A MODERN MAJOR STATUTE: ILLINOIS RAISES THE BAR IN PROTECTING CITIZEN PRIVACY FROM CELL SITE SIMULATORS

Jeremy Greenberg*

CITE AS: 1 GEO. L. TECH. REV. 147 (2016)
https://perma.cc/RN6M-9M4Q

INTRODUCTION 147
ILLINOIS SETS THE BAR HIGH WITH AN EXCLUSIONARY REMEDY 148
IMPACT OF CS SIMULATORS 149
TRANSPARENCY NOW REQUIRED 150
PROHIBITION ON COLLECTING CONTENT 151
OTHER STATES SHOULD FOLLOW SUIT 152

INTRODUCTION

It was recently discovered that Baltimore, MD—a city known for its aggressive policing of black communities, had used cell site simulators ("CS simulators")[1] to surveil these communities over 4,300 times in the last eight years.[2] All done in secret, without a warrant.[3] 4,300 already seems like a considerable figure; however, comparing it to the number of simulators deployed in New York and San Diego underscores its true magnitude. Baltimore employed four times more simulators than New York City and eleven times more than San Diego over that same time period, despite the fact that both of those cities are more than twice its size.[4] Welcome to Baltimore—where your race may put your civil liberties at risk.

---

* GTR Staff Member; Georgetown Law, J.D. expected 2018; Ithaca College, B.S. 2009.

[1] CS simulators are devices that mimic cell towers, tricking cellphones to transmit their signal to the device. This allows the user, such as a police officer, to track the location of a targeted cellphone without the cellphone owner's knowledge. Some CS simulators also allow law enforcement to access the content of the cellphone's communications, such as the Fishhawk model, which allows the user to eavesdrop on conversations.

[2] Brian Barrett, *The Baltimore's Race PD Bias Extends to High—Tech Spying Too*, WIRED (Aug. 16, 2016, 8:01 AM), https://www.wired.com/2016/08/baltimore-pds-race-bias-extends-high-tech-spying/.

[3] *Id.*

[4] *Id.*

According to the Department of Justice, the practice of deploying CS simulators should require a warrant and only be used when necessary to achieve appropriately severe public safety objectives, such as apprehending a fugitive or locating a kidnapped child.[5] However, the DOJ only regulates CS simulators at the federal level, leaving states to regulate their own use.

To protect these heavily surveilled populations from civil liberty violations, state lawmakers should look to the recently enacted Illinois Citizen Privacy Protection Act.[6] With this new law, Illinois joins several other states in requiring law enforcement to obtain a warrant prior to deployment.[7] Moreover, Illinois' law sets a new high benchmark for protecting civil liberties by including an exclusionary remedy for unlawful deployment, prohibiting non-disclosure agreements between CS simulator manufacturers and law enforcement, and mandating the deletion of data incidentally collected from non-targeted devices.[8] These new regulations are crucial for protecting the civil liberties of all citizens, but are especially vital for historically disadvantaged communities, like African-Americans, who are frequently subject to disproportionally frequent and aggressive policing.[9]

ILLINOIS SETS THE BAR HIGH WITH AN EXCLUSIONARY REMEDY

The addition of a Fourth Amendment exclusionary rule for all unlawful use of CS simulators will help deter law enforcement from deploying CS simulators for justifications that do not meet the probable cause threshold.[10] The purpose of the exclusionary rule is to incentivize police to exercise careful deliberation required by the Constitution when exercising the investigative

[5] U.S. DEPT. OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 1 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download.
[6] Citizen Privacy Protection Act, 725 Ill. Comp. Stat. Ann. 137 (2016).
[7] Shahid Buttar, *Illinois Sets New Limits on Cell-Site Simulators*, ELEC. FRONTIER FOUND. (Aug. 11, 2016), https://www.eff.org/deeplinks/2016/08/illinois-sets-new-limits-cell-site-simulators (stating California, Washington, Utah, Minnesota, and Virginia all require law enforcement to obtain a warrant prior to deployment of a CS simulator).
[8] *Id.*
[9] U. S. DEP'T OF JUST., INVESTIGATION OF THE CITY OF BALTIMORE POLICE DEPARTMENT (2016), https://www.justice.gov/opa/file/883366/download; *see also*, U.S. DEP'T OF JUST., INVESTIGATION OF FERGUSON REPORT (2015) https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf.
[10] *Id.*

prerogative that accompanies their role.[11] In turn, prohibiting the use of evidence obtained unlawfully provides relief to defendants who were subjective to illegal surveillance.[12] Ultimately, this will help deter the widespread surveillance for routine street crimes that are far below the Department of Justice's "necessary" threshold.[13] A more limited scope for the use of CS simulators will protect the rights of those being surveilled, while promoting and limiting service disruption in heavily surveilled communities where the collateral effects of untrammeled use of the technology are the highest.

IMPACT OF CS SIMULATORS

A reduction in CS simulator surveillance will benefit heavily-surveilled communities, as CS simulators negatively impact the safety of users who are not deliberately targeted by the device, but are within its vicinity.[14] A CS simulator emits a signal stronger than those emitted by nearby cell towers, forcing mobile devices within a given coverage area to connect to it in lieu of connecting to the cell tower during CS simulator deployment.[15] After the CS simulator attracts the mobile devices within its range, the CS simulator operator will target a particular device and release all others. This process, known as "catch-and-release," will cause delays in service for all of the phones that attempted to connect to the CS simulator.[16] These disruptive service delays can have dire public safety consequences by preventing important communications, such as blocking 911 calls.[17] 911 calls are said to override the catch-and-release process, but a study from Canada shows that the override does not function up

---

[11] Nathan Freed Wessler, *A 30-Year-Old Loophole Increasingly Gives Police Officers a Pass When They Violate the Fourth Amendment*, Slate (Oct. 29, 2014, 11:49 AM), http://www.slate.com/articles/news_and_politics/jurisprudence/2014/10/police_s_good_faith_exception_courts_keep_expanding_exception_that_gives.html.

[12] *Id.*

[13] Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications at 8-9, Baltimore City Police Dept. (F.C.C. 2016) http://s3.documentcloud.org/documents/3015561/CS-Simulators-Complaint.pdf [hereinafter *Complaint*].

[14] Kim Zetter, *Feds Admit That Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015, 4:55 PM), https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/.

[15] *Id.*

[16] *Id.*

[17] Colin Freeze, *RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals*, THE GLOBE & MAIL (May 24, 2016, 3:21 PM), http://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memoreveals/article29672075/.

to half the time, effectively blocking 911 calls.[18] This high margin of error can be devastating on a community that is frequently surveilled. Moreover, the catch-and-release of other emergency calls, such as those to a doctor or loved one, will be delayed because of the catch-and-release, and could result in similarly concerning consequences, in addition to inconvenience.[19]

In addition to more drastic public safety concerns, the frequent deployment of CS simulators causes service disruption for the use of mobile devices more generally. CS simulators can degrade cellular service within the area to 2G service, which is required for authentication with the targeted mobile device.[20] This will result in the service of every mobile device attempting to connect to be knocked down to the now archaic 2G protocol, resulting in slower data transmission, which harms device functionality. In addition, the strong signals sent by CS simulators that force all mobile devices to connect to it drain the phones' batteries at a faster than rate than they otherwise would.[21] Finally, the catch-and-release attacks on mobile phones result in delayed and dropped calls for all targeted and untargeted phones in the area.[22] Though these service disruptions are less harmful to public safety than dropping 911 calls, and may be a necessary tradeoff in a narrow category of high-priority targets, such widespread disruption is a detrimental and inconvenient byproduct of what should be considered illegally broad surveillance.

TRANSPARENCY NOW REQUIRED

The Illinois Citizen Privacy Protection Act also encourages increased transparency by banning non-disclosure agreements between CS simulator manufacturers and law enforcement.[23] While lawmakers generally understand how CS simulators function, non-disclosure agreements shroud the specific capabilities of the devices.[24] Some prosecutors have gone so far as to drop

[18] *Id.*
[19] Zetter, *supra* note 14.
[20] Stephanie Pell, *We Must Secure America's Cell Networks —From Criminals and Cops*, WIRED (August 27, 2014, 6:30 AM), https://www.wired.com/2014/08/we-must-secure-americas-cell-networks-from-criminals-and-cops-alike/.
[21] Joel Hruska, *Stingray, The Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move*, EXTREME TECH (June 17, 2014, 4:51 PM), http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move.
[22] Zetter, *supra* note 14.
[23] 725 Ill. Comp. Stat. Ann. 137/15(a)(1).
[24] Jeremy Scahill and Margot Williams, *Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone*, THE INTERCEPT (Dec. 17, 2015, 12:23 PM),

charges to prevent disclosing technical specifications of certain CS simulators to courts.[25] In fact, much of the knowledge of the capabilities of CS simulators has come in the form of leaked instruction manuals, such as for the popular "StingRay" model manufactured by Harris Corporation.[26]

However, the dearth of information is soon to change. The first-of-its-kind transparency requirement will finally give Illinois decision-makers insight into the precise surveillance capabilities of CS simulators, and how law enforcement agents deploy them. This increased knowledge will allow decision-makers to make more informed decisions relating to citizens' rights, and allow the populations being surveilled to have a greater understanding of how law enforcement interferes with their privacy and use of mobile devices. Further, more information about the technology behind CS simulators will open the door for technicians to develop methods of surveillance that are less invasive for the un-targeted devices in the area.

PROHIBITION ON COLLECTING CONTENT

The Illinois law also precludes CS simulators from retaining content of communications by requiring data incidentally collected from non-targeted devices to be deleted.[27] It specifically requires that all non-targeted data must be deleted as "reasonably practicable," within 24 hours of collection from known targeted devices, and within 72 hours of identifying an untargeted device.[28] The inclusion of the requirement to delete all non-targeted data is crucial, as it has come to light through the leaking of CS simulator user manuals that CS simulators deployed by law enforcement can capture and retain metadata.[29] The capturing of the actual content of communications could have a chilling effect on activities protected by the First Amendment in communities that are targeted on a frequent basis.[30] This will be especially true in protests

---

https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/.

[25] *See* Cyrus Farivar, *Prosecutors Drop Robbery Case to Preserve Stingray Secrecy in St. Louis*, ARS TECHNICA (Apr 20, 2015, 8:00 AM), http://arstechnica.com/tech-policy/2015/04/prosecutors-drop-robbery-case-to-preserve-stingray-secrecy-in-st-louis/.

[26] Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, THE INTERCEPT (Sep. 12, 2016, 2:33 PM), https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

[27] 725 Ill. Comp. Stat. Ann. 137/10.

[28] *Id.* at 137/15(b).

[29] Jennifer Lynch, *Stargazer III: Ground Based Geo-Location (Vehicular)*, THE INTERCEPT, https://theintercept.com/surveillance-catalogue/stargrazer-iii/ (last visited Sept. 30, 2016).

[30] *Complaint*, *supra* note 13, at 25.

critical of aggressive policing, which often occur in communities that are subject to the most surveillance.[31] With the knowledge that this technology is being used by law enforcement, it is crucial for regulations to specifically preclude this behavior.

OTHER STATES SHOULD FOLLOW SUIT

Though the Illinois Citizen Privacy Protection Act does not solve all the issues surrounding the harmful deployment of CS simulators, it facilitates scrutiny of deployment; reduces a public safety risk; broadly encourages transparency surrounding the device's capabilities; and diminishes collateral privacy violations. Other states should follow Illinois in an effort to bring state legislation in line with the Department of Justice's stated goal of increasing public safety, rather than jeopardizing it by allowing law enforcement's violation of civil liberties to remain unchecked.

[31] *Id.* at 26-27.