's Open Technology Institute

Laura M. Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9547

Counsel for Complainants

August 16, 2016

Table of Contents

The Center for Media Justice, Color Of Change, and the Open Technology Institute at New America (collectively, "Complainants") respectfully petition the Federal Communications Commission ("Commission" or "FCC") under 47 C.F.R. § 1.41 to enforce Sections 301 and 333 of the Communications Act and Section 1.903 of the Commission's rules against the Baltimore City Police Department ("BPD"). Through its use of cell site simulators ("CS simulators"), BPD operates cellular transceivers without proper authorization, causes willful interference with the cellular network, disrupts emergency calling services, and inhibits the availability of the cellular network on a racially discriminatory basis.

Summary and Background

CS simulators are powerful, invasive, and harmful surveillance devices. CS simulators intentionally interfere with the normal exchange between cellphones and the cellular network by transmitting a signal over frequencies reserved for cellular use, impersonating a legitimate cellular tower, and forcing cellphones in the area to connect to them. This enables law enforcement agents who use the devices to catalog all cellphones within range of their CS simulator equipment, based on the unique network identifiers that cellphones share with cell towers when they establish a new connection. Law enforcement agents further use CS simulators to track down the precise location of cellphones known to be of interest in a case or investigation, using signal strength as a guide.

BPD is known to be in possession of CS simulator equipment. And it makes exceptionally heavy use of the equipment—BPD may even make greater use of its CS simulator equipment than any other city, state, or local law enforcement agency in the country. BPD uses the equipment not only to investigate violent crimes of the most troubling nature, but also to investigate everyday street crimes, to locate witnesses, and for other unspecified purposes.

This widespread use is obscured from the public. Some information about BPD's use of CS simulators has come to light through the efforts of journalists

and disclosures made before courts and legislators, but the BPD makes every effort to conceal its use of the devices. BPD has not released any information at all about thousands of undocumented deployments, and has no written policy governing its use of CS simulator equipment for the public to inspect.

CS simulator equipment is harmful to the residents of Baltimore. CS simulators mimic cell towers to force nearby cellphones to connect to them, but because they are not real cell towers and are not actually connected to the phone network, CS simulators then preclude phones connected to them from completing calls. This interference with calls extends to emergency calls. In this way, these devices disrupt the cellular telephone network and emergency services. Like other law enforcement surveillance equipment, CS simulators also chill speech, including the speech of protestors focusing scrutiny on BPD.

Worse, the harms that stem from BPD's use of CS simulator equipment fall disproportionately on Baltimore's Black residents. BPD is most aggressive in Black neighborhoods; indeed, according to a recently released report from the Department of Justice BPD clearly exercises its enforcement authority in a way that is statistically heavily biased against African Americans. Where BPD focuses its policing power, it also focuses its surveillance technology—including CS simulator equipment—and residents in targeted neighborhoods therefore suffer disproportionate harms.

BPD's operation of CS simulator equipment is not only harmful, but unlawful. Under the Communications Act, to operate a cellular transceiver on licensed spectrum reserved for operation of cellular networks, BPD is required by federal law to obtain a license. But in a clear violation of law, BPD has no license whatsoever to operate its CS simulator equipment on frequency bands that are exclusively licensed to cellular phone carriers in Baltimore.

BPD further violates the Communications Act by willfully interfering with the cellular network through its use of CS simulator equipment. The core function of CS simulators is to interfere with the network by impersonating

cellular towers and superseding the legitimate cellular towers with which cellphones would remain connected in the absence of CS simulator activity. BPD agents have received training on this equipment and on the functioning of the cellular network, understand that CS simulator operation causes harmful interference to the cellular network, and willfully cause that interference anyway.

As the statutorily mandated custodian of the public airwaves on which the public relies, the FCC must act to address harms caused by BPD's unauthorized use of CS simulators. The FCC has legal obligations to protect against harmful interference caused by unauthorized transmissions on licensed spectrum, to manage spectrum to promote the safety of life and property, to ensure availability of emergency calling services, and to strive to make communications networks available to the public without discrimination on the basis of race, color, religion, national origin, or sex.

In addition, the Commission made a commitment to Congress and the public to address illicit and unauthorized use of CS simulator equipment. Over two years have passed since Chairman Wheeler made that commitment and established a task force to "initiate immediate steps" to address the issue, and in that time the FCC has made no progress.

The Commission should protect the public from harms caused by CS simulators by bringing an enforcement action against BPD for its unauthorized use of licensed spectrum and harmful interference with cellular communications, and by issuing an enforcement advisory advising law enforcement agencies around the country that they must abide by the laws that protect wireless spectrum and emergency services from harmful interference. The public is relying on the Commission to carry out its statutory obligation to do so, to fulfill its public commitment to do so, and to put an end to widespread network interference caused by rampant unlicensed transmissions made by BPD and other departments around the country.

Interest of Complainants

The Center for Media Justice ("CMJ") was launched in 2008 to organize the most under-represented communities into a national movement for media rights, access, and representation. CMJ has its roots in the Youth Media Council ("YMC"), launched in 2002 to counter dangerous media stereotypes about California's youth of color in the news. As YMC grew, so did its analysis and approach. Within three years and with support the Movement Strategy Center, YMC expanded to a national scope, organizing a broad base of diverse social justice groups by co-founding the Media Action Grassroots Network ("MAG-Net"). In 2008, YMC staff launched CMJ. Today, CMJ coordinates MAG-Net—the largest racial justice network for media rights, access, and representation in the United States, and remains a powerful network hub winning racial equity through media policy change. MAG-Net organizes a national membership of affiliate groups, mobilizes and supports media justice campaigns, and strengthens the power of social justice movements to win the media representation they deserve through research, training, and strategic convening.

Color Of Change exists to strengthen Black America's political voice. Its goal is to empower its members—Black Americans and their allies—to make government more responsive to the concerns of Black Americans and to bring about positive political and social change for everyone. Color Of Change is comprised of Black folks from every economic class, as well as allies of every color who seek to help Black voices be heard. Its members are united behind a simple, powerful pledge: to do all they can to make sure all Americans are represented, served, and protected—regardless of race or class.

New America's Open Technology Institute works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. It promotes universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Argument

I. Baltimore City Police Department uses cell site simulators on licensed spectrum without a license

The BPD uses CS simulators to locate and track cell phones in their area on a regular basis. BPD does this over licensed spectrum, without authorization to use that spectrum.

A. Baltimore City Police Department makes frequent use of cell site simulators

There is no question that BPD is in possession of and makes frequent use of CS simulators. BPD has been in possession of CS simulator equipment since at least 2007.[1] The department's current CS simulator equipment includes at least one HailStorm device sold by Harris Corporation, as indicated by a $99,786 contract that was approved by the city's Board of Estimates in January 2013.[2] As described by Detective John Haley of the Advanced Technical Team ("ATT") in a Maryland Court,[3] HailStorm is newer generation technology than the commonly known StingRay made by the same company.[4] Not much is known to the public about HailStorm, but it appears to be Harris's CS simulator technology for LTE

---

[1] *See* Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, Baltimore Sun (Apr. 9, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[2] *See* City of Baltimore, Board of Estimates Agenda, Jan. 23, 2013, at 51, available at http://www.baltimorecitycouncil.com/BOE/BOEAgenda01-23-13FULL.pdf.

[3] June 4, 2015 Transcript at 47, *Maryland v. Andrews*, 227 Md. App. 350 (Mar. 30, 2016).

[4] *Id.* at 48.

networks.[5] HailStorm can be purchased as a standalone unit or as an upgrade to existing StingRay hardware.[6] Based on a bid solicitation also from January 2013, it seems BPD's HailStorm purchase was an upgrade to a StingRay II already in BPD's possession at that time.[7]

Available information indicates that BPD may well use CS simulator equipment more expansively than any other police department in the country, as statements from its own representatives suggest. For example, in April 2015, Detective Emmanuel Cabreja, also of BPD's ATT, testified in court that BPD had used the technology 4,300 times since 2007.[8] That's an average of 516 uses per year, or more than once per day. Cabreja alone used a CS simulator device 600 to 800 times in less than two years as a member of the unit, he told the court.[9] In March 2016, BPD Lieutenant Michael Fries told lawmakers in Annapolis, "Obviously, we probably use the [CS simulator] equipment more than anybody, in total."[10]

---

[5] *See Deciphering the Harris Hailstorm IMSI Catcher: All About LTE*, Insider Surveillance (Jun. 2, 2016), https://insidersurveillance.com/deciphering-harris-hailstorm-imsi-catcher-lte/.

[6] *Id*.

[7] *See* Bid Solicitation: B50002783, *available at* https://assets.documentcloud.org/documents/1280841/bid-document-375313665.pdf.

[8] Fenton, *supra* note 1; *see* YouTube, *Baltimore Police Address 'Operation Stingray,' ABC 2 News – WMAR*, at 1:00, *available at* https://www.youtube.com/watch?v=zX4GhFvhRzw; Justin Fenton, *Baltimore Judge Allows Police Use of Stingray Phone Tracking in Murder Case*, Baltimore Sun (Apr. 20, 2015), http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-new-disclosures-20150420-story.html.

[9] Fenton, *supra* note 1.

[10] March 10, 2016 Hearing before Maryland State Senate at 59:55, *available at* http://mgahouse.maryland.gov/mga/play/462e6ce5-f28b-4103-9a0d-a79ff4e226da/?catalog/03e481c7-8a42-4438-a7da-93ff74bdaa4c&playfrom=728000.

Indeed, BPD uses CS simulator equipment more than any other police department for which there is sufficient information publicly available to make a comparison—including in cities with populations that greatly exceed Baltimore's estimated 621,849 residents.[11] For example, police in Boston (est. population 667,137) used the technology 11 times in 7 years,[12] police in San Diego (est. population 1,394,928) used it "at least 30 times" in 5.5 years,[13] and police in New York City (est. population 8,550,405) used it approximately 1,016 times in 7.5 years.[14]

BPD's use of CS simulators is as widespread as it is because BPD does not limit its use of CS simulators to exceptional cases. Speaking at a press conference in 2015, BPD Captain Eric Kowalczyk said the department uses CS simulators to find "violent criminals causing violent action in our city."[15] But in contrast with that assertion, news reports indicate BPD routinely and indiscriminately uses the devices to investigate run-of-the-mill street crimes involving non-violent offenders. Writing for *USA Today*, investigative reporter Brad Heath found, "In

---

[11] U.S. Census Bureau, *American FactFinder*, http://factfinder.census.gov/faces/nav/jsf/pages/index.xhtml.

[12] Shawn Musgrave, *Police Use of Cellphone Tracking Devices Raises Questions*, Boston Globe (Jul. 27, 2016), https://www.bostonglobe.com/metro/2016/07/26/boston-police-use-cellphone-tracking-devices-without-warrants-raises-questions/r98oKPmI6XP3a2tPDxB9BO/story.html.

[13] *See* Greg Moran, *Records Show How Often SDPD Uses Its Stingray*, San Diego Union-Tribune (Aug. 8, 2016), http://www.sandiegouniontribune.com/news/2016/jul/31/san-diego-police-surveillancecell-phone-stingray/ ("San Diego police have used a controversial surveillance tool that can locate an individual cell phone by mimicking a cellphone tower at least 30 times since 2011.").

[14] *See NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, NYCLU (Feb. 11, 2016), http://www.nyclu.org/news/nypd-has-used-stingrays-more-1000-times-2008 ("In response to an NYCLU FOIL request, the NYPD disclosed it used Stingrays nearly 1,016 times between 2008 and May of 2015.").

[15] YouTube, *Baltimore Police Address 'Operation Stingray,' ABC 2 News – WMAR*, at 1:35, *available at* https://www.youtube.com/watch?v=zX4GhFvhRzw.

one case after another, . . . police in Baltimore and other cities used the phone tracker, commonly known as a stingray, to locate the perpetrators of routine street crimes and frequently concealed that fact from the suspects, their lawyers and even judges."[16] Heath's report includes these details:

> "We're out riding around every day," said one officer assigned to the [BPD] surveillance unit, who spoke on the condition of anonymity because of the department's non-disclosure agreement with the FBI. "We grab a lot of people, and we close a lot of cases."
>
> Not all of those cases are big. Records show police used a cell-site simulator to track down a woman charged with stealing credit cards from a garage and using them to pay two months' rent at a self-storage unit. They used it to hunt for a stolen car and to find a woman who sent hundreds of "threatening and annoying" text messages to a Baltimore man. In each case, prosecutors ultimately dropped the charges or agreed to pretrial diversion.
>
> In 2011, detectives used a stingray to try to find a man who took his wife's cellphone during an argument, telling her, "If you won't talk to me, you're not going to talk to anyone," according to court records, a crime the surveillance team classified as a robbery. Police tracked the phone that day, but by then, it had already been returned to his wife, so they tracked it to her house.[17]

Heath's report is based in large part on a BPD surveillance log that he published alongside the in-depth report.[18] A review of the 2,116 entries in which

---

[16] Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY, Aug. 24, 2015, http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[17] *Id.*

[18] Cell Site Data Request, *available at* https://assets.documentcloud.org/documents/2287407/cell-site-data-request-060815-bds-2.pdf. The word "captured" means CS simulator.

CS simulator equipment was used includes circumstances classified as "witness location," "unarmed robbery," and the ambiguous "other."[19] In one unarmed robbery case, a status note documents the recovery of one pizza box.[20] In a number of entries in the log, the status field states, "wrong number."[21]

BPD makes frequent use of CS simulator surveillance technology, and seems to exercise little or no discretion when deciding when to deploy this powerful surveillance technology with such great potential to harm bystanders.

B. Baltimore City Police Department's uses cell site simulator equipment to transmit over licensed spectrum without a license

As mentioned briefly above, to impersonate cell towers on the network and establish a connection with handsets that in turn facilitates surveillance, CS simulators must transmit over frequency ranges licensed to cellphone carriers. As DOJ explains,

> Cell-site simulators . . . function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.[22]

A representative of another police department explained before a Florida court in 2010, "In essence, we emulate a cellphone tower. So just as the phone was registered with the real Verizon tower, we emulate a tower; we force that

---

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Department of Justice, *Policy Guidance: Use of Cell-Site Simulator Technology* at 2, *available at* https://www.justice.gov/opa/file/767321/download.

handset to register with us."[23] In an article on cellphone surveillance published in the *Harvard Journal of Law & Technology*, Christopher Soghoian and Stephanie Pell explained that CS simulators "send signals, often indiscriminately, through the walls of homes, vehicles, purses, and pockets in order to probe and identify the phones located inside."[24]

BPD's use of the spectrum is unauthorized. Because so much information about particular CS simulator devices is kept secret, it is difficult to know precisely in which frequency ranges BPD's specific device(s) can transmit. However, the equipment authorization application submitted for one device marketed by Harris Corporation to law enforcement officials indicates that Harris's equipment is capable of operating over virtually all bands reserved for operation of CMRS: 869.2–893.8 MHz, 1930.2–1989.8 MHz, 870.25–893.75 MHz, and 1931.25–1988.75 MHz.[25] In Baltimore, these ranges are licensed to phone carriers AT&T,[26] Verizon,[27] Sprint,[28] T-Mobile,[29] and Tecore (a prison phone servicer).[30]

---

[23] Transcript, Motion to Suppress, Case No.: 2008-CF-33350A (Aug. 23, 2010), at 12, *available at* https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

[24] Stephanie K. Pell & 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*, 28 Harv. J.L. & Tech. 1 (2014) at 12, *available at* http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf.

[25] *See* FCC, Grant of Equipment Authorization, Harris Corporation, Apr. 19, 2011, *available at* https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=9nDFvP9N200RJUhSYM6ASQ%3D%3D&fcc_id=NK73092523.

[26] *See* Cellular License - KNKA242 - NEW CINGULAR WIRELESS PCS, LLC – Frequencies, *available at* http://wireless2.fcc.gov/UlsApp/UlsSearch/frequenciesCell.jsp?licKey=12641&channelBlock=A (NEW CINGULAR WIRELESS PCS, LLC dba AT&T: 824 - 835 MHz paired with 869 - 880 MHz, 845 - 846.5 MHz paired with 890 - 891.5 MHz); PCS Broadband License - KNLF220 - New Cingular Wireless PCS, LLC, *available at* http://wireless2.fcc.gov/UlsApp/

(continued on next page)

A search of the FCC's Universal Licensing System for all of the frequency ranges named in Harris's equipment authorization application to the FCC yields not one instance of a license issued to BPD. Thus it is clear that BPD's use of CS simulator equipment constitutes transmission over licensed spectrum without an appropriate license.

C. Baltimore City Police Department obscures its use of cell site simulators, and the policy that governs that use, from the public

BPD obscures its use of CS simulators, making existence of the technology public but keeping the public intentionally in the dark on the details. Although the department has made heavy use of the technology for over nine years, a thick veil of secrecy remains over exactly what equipment BPD owns and what it is capable of, when and where that equipment is used, and what—if any—use policy governs officers with access to the equipment.[31]

(footnote continued)
UlsSearch/license.jsp?licKey=8897 (New Cingular Wireless PCS, LLC dba AT&T Mobility LLC, 1870.0–1885.0, 1950.0–1965.0).

[27] *See* Cellular License - KNKA232 - Cellco Partnership – Frequencies, *available at* http://wireless2.fcc.gov/UlsApp/UlsSearch/frequenciesCell.jsp?licKey=13197&channelBlock=B (Cellco Partnership dba Verizon Wireless: 835 - 845 MHz paired with 880 - 890 MHz, 846.5 - 849 MHz paired with 891.5 - 894 MHz).

[28] *See* PCS Broadband License - KNLF200 - APC PCS, LLC., *available at* http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=8878 (Sprint Nextel Corporation dba APC PCS, LLC., 1850.0–1865.0, 1930.0–1945.0).

[29] *See* PCS Broadband License - WPZQ943 - T-Mobile License LLC, available at http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=2596021 (T-Mobile License LLC dba T-Mobile USA, Inc., 1850.0–1865.0, 1930.0–1945.0).

[30] *See* KNLF200 - L000010050 - Tecore Government Services, LLC, available at http://wireless2.fcc.gov/UlsApp/UlsSearch/leaseMain.jsp?licKey=3417308.

[31] BPD has been under a non-disclosure agreement with the FBI related to CS simulators since at least 2011. Baltimore FBI Non-Disclosure Agreement (July 13, 2011), *available at* https://www.documentcloud.org/documents/1809046-baltimore-fbi-agreement.html.

Little or nothing is known about specific circumstances in which BPD uses CS simulators, other than that the devices are used much more than merely to investigate violent crimes, as noted above.[32] The surveillance log unearthed by reporter Brad Heath includes 2,116 entries in which CS simulator equipment appears to have been used.[33] Hundreds of those entries, however, classify the type of case under investigation as "other."[34] And 2,116 entries constitute only half of the reported 4,300 times BPD used the device in a similar timeframe.[35] Nothing is known to the public about the missing thousands of uses.

Nor does BPD have a written CS simulator use policy that the public could inspect, let alone participate in drafting. When asked in a March 2016 legislative hearing—more than nine years after BPD began using CS simulators—whether the department has such a policy, Lt. Michael Fries stated, "Baltimore City does not; we're in the process of drawing up a policy that would guide it."[36]

II. Cell site simulators harm the communities where they are deployed and the individuals in those communities

Cell site simulators are harmful to individuals in their vicinity. These devices disrupt normal operation of the cellular phone network, preventing those within their reach from placing cellular phone calls normally. Disruption of the network extends to emergency calls. Worse, these disruptions to the cellular network and the life-saving communications it serves are not experienced equally by all Americans. Rather, CS simulators disproportionately interfere with

---

[32] *See supra* notes 16–21 and corresponding text.
[33] *See* Cell Site Data Request, *supra* note 18.
[34] *See id.*
[35] See Fenton, *supra* note 1.
[36] Hearing before Maryland State Senate, *supra* note 10, at 1:14:45.

communications in communities of color, where police surveillance tools are disproportionately deployed. The Baltimore Police Department has long exhibited well-documented embedded racial bias, making excessive CS simulator use all the more concerning. Finally, CS simulators chill protected First Amendment activities.

A. Cell site simulators disrupt normal operation of the cellphone network

It is indisputable that CS simulators disrupt the communications of nearby cellphones. Indeed, the core function of CS simulator equipment is to interfere with the normal exchange between cellular handsets and the cellular network, as explained above. The resultant interference has been acknowledged in statements made by law enforcement officials. For example, in 2015, Assistant United States Attorney Osmar J. Benvenuto told a federal court in New Jersey, "Because of the way the Mobile Equipment sometimes operates, its use has the potential to intermittently disrupt cellular service to a small fraction of Sprint's wireless customers within its immediate vicinity."[37] According to a primer on CS simulators that accompanied a Royal Canadian Mounted Police ("RCMP") memo, which was disclosed in a Canadian court case and reported on by the

[37] Application of the United States of America for an Order Authorizing the Installation and Use of Pen Register and Trap and Trace Devices for the Cellular Telephone Facility Assigned Telephone Number 908-448-3855, Sealed Application, at 8 (D.N.J. July 13, 2015), *available at* http://www.wired.com/wp-content/uploads/2015/02/Stingray-pen-register-order-and-application.pdf; *see also United States v. Rigmaiden*, 2013 WL 1932800 *1, *15 (D. Ariz. May 8, 2013) ("The mobile tracking device caused a brief disruption in service to the aircard."); Anchorage Police Department, Sole Source Proprietary Purchase Request: Harris KingFish Dual Mode System, Memorandum (June 24, 2009), *available at* http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf ("[The CS simulator] allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection[s].").

Globe & Mail, "When it attracts all the mobile telephones in its range, the [CS simulator] may, depending on how it is used, temporarily take them off the public telecommunications network."[38]

The area of interference is substantial. According to a catalogue of cellphone surveillance devices obtained and published by *The Intercept*, StingRay I and II devices, from the same family as the later generation HailStorm in use by BPD, have an approximate ground distance of 200 meters.[39] This aligns with testimony provided by Sergeant Tom Bonin of the Maryland State Police, who told the state legislature that the CS simulator he uses has a range of 200 meters.[40] Within densely populated areas of Baltimore, a radius of 200 meters encompasses several blocks and potentially dozens or even more than a hundred homes. For example, the below image shows a 200-meter radius around an address in Baltimore where, according to surveillance logs, a CS simulator was used to locate a witness:[41]

---

[38] Colin Freeze, *RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals*, The Globe and Mail (Apr. 18, 2016), http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/.

[39] *Government Cellphone Surveillance Catalogue*, The Intercept (Dec. 17, 2015), at slide 51, *available at* https://theintercept.com/document/2015/12/16/government-cellphone-surveillance-catalogue/.

[40] Hearing before Maryland State Senate, *supra* note 10, at 55:50.

[41] Image generated courtesy of FreeMapTools, https://www.freemaptools.com/.

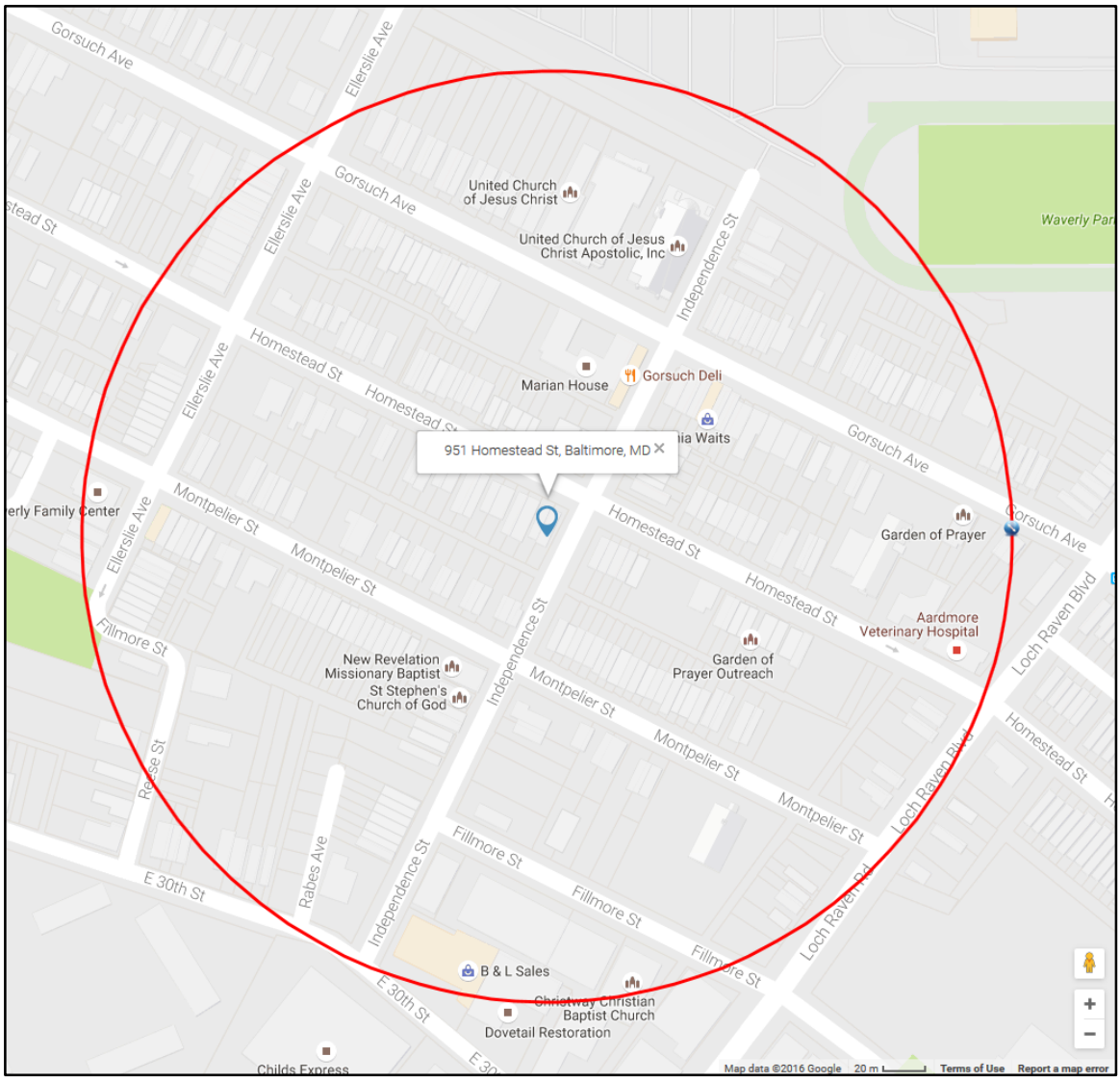

Figure 1 – Sample 200 Meter Radius Around CS Simulator

The range of BPD's CS simulator equipment could be even greater if the department also has an amplifier called a Harpoon, as a 2013 bid solicitation suggests is possible.[42] According to Harris Corporation's sales materials, "Harpoon is a software-controlled, high-power filtered amplifier that maximizes the multichannel transmit capability of the StingRay II and significantly improves the performance of the single-channel Stingray and KingFish systems

[42] *See* Bid Solicitation: B50002783, *supra* note 7.

by providing high-gain, wide dynamic range, and excellent linearity along with 30 watts of filtered output power."[43]

Worse, CS simulators create further network disruption by directly harming individual handsets. According to the catalogue published by *The Intercept*, StingRay I and II devices drain batteries and raise signal strength of devices locked on to them.[44] This is supported by scattered anecdotes. For example, when police used CS simulators to track protestors during the 2012 NATO summit in Chicago, "NATO summit protestors had problems with their cellphones, including dropped calls and difficulties sending text messages. Protestors also noticed their cellphone batteries losing power faster than usual."[45]

Testimony provided by an Investigator in the Tallahassee, Florida Police Department explains why CS simulators deplete phone batteries:

> [O]nce the equipment comes into play and we capture that handset, to make locating it easier, the equipment forces that handset to transmit at full power.
>
> Again, that's why I say once we capture it, it becomes much easier to specifically locate.

---

[43] Harris, *Harpoon, Software-Controlled, High-Powered Filtered Amplifier*, *available at* https://cdn.arstechnica.net/wp-content/uploads/2013/09/harpoon.pdf.

[44] *See* Government Cellphone Surveillance Catalogue, *supra* note 39, at slide 51 ("Locking handset into SDCCH drains battery and raises signal strength").

[45] Ellyn Fortino, *Are The Chicago Police Tracking People's Cellphones?*, Progress Illinois (Jun. 18. 2014), http://progressillinois.com/posts/content/2014/06/17/lawsuit-against-chicago-police-seeks-transparency-possible-cellphone-survei; *see* Mike Dumke, *Chicago Police Are Spying on Citizens*, Chicago Reader (Mar. 18, 2015), http://www.chicagoreader.com/chicago/chicago-police-spying-surveillance-first-amendment-protesters-nato/Content?oid=16893815 (confirming that police were in fact monitoring NATO summit protestors using CS simulators).

> So we're forcing that handset to transmit at full signal, consuming battery faster, in an effort to help us locate that handset.[46]

That CS simulators interfere both with the cellphone network and with individual handsets is an ever-increasing concern, as more and more households do away with landlines and come to rely completely on cellphones. According to the National Health Interview Survey conducted by the Centers for Disease Control and Prevention, less than 50% of American households had landlines in 2015.[47]

CS simulators cause extensive network disruption in the area where they are deployed. They block calls and also drain batteries in bystanders' cellphones, and these harms can extend blocks away from where the device is located.

B. Cell site simulators interfere with emergency calls

It is of particular significance that disruptions caused by CS simulators extend even to crucially important emergency calls. CS simulator manufacturers anticipated that CS simulators could block 911 calls, and reportedly have therefore programmed some CS simulators to allow 911 calls placed by connected handsets to pass through to cell towers.[48] But even in devices that have this functionality, the 911 pass-through feature is known and has been

---

[46] Transcript, Motion to Suppress, Case No.: 2008-CF-33350A, *supra* note 23, at 17.

[47] *See* Stephen J. Blumberg, Ph.D., and Julian V. Luke, *National Health Interview Survey Early Release Program*, Centers for Disease Control and Prevention (Dec. 2015), at 5, *available at* http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201512.pdf (of households interviewed between January and June 2015, 41.6% had landlines and wireless, 7.6% had landlines without wireless, and 0.1% had landline with unknown wireless, for a total of 49.3%).

[48] *See* Freeze, *supra* note 38; *see also* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, Wall St. J. (Nov. 13, 2014), http://on.wsj.com/26or7qK.

demonstrated to be unreliable. For example, the RCMP ran tests of the 911 pass-through function on CS simulators in Canada and found that about half of bystanders' 911 calls failed during CS simulator operations on the Canadian cellphone network, even when the 911 pass-through feature was active.[49] Alarmed at the high rate of 911 blockage, RCMP has gone so far as to restrict officers' use of the devices in an attempt to ensure that bystanders are able to make emergency calls.[50] RCMP policy now requires that officers limit the range of CS simulators "as much as is reasonably necessary," limit the duration of use, and observe mandatory rest periods between uses.[51] RCMP policy further instructs officers to weigh the benefits of CS simulator use "against the importance of having a reliable 911 system that Canadians can count on in all circumstances."[52]

Moreover, even when and if the pass-through function works as device manufacturers claim it does, CS simulators still block emergency calls to numbers other than 911. In emergency situations, cellphone users do not dial 911 alone—especially where, as in Baltimore, "racial disparities and indications of intentional discrimination erode community trust" in the police.[53] Depending on the nature of an emergency, it may be urgently necessary for a caller to reach, for example, a parent or child, doctor, psychiatrist, school, hospital, poison control center, or suicide prevention hotline. Thus, even if the 911 pass-through feature

---

[49] *See* Freeze, *supra* note 38 ("[R]ecent testing at HQ revealed that more than 50% of the GSM mobile telephones tested had not automatically completed their 911 calls after the [CS simulator] had shut itself off.").

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Investigation of the Baltimore City Police Department, U.S. Department of Justice, Civil Rights Division (Aug. 10, 2016), at 47, *available at* https://www.justice.gov/opa/file/883366/download ("DOJ Report").

were functional 100% of the time, non-911 emergency calls would still be subject to disruption.

C. Interference caused by cell site simulators disproportionately harms Black neighborhoods in Baltimore

Even more troubling, these disruptions of the cellphone network—including of emergency calls—disproportionately harm the residents of Baltimore's Black neighborhoods, where BPD exercises its authority in a racially biased way. As the Department of Justice ("DOJ") recently found, BPD "intrudes disproportionately upon the lives of African Americans at every stage of its enforcement activities."[54] According to the DOJ, statistical evidence shows that "BPD officers disproportionately stop African Americans; search them more frequently during these stops; and arrest them at rates that significantly exceed relevant benchmarks for criminal activity."[55] African Americans in Baltimore are also subjected more often to false arrests and uses of force, including constitutionally excessive force.[56] DOJ also found "numerous examples of BPD officers using racial slurs or other statements that exhibit bias."[57] City and BPD leaders have recently also acknowledged the damage done to the city's Black communities by BPD's "zero tolerance" policing strategy, which focused stops, searches, and misdemeanor enforcement on predominantly Black neighborhoods.[58] One of BPD's top officials reportedly told DOJ that "stop and frisk killed the hopes and dreams of entire communities."[59]

---

[54] DOJ report at 47.
[55] *Id.*
[56] *Id.*
[57] *Id.* at 66.
[58] *Id.* at 62–63.
[59] *Id.* at 63.

The DOJ report is just the latest evidence of BPD's longstanding and deep-seated institutionalized racism. In 1998, the Equal Employment Opportunity Commission determined that BPD routinely disciplined Black officers more harshly than white officers.[60] In 2009, BPD reached an agreement with 15 officers and former officers to settle allegations that it engaged in a pattern or practice of discrimination against Black police officers.[61] Under that settlement, BPD agreed to pay out $2.5 million, as well as to retain an outside consultant for a period of 3–5 years to collect information about racial discrimination or disparities in BPD's disciplinary system and file periodic reports with the Police Commissioner.[62] In 2014, the *Baltimore Sun* reported that since 2011, Baltimore had paid about $5.7 million to resolve lawsuits claiming that police officers brazenly assaulted suspects, the majority of whom were Black.[63] And in 2015, even before the tragic death of Freddie Gray, then–Police Commissioner Anthony W. Batts stated that Baltimore is still "dealing with 1950s-level black-and-white racism."[64]

Racial disparities in policing extend to surveillance. As Complainants and 42 other organizations explained in a letter earlier this year urging Chairman

---

[60] Michael Janofsky, *Agency Finds Racial Bias in Baltimore's Police Force*, N.Y. Times (Dec. 24, 1998), http://www.nytimes.com/1998/12/24/us/agency-finds-racial-bias-in-baltimore-s-police-force.html.

[61] Settlement Agreement, *Hopson et al v. City Of Baltimore et al* (Dec. 6, 2004).

[62] *Id.*

[63] Mark Puente, *Undue Force*, Baltimore Sun (Sep. 28, 2014), http://data.baltimoresun.com/news/police-settlements/ ("Such beatings, in which the victims are most often African-Americans, carry a hefty cost. . . . They . . . divert money in the city budget — the $5.7 million in taxpayer funds paid out since January 2011 would cover the price of a state-of-the-art rec center or renovations at more than 30 playgrounds.").

[64] Justin George & Mark Puente, *Baltimore Leaders Agree: City Has a Race Problem*, Baltimore Sun (Mar. 14, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-baltimore-racism-20150314-story.html.

Wheeler to investigate and address the disproportionate impact of CS simulators on historically disadvantaged communities,

> New technological tools that amplify police power can amplify existing biases in policing. Lack of effective oversight and supervision . . . 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.[65]

MAG-Net recently explained in a statement to the United Nations Special Rapporteur on the Right to Privacy,

> In the United States, racebased discrimination and control has always been at the center of surveillance. From slave pass laws to Jim Crow laws in the 19th century that enforced racial segregation at the state and local level to the 20th century where federal and local agencies targeted political activists and civil rights leaders. In the 21st century, a new, racialized system of mass surveillance has brought racial segregation into the digital age by expanding the carceral state and fueling growing income inequality all of which threatens human rights for all people.[66]

This is a problem all over the country. In Los Angeles, the Stop LAPD Spying Coalition has described an "architecture of surveillance" which disproportionately targets people of color and which includes, among other things, the use of CS simulators, "predictive" policing, and a Suspicious Activity

---

[65] Letter to Chairman Thomas Wheeler and Erika Brown Lee, Mar. 16, 2016, at 2 http://www.media-alliance.org/downloads/FinalStingrayLetter_3-14-2016_45.pdf.

[66] Statement to United Nations Special Rapporteur on the rights to privacy, MAG-Net, Jul. 6, 2016, in "The Relentless 'Eye,' Local Surveillance: its impact on human rights and its relationship to National and International surveillance," at 4, *available at* http://centerformediajustice.org/wp-content/uploads/2016/07/Relentless-Eye.pdf.

Reporting ("SAR") program.[67] The FBI has disclosed before Congress that it flew surveillance aircraft over Ferguson and Baltimore during the protests following the police killings of Michael Brown and Freddie Gray.[68] In Lansing, Michigan, neighborhoods selected for video surveillance based on reported crime rates were found to have approximately 15 percent more black residents than non-surveilled neighborhoods.[69] And in at least some cases, racial bias could be embedded in the surveillance technology itself.[70]

The problem of racialized surveillance is particularly pronounced in Baltimore, where BPD's racially biased policing is clearly reflected in its racially biased deployment of CS simulators. To illustrate, the map below pinpoints hundreds of addresses where *USA Today* reporter Brad Heath reported that BPD used CS simulators, laid on top of a map of Baltimore's Black population that was included in DOJ's recent report based on 2010 Census data.[71]

---

[67] Statement of Stop LAPD Spying Coalition, June 30, 2016, in "The Relentless 'Eye,' Local Surveillance: its impact on human rights and its relationship to National and International surveillance," at 3, *available at* http://centerformediajustice.org/wp-content/uploads/2016/07/Relentless-Eye.pdf.

[68] Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights*, ACLU (Oct. 30, 2015), https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights.

[69] *See e.g.*, American Civil Liberties Union, *Eyes in the Sky: Lansing Residential Surveillance and its Intrusion on Privacy*, at 11 (2012), *available at* http://www.aclumich.org/sites/default/files/Eyes%20in%20the%20Sky.pdf.

[70] *See* Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, The Atlantic (Apr. 7, 2016), http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[71] Brad Heath; DOJ Report at 13. Mashup created by Georgia Bullen.

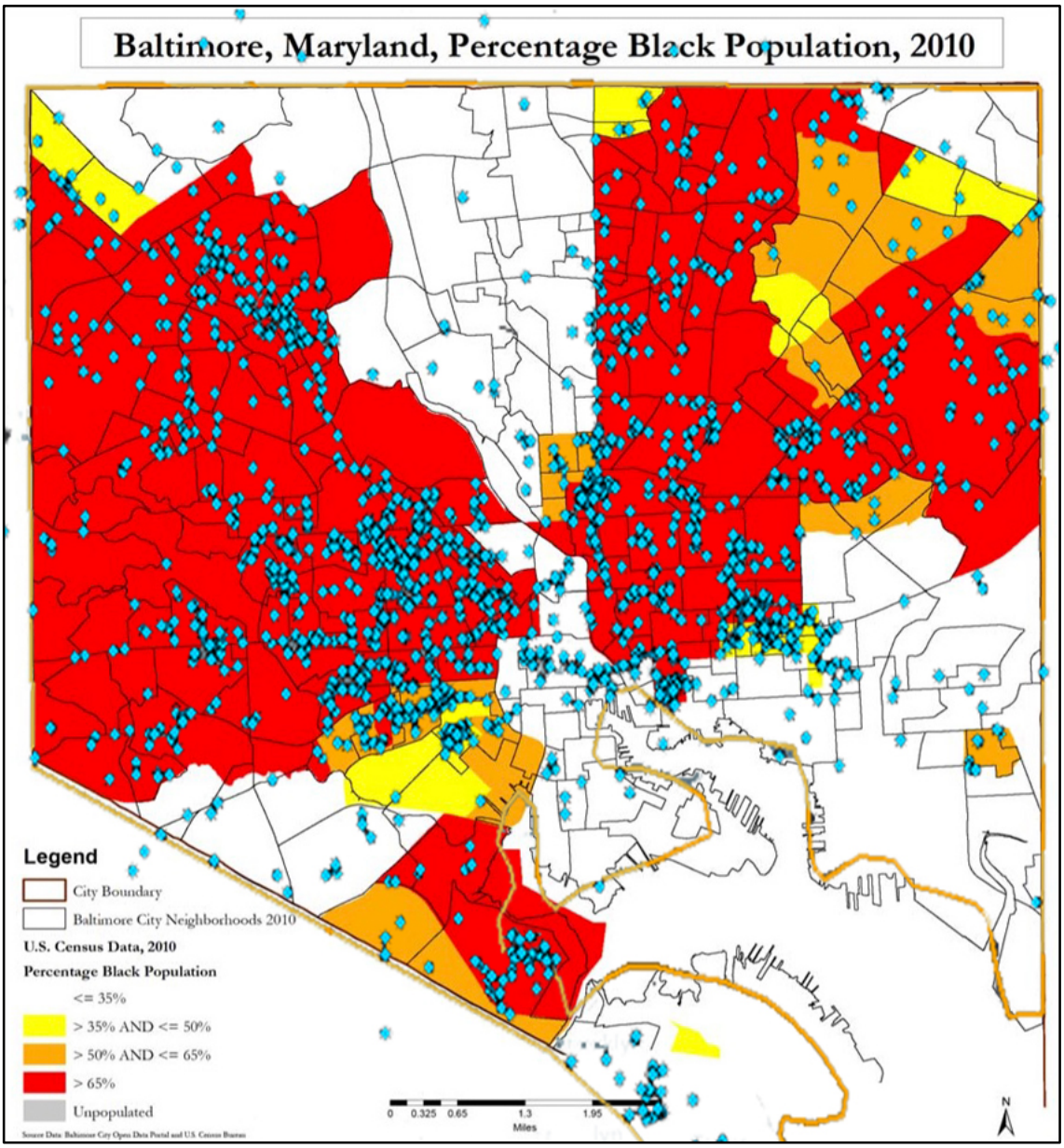

Figure 2 –Deployment Sites Overlaid on Map of Baltimore's Black Residents

As discussed above, BPD uses CS simulators to investigate street crimes involving non-violent offenders. This compounds the disproportionate impact on Black communities, which studies have established suffer disparate impact from street crime enforcement.[72]

[72] *See, e.g.*, Eduardo Bonilla-Silva, supra note 5, at 109 (citing numerous studies demonstrating that African-American communities are "overpatrolled" and that

(continued on next page)

D. Baltimore City Police Department's use of CS simulator equipment chills speech

BPD's use of CS simulator equipment harms the public in another important way: it chills free speech and association. As Karen Gullo of the Electronic Frontier Foundation explained in a blog post discussing recent studies that examined the effects of surveillance on speech,

> Now two new studies examining the use of Facebook and Wikipedia show that this chilling effect is real. Both studies demonstrate that government surveillance discourages speech and access to information and knowledge on the Internet. What happens is that people begin to self-police their communications: they are more likely to avoid associating with certain groups or individuals, or looking at websites or articles, when they think the government is watching them or the groups/people with whom they connect. This hurts our democracy and society as a whole [73]

Brandi Collins of Color Of Change has discussed the consequences of surveillance specifically for protestors, especially participants in racially charged protests against incidents of police violence, such as the death of Freddie Gray in BPD custody:

> The surveillance and monitoring practices of . . . federal, state, and local law enforcement entities are chilling the protected activities of organizers, activists and members of the public at large who are or who wish to speak out publicly in opposition to the

(footnote continued)
police are more likely to "see" criminal behavior in such communities than in white communities).

[73] Karen Gullo, Electronic Frontier Foundation, *Surveillance Chills Speech – As New Studies Show – And Free Association Suffers* (May 19, 2015), https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association.

> alarming—indeed crisis-level—trend of police brutality and killing in the United States.[74]

Worse, BPD's use of CS simulator equipment may not only chill First Amendment–protected activities incidentally, but could in fact include direct monitoring of protestors. As noted and discussed above, BPD disclosures have failed to explain or justify thousands of undocumented uses of this equipment, and the department has no written policy governing the equipment.

It is clear, however, that BPD has exercised a pattern of unlawfully restricting speech. According to the DOJ, "BPD officers routinely infringe upon the First Amendment rights of the people of Baltimore City."[75] DOJ noted, "The people of Baltimore have a constitutional right to observe and verbally criticize the police."[76] Examining numerous instances in which BPD officers demonstrated harsh responses to civilian criticism, DOJ concluded, "BPD officers may consider speech critical or disrespectful of their activities to be assaultive or disruptive, and therefore sufficient to justify suppression through the unlawful use of police powers to detain and arrest."[77]

It is also clear that BPD has a habit of focusing its surveillance power on protestors critical of its practices. For example, during the Baltimore protests that followed the death of Freddie Gray, who died from injuries sustained in BPD custody, BPD joined the FBI on flights over the city to conduct surveillance of

---

[74] Statement of Brandi Collins, ColorOfChange.org, Jul. 2016, in "The Relentless 'Eye,' Local Surveillance: its impact on human rights and its relationship to National and International surveillance," at 11, *available at* http://centerformediajustice.org/wp-content/uploads/2016/07/Relentless-Eye.pdf.

[75] DOJ Report at 116.

[76] *Id.*; *see City of Houston v. Hill*, 482 U.S. 451, 462–63 (1987)("The freedom of individuals verbally to oppose or challenge police action without thereby risking arrest is one of the principle characteristics by which we distinguish a free nation from a police state.").

[77] DOJ Report at 118.

protestors.[78] According to the FBI, the surveillance aircraft were provided to BPD for the purpose of "providing aerial imagery of possible criminal activity."[79] Also during that time, the city of Baltimore received a report from cybersecurity firm ZeroFox indicating that the firm monitored Black Lives Matter protestors during the Freddie Gray protestors, and identified organizers DeRay McKesson and Johnetta Elzie as "threat actors" for whom it recommended "immediate response."[80]

When police illegitimately conduct surveillance of individuals and communities who are speaking out against problems with the police, chilling effects may not be a mere side effect of surveillance, but its very objective. In the words of Color Of Change's Brandi Collins,

> The revelations of FBI, DHS, and local law enforcement surveillance of movement for Black lives . . . leads us to fear that the current surveillance of the emerging movement for political accountability and justice is more coordinated, extensive, and systematic than has been revealed thus far and that it is intended to silence the demands of the movement for Black lives and related movements.[81]

Others have also noted the chilling effects of police surveillance of protestors, particularly as experienced by activists. In April, Black Lives Matter

---

[78] Wessler, *supra* note 68.

[79] Craig Timburg, *Surveillance Planes Spotted in the Sky for Days After West Baltimore Rioting*, Wash. Post (May 5, 2015), https://www.washingtonpost.com/business/technology/surveillance-planes-spotted-in-the-sky-for-days-after-west-baltimore-rioting/2015/05/05/c57c53b6-f352-11e4-84a6-6d7c67c50db0_story.html.

[80] Brandon Ellington Patterson, *Black Lives Matter Organizers Labeled as "Threat Actors" by Cybersecurity Firm*, Mother Jones (Aug. 3, 2015), http://www.motherjones.com/politics/2015/07/zerofox-report-baltimore-black-lives-matter.

[81] Statement of Brandi Collins, *supra* note 74.

activist Elsa Waithe told *The Intercept* that she believes police surveillance in New York is designed to chill dissent and gather information in order to better target organizers.[82] Activist DeRay Mckesson, who recently ran for mayor in Baltimore, said, "Some of this surveillance is meant to scare us and potentially to figure out what people's next steps are."[83]

There is no direct evidence that BPD is in fact using CS simulator equipment to monitor the activities of protestors. But the opaqueness of its secret and unwritten use policy, combined with its pattern of hampering speech and its history of surveilling protestors, suggest that this is a likely possibility.

III. The FCC should enforce the prohibitions on unauthorized spectrum use and interference, and should prohibit BPD from using CS simulators

The FCC can and should take swift action to address harms caused by operation of CS simulators by bringing an enforcement action against BPD for its operation of cellular transceivers without authority and for the resultant interference with the cellular network, including delivery of emergency calls. Americans rely on the FCC to protect the cellphone network from disruption and to ensure that emergency calls can be completed under any circumstances. Safeguarding communications networks is a responsibility of paramount importance for the FCC. Known disruptions of the cellphone network and interference with emergency calls are serious problems that the FCC can and must address. This issue is all the more urgent given the disparate harms experienced by communities of color, and the fact that police surveillance has

---

[82] George Joseph, *Undercover Police Have Regularly Spied on Black Lives Matter Activists in New York*, The Intercept (Aug. 18, 2015), http://interc.pt/1LjAe3x.

[83] *Id.*

racially biased chilling effects on First Amendment–protected speech and association.

A. The FCC has an unfulfilled commitment to protect the public from harms caused by cell site simulators

The FCC has a yet-unfilled commitment to address the threat posed by illicit CS simulators.[84] Chairman Wheeler made that commitment in response to a letter from Representative Grayson urging FCC action on CS simulators, then went on to explain that he had recently established a "task force to initiate immediate steps to combat the illicit and unauthorized use" of these devices.[85] When Senator Bill Nelson asked for a "status report" on the task force's activities in early 2015, Chairman Wheeler reassured him the task force is monitoring CS simulator–related issues, but he did not elaborate and provided no specifics.[86] Congress and the public still await the Chairman's promised "immediate steps."[87]

As devices that use licensed spectrum without a license, and that cause actual interference to many phone users, the CS simulators in use by BPD are

---

[84] Letter from Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, to Alan Grayson, U.S. Congressman 1 (Aug. 1, 2014), http://bit.ly/1YQelvB.

[85] *Id*. at 2.

[86] *See* Letter from Bill Nelson, U.S. Senator, to Tom Wheeler, Chairman, Fed. Commc'ns Comm'n 2 (Feb. 24, 2015), http://bit.ly/1QAbEIt; Letter from Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, to Bill Nelson, U.S. Senator 2 (Apr. 13, 2015), http://bit.ly/1NzBRvW.

[87] Letter from Tom Wheeler, *supra* note 84 and accompanying text. In early 2016, FCC spokesperson Neil Grace said the task force is still examining "the facts surrounding IMSI catchers," but he did not provide details on what the task force is doing or what it has found. Robert Kolker, *What Happens When the Surveillance State Becomes an Affordable Gadget?*, Bloomberg (Mar. 10, 2016, 6:00 AM), http://bloom.bg/1QJMmMR.

"illicit and unauthorized," and the FCC must honor its commitment to address the threat they present.

B. Baltimore City Police Department's unlicensed transmissions in the commercial mobile radio service bands violates Section 301 of the Communications Act and Section 1.903(a) of the Commission's rules

As discussed above, CS simulators such as BPD's HailStorm equipment transmit over spectrum reserved for operation of cellphone networks. In the Baltimore area, the frequency bands in which CS simulators operate are already licensed to wireless phone carriers. BPD operates CS simulator equipment in these bands, but has no license to operate in these frequency bands.

BPD's actions violate Section 301 of the Communications Act. As the FCC's Enforcement Bureau has explained,

> Section 301 of the Act states that no person shall use or operate any apparatus for the transmission of energy or communications or signals by radio within the United States, except under and in accordance with the Act and with a license granted under the provisions of the Act.[88]

BPD operates CS simulator equipment that transmits over licensed frequency bands without a license, and therefore violates Section 301 of the Act.

BPD's actions also violate Section 1.903(a) of the Commission's rules:

---

[88] *In the Matter of Towerstream Corporation*, Consent Decree, DA 16-653, ¶ 3 (2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0729/DA-16-653A1.pdf; 47 U.S.C. § 301 ("No person shall use or operate any apparatus for the transmission of energy or communications or signals by radio . . . except under and in accordance with this [Act] and with a license in that behalf granted under the provisions of this [Act].").

> Section 1.903(a) of the Rules requires that stations in the Wireless Radio Services must be used and operated only in accordance with the rules applicable to their particular service, and with a valid authorization granted by the Commission.[89]

BPD's CS simulator equipment qualifies as a "station" that is "equipped to engage in radio communication or radio transmission of energy.[90] According to an equipment authorization granted to Harris, its equipment is designed to be operated in accordance with part 22, subpart H or part 24, subpart E of the Commission's rules.[91] BPD fails to operate its equipment in accordance with those rules by, at a minimum, failing to secure any appropriate license. BPD therefore violates Section 1.903(a) of the Commission's rules.

C. Baltimore City Police Department's use of cell site simulators interferes with cellular communications in violation of Section 333 of the Communications Act

As discussed above, BPD's operation of CS simulator equipment causes actual interference to cellular communications by forcing cellphones in the vicinity to register with the CS simulator, then preventing connected cellphones from completing phone calls during the time when they are connected.

BPD's actions violate Section 333 of the Communications Act. Under Section 333,

> No person shall willfully or maliciously interfere with or cause interference to any radio communications of

---

[89] 47 C.F.R. § 1.903(a).

[90] 47 U.S.C. § 153(42).

[91] *Harris Corporation*, Grant of Equipment Authorization, EA994680 (Apr. 19, 2011), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=9nDFvP9N200RJUhSYM6ASQ%3D%3D&fcc_id=NK73092523.

> any station licensed or authorized by or under this Act or operated by the United States Government.[92]

BPD's use of CS simulator equipment interferes with radio communications of stations operated by a number of licensed cellular providers in Baltimore, as well as with the handsets, or mobile stations, of subscribers to those providers' services.[93] This interference is willful because interference is, in fact, the core functionality of CS simulators, which are used intentionally to supersede the legitimate cellular towers with which cellphones would remain connected in the absence of CS simulator activity. BPD undoubtedly is well aware of the harmful interference caused by operation of its CS simulator equipment—officers on BPD's surveillance team reportedly receive 40 hours of training on using the equipment and an additional eight hours of "cellular theory" training from the U.S. Secret Service.[94] BPD therefore violates Section 333 of the Communications Act.

---

[92] 47 U.S.C. § 333.

[93] Because they are "designed to intentionally . . . interfere with authorized radio communications," CS simulators constitute jamming devices, which the FCC has clearly stated are prohibited under, *inter alia*, Sections 301 and 333 of the Communications Act. Jammer Enforcement, FCC, https://www.fcc.gov/general/jammer-enforcement (last visited Aug. 15, 2016).

[94] Heath, *supra* note 16. "Willful" is not defined in Section 333, but it is reasonable to assign it the same meaning it has in Section 312(f), in which "'willful', when used with reference to the commission or omission of any act, means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision of this chapter or any rule or regulation of the Commission authorized by this chapter or by a treaty ratified by the United States."

D. Baltimore Police Department is not exempt from provisions of the Communications Act that protect Americans from spectrum misuses and interference

The Communications Act applies to BPD just as it does to all other Americans. As Baltimore Mayor Stephanie Rawlings-Blake stated in 2015, "No one in our city is above the law."[95] The FCC has clear authority to hold law enforcement agencies to the same standards to which it holds the American public, and it has exercised this authority in the past. For example, a 2014 FCC Enforcement Advisory underscoring the prohibition against use of jamming devices stated, "This prohibition extends to every entity that does not hold a federal authorization, including state and local law enforcement agencies."[96] The Commission could not have been more explicit on this point, explaining,

> Federal law provides no exemption for use of a signal jammer by school systems, police departments, or other state and local authorities. Only federal agencies are eligible to apply for and receive authorization.[97]

Moreover, to the extent BPD applies for and obtains court orders for use of CS simulator equipment, those court orders do not negate BPD's separate obligation to abide by federal communications law.

---

[95] *National and Local Reaction to Charges in Freddie Gray Case*, Baltimore Sun (May 2, 2015), http://www.baltimoresun.com/sports/bs-md-ci-freddie-gray-reax-quotes-0502-20150501-story.html.

[96] *FCC Enforcement Advisory, Warning: Jammer Use is Prohibited*, DA 14-1785, Public Notice, 29 FCC Rcd 14737 (2014), https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1785A1_Rcd.pdf ("*FCC Enforcement Advisory*").

[97] *Id.*

E. The FCC has a duty to protect Americans against discriminatory unavailability of emergency calling service

As discussed above, BPD's CS simulator equipment interferes not only with normal operation of the network, but also with 911 and other emergency calls on a racially discriminatory basis. The FCC must take swift action to correct this in order to fulfill its duty under Section 151 of the Communications Act:

> to make available, so far as possible, to all people of the United States, *without discrimination on the basis of race, color, religion, national origin, or sex*, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities . . . for the purpose of . . . promoting safety of life and property through the use of wire and radio communications.[98]

It is among the Commission's most fundamental duties to ensure that 1) America's communications networks provide everyone with access to adequate emergency calling services, and 2) that access is available *without discrimination on the basis of race or color*.

The Commission has taken countless steps in pursuit of its Section 151 duty. It has devoted substantial attention and resources to ensuring the availability of robust 911 services that embrace the best available technology to keep Americans safe.[99] The Commission also has not been shy about taking decisive action wherever emergency calling services have been compromised.[100]

---

[98] 47 U.S.C. § 151 (emphasis added).

[99] *See 9-1-1 and E9-1-1 Services*, FCC, http://fcc.us/24fr9iI (last updated Feb. 16, 2016) (detailing the history of the Commission's 9-1-1 rules, ongoing efforts to improve the "E911" system, and other regulations designed to secure emergency calling for all).

[100] *See, e.g.*, *In the Matter of T-Mobile USA, Inc.*, DA 15-808, Order, 30 FCC Rcd 7247 ¶ 3 (2015).

For example, the FCC fined T-Mobile $17.5 million in 2015 for failing to promptly resolve a 911 outage, observing: "One of the bedrock principles of the Communications Act and the Commission's rules is that reliable 911 service must be available *to all Americans at all times*."[101] The FCC has also pointed to the importance of protecting emergency calling in its most recent enforcement advisory regarding signal jamming prohibitions.[102]

Congress has given the Commission, through Section 154(o) of the Act, broad authority when it comes to fulfilling its Section 151 mandate to ensure the availability of emergency calling services:

> For the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the Commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems.[103]

Congress's intent here is unmistakable. In order to ensure the availability of emergency calling services, the Commission has wide latitude and should take a holistic approach to resolving concerns regarding the availability of such services.

Furthermore, the FCC operates under the Communications Act's Section 332(a) mandate to consider, "consistent with section 151," whether its spectrum management actions will "promote the safety of life and property."[104] Thus, to supplement its general Section 151 duty to provide for emergency calling

---

[101] *Id*. at ¶ 1 (emphasis added).
[102] *FCC Enforcement Advisory, supra* note 94. As noted above, this enforcement advisory explicitly states that it applies even to law enforcement.
[103] 47 U.S.C. § 154(o).
[104] 47 U.S.C. § 332(a).

services, Congress has given the Commission a special responsibility to ensure that its actions do not frustrate the availability of those services.

Ensuring that all people have access to emergency calling services, regardless of their race or color, is fundamental to the FCC's mission. The FCC itself has pointed to Sections 151, 154, and 332 in its actions to ensure the availability of emergency calling services.[105] Because the Commission's authorization of CS simulator equipment has had the consequence of disrupting the ability of the communications networks to facilitate emergency calling, especially in historically disadvantaged communities, it has a special responsibility under the Communications Act to address the problem and broad discretion as to how to do so.

[105] *See, e.g.*, *Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, FCC-07-177, Order on Reconsideration, 22 FCC Rcd 10541, 10580 (2007) (citing, among other provisions, 47 U.S.C. §§ 151, 154, and 332 in adopting rules requiring communications providers to maintain emergency back-up power in order to ensure the resiliency and redundancy of 9-1-1 networks).

Conclusion

For the foregoing reasons, Complainants urge the Commission to take swift action to enforce Sections 301 and 333 of the Communications Act against the Baltimore City Police Department, and put an end to its rampant unauthorized use of licensed spectrum, which causes widespread disruption to the cellular network; interferes with calls, including emergency calls; disproportionately harms Black individuals and communities; and chills First Amendment activities. Complainants further request an enforcement advisory advising other law enforcement agencies of the general prohibition on use of harmful CS simulator equipment without proper authorization.

By:

/s/ _____
Laura M. Moy
Institute for Public Representation
600 New Jersey Ave, NW Suite 312
Washington, DC 20001

Counsel for Complainants

Respectfully submitted,

Center for Media Justice
Color Of Change
New America's Open Technology Institute

August 16, 2016