STINGRAY SEARCHES AND THE FOURTH AMENDMENT IMPLICATIONS OF MODERN CELLULAR SURVEILLANCE

Austin McCullough*

Since the Snowden revelations, law enforcement agencies' broad technological surveillance tactics have come under greater public scrutiny.[1] One such surveillance technique is the StingRay, which is a device used to gather information. Unlike other devices, the StingRay can collect serial numbers and locations from surrounding cell phones without the phone owners' knowledge.[2] StingRays are substantially different than previous phone-tracking technology, as they are not only capable of revealing phones' location, but they also record phone numbers and the content of voice and text communication.[3] Law enforcement agencies go to great lengths to keep StingRays mired in obscurity and maintain their secrecy.[4] As these devices are challenged in courts, their use implicates numerous, unaddressed concerns under the Fourth Amendment.

StingRays go by many names—International Mobile Subscriber Identity catchers ("IMSI-catcher"), cell-site simulators, triggerfish[5]—and can be carried by hand, installed in a police car, or mounted on an aircraft.[6] At least sixty local and state law enforcement agencies in twenty-three states and numerous federal agencies, such as the FBI, National Security Agency, and Immigration and Customs Enforcement, own these devices.[7] StingRays operate by impersonating a cell phone tower and tricking mobile devices into connecting and revealing their

---

* Georgetown University Law Center, J.D. expected 2017. Mr. McCullough is a Featured Online Contributor for the *American Criminal Law Review*.

[1] Doug McKewlay, *The Next NSA? Police Departments Under Scrutiny for Phone, License Plate Surveillance*, FOX NEWS (May 3, 2014), http://www.foxnews.com/politics/2014/05/03/next-nsa-police-departments-under-scrutiny-for-phone-license-plate-surveillance.html.

[2] Brian L. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 MICH. L. REV. FIRST IMPRESSIONS 75, 76 (2015).

[3] Kim Zetter, *Turns out Police StingRay Spy Tools can Indeed Record Calls*, WIRED (Oct. 28, 2015), http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/.

[4] *Id.*

[5] *Id.*

[6] Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 145–46 (2013–2014).

[7] *Stingray Tracking Devices: Who's Got Them*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Feb. 18, 2016).

information.[8] These devices emit a stronger signal which overpowers nearby towers, thus forcing phones to connect as they are programmed to gravitate towards the stronger signal.[9] Since they indiscriminately cast their net over all phones within a surrounding area, these devices connect with and collect information from many phones other than the phone targeted.[10] In addition to serial numbers and locations, these devices can also intercept the content of calls, text messages, and data that a phone transmits and receives.[11]

StingRays also impact cell service. The FBI has acknowledged that a StingRay haa "the potential to intermittently disrupt cellular service to a small fraction of . . . wireless customers within its immediate vicinity."[12] This raises a concern that StingRays may interfere with important calls unrelated to the phone they are targeting. Though they are designed to recognize and allow 911 calls to connect to legitimate cell towers, non-911 emergency calls could struggle to get through if they were placed in the vicinity of a StingRay.[13]

StingRays act in a way that is substantially different than cell tower tracking—the most similar search procedure with which courts have wrestled. With cell tower tracking, when a phone is moved around it switches between different towers to maintain a connection with the strongest signal, and police can review these switches to get a rough idea of a person's movements.[14] At best, cell tower tracking can locate an area within fifty yards of a phone carrier,[15] while StingRays identify the specific location within six feet of a person.[16] Cell tower tracking involves law enforcement agencies subpoenaing phone records from third-party service carriers to approximate where a phone is located.[17] Cell tower tracking also requires assistance from the service carrier, which ensures that someone other than law enforcement is aware that surveillance is occurring and maintains records of the information used in each search.[18] StingRays do not involve any third party service carriers. The only person who necessarily knows how and why the device is being used is the StingRay operator.

---

[8] Kim Zetter, *California Police Used StingRays on Planes to Spy on Phones*, WIRED (Jan. 27, 2016), http://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/.
[9] *Id.*
[10] Zetter, *supra* note 8.
[11] Pell & Sogoian, *supra* note 6, at 146.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.* at 14.
[17] C. Justin Brown, *Stingray Devices Usher in a New Fourth Amendment Battleground*, CHAMPION 13 (2015).
[18] *Id.* at 14.

StingRays have operated largely outside of the scrutiny of the public or the courts due to law enforcement's efforts to maintain a high level of secrecy. Agencies frequently cite nondisclosure pledges made either to the FBI or the Harris Corporation,[19] which manufactures many of these devices, when refusing to disclose information.[20] This secrecy is upheld even in court proceedings, where prosecutors have made favorable plea deals or dismissed entire cases rather than disclose information about the use of StingRays.[21] This level of secrecy has made it harder for courts to determine the correct way to handle this new technology. Last year Jason Chaffetz, Chairman of the House Committee on Oversight and Government Reform, introduced a billthat would require a warrant for all levels of law enforcement.[22] Some states have already passed similar laws.[23] Though the Department of Justice recently shifted its policies to require that federal agents seek a warrant prior to using a StingRay,[24] local and state agencies may still choose to pursue other avenues of authorization.

Law enforcement agencies not required to seek warrants have authorized StingRay use under pen register or trap and trace device

---

[19] Learn more about the Harris Corporation at http://harris.com/.

[20] *See, e.g.*, Joseph Goldstein, *New York Police are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. TIMES (Feb. 11, 2016), http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html.

[21] Jason M. Weinstein et al., *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729, 742 (2015) (describing a prosecutor who offered a plea deal that was more than three years shorter than the prison sentence a defendant was entitled to in order to avoid disclosing information); Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, THE BALT. SUN (Nov. 17, 2014), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html (describing how a local prosecutor withdrew evidence obtained by phone tracking device rather than disclose information on the device).

[22] Nicky Woolf, *Congressman Introduces Bill to End Warrantless Stingray Surveillance*, THE GUARDIAN (Nov. 4, 2015), http://www.theguardian.com/world/2015/nov/04/house-bill-end-warrantless-stingray-surveillance-jason-chaffetz.

[23] Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We do while We Wait for the Supremes?*, 8 FED. CTS. L. REV. 215, 227 (2015) ("States like Indiana, Maine and Montana have already passed laws requiring state law enforcement officers to obtain a search warrant (based upon probable cause) in order to retrieve cell site information. Other states - Wisconsin, Tennessee, Minnesota, Missouri, South Carolina, Illinois (and others) - are considering similar legislation.").

[24] *The Department Announces Enhanced Policy for Use of Cell-Site Simulators*, DEPT. OF JUST. (Sept. 3, 2015), http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators ("While the department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator.").

statutes ("pen/trap application").[25] These allow agencies to petition a court to compel service providers to disclose real-time information about electronic devices they cover.[26] Pen registers are defined as devices "which [record] or [decode] dialing, routing, addressing, or signaling information" from "wire or electronic communication," and trap and trace devices are devices that "capture[] the incoming electronic or other impulses which identify the originating number . . . reasonably likely to identify the source of a wire or electronic communication."[27] The evidentiary standard for these petitions is lower than a warrant's probable cause requirement. Pen/trap applications require only a showing that "the information likely to be obtained is relevant to an ongoing criminal investigation,"[28] which has resulted in nearly all pen/trap applications being granted.[29] Many argue that pen/trap applications are not appropriate for StingRays because these statutes were designed for "the use of the primitive devices of the past that captured outgoing and incoming phone numbers on a landline."[30] StingRays are capable of grabbing far more specific data from a far larger swath of people than a traditional pen register,[31] posing a greater threat to privacy in both scope and kind.

Potential Fourth Amendment Challenges

Few courts have directly addressed the application of the Fourth Amendment to StingRays. In *United States v. Skinner*, the Sixth Circuit held that Fourth Amendment concerns were not raised when the government tracked a defendant's "pay-as-you-go" cell phone that was being used in drug trafficking.[32] Though the court explained that criminals using modern technology to reduce the possibility of detection "can hardly complain when the police take advantage of the inherent characteristics of these very devices to catch them",[33] it did not address situations where a StingRay is used to track someone's personal cell phone. Multiple federal district courts have held that pen/trap applications do not cover StingRays, implying a warrant is required to avoid Fourth Amendment violations.[34] As these types of cases become

[25] 18 U.S.C. § 3123 (2001).
[26] Pell & Sogoian, *supra* note 6, at 155.
[27] 18 U.S.C. § 3127 (3)–(4) (2009).
[28] 18 U.S.C. § 3122(b)(2) (1986).
[29] Owsley, *supra* note 2, at 81.
[30] Goldstein, *supra* note 20.
[31] Owsley, *supra* note 2, at 81.
[32] United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).
[33] *Id.* at 774.
[34] United States v. Rigmaiden, 844 F. Supp. 2d 982, 1000–01 (D. Ariz. 2012) (confirming that the government relied on a warrant, and not the pen/trap application,

more prevalent, the Court may ultimately have to definethe Fourth Amendment's applicability to StingRays. Judging from current search and seizure precedent, the use of StringRays potentially implicates the Court's interpretations of searches of a phone, a home, or a person.

The most obvious line of precedent implicated involves cases which deal with searches of cell phones. *United States v. Jones* held that attaching a GPS device to a vehicle was a search.[35] Dicta in the Court's opinion suggests that when law enforcement achieves "the same result through electronic means, without an accompanying trespass," they could cause an unconstitutional privacy invasion.[36] Furthermore, the Court held in *Riley v. California* that warrantless searches of digital information on an individual's cellphone seized during arrest was unconstitutional.[37] Though this case addressed the physical search and seizure of a phone, the use of a StingRay implies the same result. The wide array of information a StingRay can pull from all nearby cellphones when activated is the same "digital form [of] many sensitive records" and "broad array of private information" the Court protected from warrantless search in *Riley*.[38] *Riley* thus suggests that the use of StingRays also necessitates a warrant.

Moreover, the Court held in *Kyllo v. United States* that electronically monitoring the inside of a home with a thermal imaging device was a Fourth Amendment search.[39] When the government uses "a device that is not in the general public use"[40] to enter the walls of a home and discover what otherwise would remain private but for physical intrusion, the government has effected a search and must be held to the probable cause standard.[41] This suggests that a warrant is necessary for the use of StingRays since they have the possibility of invading the interior of a home. In *Kyllo*, thermal scans revealing abnormally high heat inside a house to determine where marijuana plants were being grown was considered an improper invasion.[42] Were a targeted person to be inside his or her home when a StingRay was used, the discovery of their location and communication seems to also be information protected from technologically-enhanced intrusion. This view was endorsed by the

---

for its StingRay search); *In re* the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) (denying pen/trap applications' applicability to StingRays, implying that a warrant is necessary).

[35] 132 S. Ct. 945, 946 (2012).

[36] *Id.* at 954.

[37] 134 S. Ct. 2473, 2477 (2014).

[38] *Id.* at 2491.

[39] 533 U.S. 27, 27 (2001).

[40] *Id.* at 28.

[41] *Id.* at 40.

[42] *Id.* at 27.

Supreme Court of Wisconsin in *State v. Tate*, when StingRay tracking led police to discover a person's location within his mother's home.[43] United States Supreme Court's precedent on home searches thus suggests warrantless StingRay use could violate the Fourth Amendment.

Additionally, StingRays seem to be in some sense a search of the person themselves. Cell phones have become so ubiquitous in society that the Court in *Riley* stated, "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[44] Since many people keep their phones with them at all times of the day, tracking a phone with great precision using StingRays is in a real sense tracking the physical person themselves. This observation implicates the same concerns the Court grappled with about planting GPS trackers in *Jones*,[45] leading to the conclusion that a warrant would be necessary to make this search constitutional.

Regardless of which stream of cases the Court finds to be most closely analogous, the use of StingRays addresses the same concerns with previous technologies that have led to a warrant requirement for home searches, and searches of one's physical person.

[43] 849 N.W. 2d 798, 812–13 (Wis. 2014).
[44] 134 S. Ct. at 2484.
[45] 132 S. Ct. at 946.