Cell-Site Simulators and the Fourth Amendment: Government Surveillance

Posted on 11-08-2016 Share

By: **James B. Astrachan and Christoper J. Lyon**, Astrachan Gunst Thomas, P.C.

IN JUNE 2001, THE LATE JUSTICE ANTONIN SCALIA REMARKED, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Kyllo v. U.S., 533 U.S. 27, 33–34 (2001). The Supreme Court, addressing government surveillance, confronted the question of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[1] Justice Scalia's remark resonates as soundly today as it did in pre-9/11 America, if not more so.[2]

The technology considered in Kyllo was admittedly "crude," a thermal imaging device.[3] The device enabled law enforcement, when they otherwise were unable, to observe the amount of heat emanating from inside a home.[4] The "realm of guaranteed privacy" was that of the "interior of homes,"[5] a space held "sacred" by the Fourth Amendment.[6]

Notwithstanding the rudimentary technology, Justice Scalia cautioned that "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[7] He noted that "[t]he ability to 'see' through walls and other opaque barriers is a clear, and scientifically feasible, goal of law enforcement research and development."[8] In view of this ever-advancing surveillance technology, the Supreme Court held: "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[9]

Enter the cell-site simulator, a surveillance device used by the government and within the ambit of Kyllo's rule. The device is marketed under various brand names, including "Stingray," "Hailstorm," or "Triggerfish,"[10] and can be used by police and other law enforcement groups to determine the precise location of a person's cell phone and, consequently, its owner.[11]

The device respects no boundaries or privacy and searches regardless of whether the cell phone sought is inside a home or in the pocket of a person on the street. Its search casts a wide net, analyzing all cell phones within its range until the target phone is located. Law enforcement can utilize a cell-site simulator to locate a person and to listen to his or her calls.

Law enforcement agencies have secretly used cell-site simulators for decades to track suspects.[12] The use today, however, is less of a secret.[13] As a result, privacy violations are coming to light and courts are enforcing the Fourth Amendment.[14] Criminal defendants are learning they have been the subject of Stingray searches and are moving to exclude results of the searches under the Fourth Amendment.

The Secrecy Surrounding Cell-Site Simulators

The privacy implications, once it is understood how these devices work, become apparent. Yet information about these devices has been difficult to obtain because the government and its contractors have employed non-disclosure agreements to make it difficult for the public to learn of even the mere existence of the devices.

The Baltimore Police Department (BPD) is an example. As a condition to selling or transferring the device to the BPD, the Federal Bureau of Investigation (FBI) in 2011 required both the BPD and the Office of the State's Attorney for Baltimore City to sign a non-disclosure agreement with the FBI.[15]

Baltimore is not unique. The news reports similar nondisclosure agreements entered into by law enforcement agencies seeking to purchase cell-site simulators.[16] The American Civil Liberties Union has identified 66 agencies in 24 states and the District of Columbia that have purchased cell-site simulators.[17] Presumably, these buyers, like the BPD and the Baltimore City state's attorney, have also entered into non-disclosure agreements.

Typically, the terms of a non-disclosure agreement prohibit the acting law enforcement agency from disclosing any information about the device to the public and to judges, defense lawyers, and juries.[18] A typical agreement provides:

In order to ensure that such wireless collection equipment/ technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including by [sic] not limited to: in press releases, in court documents, during judicial hearings, or during other public forums or proceedings.[19]

In addition to the restrictions already set forth, the nondisclosure agreement prohibits disclosure of the equipment by law enforcement "in search warrants and related affidavits" and "in response to court ordered disclosure."[20] Incredibly, the FBI, through the non-disclosure agreement, reserves to itself a right to require that a state's attorney "seek dismissal of the case" in lieu of disclosing any information relating to cellsite simulators.[21] Thus, to maintain the secrecy of this search equipment, even from judges, the FBI—an arm of the federal government—can require an elected state's attorney to dismiss a case.

As a result of the secrecy imposed on members of local government and their enforcement arms, information about the use and functioning of cell-site simulators has been difficult to come by. But, through public records requests and litigation efforts such information is beginning to surface.

How Cell-Site Simulators Function

In 2008, a Freedom of Information Act request yielded production of documents from the Executive Office for United States Attorneys including portions of an Electronic Surveillance Manual.[22] The pages produced from the manual addressed the cell-site simulator device, which was also referred to as a "digital analyzer" and a "triggerfish."[23]

The manual describes in general terms how a cell-site simulator functions. It explains that cell phones, when turned on, as "a necessary aspect of cellular telephone call direction and processing," continuously transmit "cell site data" to the cellular network provider's nearest cell tower, also known as a "cell site."[24] "Cell site data," it explained, includes the cell phone's telephone number, known as its "mobile

identification number," its "electronic serial number" and "the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting."[25]

Taking advantage of this functional feature of cell phones, a cell-site simulator "can electronically force a cellular telephone to register its mobile identification number (MIN, i.e., telephone number) and electronic serial number (ESN, i.e., the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on."[26] The device does this by simulating or mimicking a service provider's cell tower causing all cell phones within the simulator's range, including those of people unrelated to the investigation, to transmit to the simulator until the target phone is located.[27] By forcing connections from all cell phones within the device's range, the cell-site simulator obtains cell site data from those phones, including telephone numbers, and then homes in on the target phone to locate that phone based on the strength of its signal.[28] Law enforcement, with knowledge of the surveillance target's telephone number, can use the device to locate the target. Cellsite simulators are portable and can be mounted on vehicles or drones or carried by a person.[29]

The Executive Office for United States Attorneys advises that cell-site simulators also "may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function."[30] Indeed, one document produced in response to an information act request reads, "With very little additional effort, the 'triggerfish' can also intercept the conversations taking place on a particular cellular telephone."[31] Manufacturers of the device boast that cell-site simulators are able to read incoming and outgoing text messages.[32]

Notwithstanding the information available in 2008 about the general functionality of cell-site simulators, courts have only recently begun to scrutinize the technology and consider the implications on privacy rights.[33] The lateness of the inquiry should come as no surprise given that non-disclosure agreements have obstructed the ability of law enforcement from revealing to judges even the mere existence of the device.

The Maryland Court of Special Appeals, Maryland's intermediate appellate court, reacted. "A nondisclosure agreement that prevents law enforcement from providing details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion made in a proper manner and 'justified by the circumstances,' obstructs the court's ability to make the necessary constitutional appraisal."[34] A not-so-pleased court said:

We perceive the State's actions in this case to protect the Hailstorm technology, driven by a nondisclosure agreement to which it bound itself, as detrimental to its position and inimical to the constitutional principles we revere.[35]

Fourth Amendment Privacy Implications Posed by Cell-Site Simulators

Among other protections, the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion."[36]

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[37]

The Framers were determined "that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant."[38]

When considering whether government surveillance implicates privacy rights secured by the Fourth Amendment, the first question to be posed and answered is whether the surveillance technique at issue constitutes a search under the Fourth Amendment. If the answer is affirmative, "[t]he Fourth Amendment generally requires police to secure a warrant before conducting a search"[39] as "warrantless searches are presumptively unconstitutional."[40]

The Supreme Court emphasizes that "the Fourth Amendment protects people, not places."[41] Whether a Fourth Amendment search has occurred, therefore, requires more than simply determining where or how police looked (e.g., inside a home from a window or in a backyard from an airplane), although those inquiries are relevant. The primary focus is whether the government's surveillance "violates a subjective expectation of privacy that society recognizes as reasonable."[42]

Cell-site simulators enable law enforcement officers to gather, employ, and reveal private information about people, information in which there are reasonable expectations of privacy. This protected information includes:

- Private details behind the walls of a person's home
- Content of a person's communications
- Data stored on a person's cell phone
- A person's real-time, or present moment, cell phone location

Each time law enforcement uses a cell-site simulator to obtain, gather, employ, or reveal one or more items of protected information, it has conducted a search that implicates privacy interests protected by the Fourth Amendment. Before turning to each of these privacy interests, however, a more specific concern posed by these devices arises—namely, whether their use is ever constitutional, even with a warrant.

General Warrants Prohibited

In Colonial America, "writs of assistance" or "general warrants" granted officers of the Crown "blanket authority to search where they pleased for goods imported in violation of the British tax laws."[43] These "hated writs of assistance" were "[v]ivid in the memory of the newly independent Americans."[44] The general warrants were denounced "because they placed 'the liberty of every man in the hands of every petty officer.'"[45] The U.S. Supreme Court recognizes "that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era."[46]

A cell-site simulator forces the target phone of the suspect under investigation to communicate with the simulator and reveal identifying information, and at the same time it forces all cell phones within its range of operation to reveal identifying information and sorts through that information in search for the target phone.[47]

Consider the facts of *U.S. v. Lambis*.[48] Drug Enforcement Administration (DEA) agents, as part of their investigation into an international drug-trafficking organization, sought to locate a suspect's cell phone.[49] Through records obtained from the service provider specific to the target phone, the agents were able to determine that the phone was located in New York City "in the general vicinity" of Washington Heights

near 177th and Broadway.[50] The DEA was unable to use the records received from the cell phone provider to precisely locate the phone within any of the apartment houses in the area, much less within a specific apartment.[51]

To locate the phone, the DEA agents used a cell-site simulator.[52] A government technician began the search by activating the device at "the intersection of 177th Street and Broadway,"[53] a bustling intersection densely populated with apartment buildings and businesses. The simulator caused all cell phones in the vicinity to transmit identifying information to the device.[54] It did not matter if the phones were in homes, offices, purses, or pockets.

The search led the technician to an apartment building where he "walked the halls until he located the specific apartment where the signal was strongest."[55] The government agents knocked, asked for and obtained permission to enter, and discovered drug paraphernalia.[56]

The cell-site simulator enabled the agents to penetrate the walls of the defendant's apartment, and those of countless other apartments and private places where cell phones were located, until the target phone was found.

Under these circumstances, it is difficult to conceive how any warrant authorizing use of a cell-simulator could "particularly" describe a place to be searched as required by the Fourth Amendment and avoid granting an "unbridled authority of a general warrant."[57]

Privacy of the Home

In *Lambis* the court recognized that use of a cell-site simulator revealed details about the interior of defendant's apartment— namely, that the cell phone was located therein.[58] This, the court held, "was an unreasonable search."[59] The agents had not obtained a warrant to use the device, so the fruit of their illegal search, the drug paraphernalia found inside the apartment, was suppressed.[60]

A similar outcome resulted in the case of State v. Andrews,[61] where law enforcement used a cell-site simulator without a warrant to locate the cell phone of a suspect.[62] The device enabled a detective to locate the phone, and the suspect, inside one of approximately 30 to 35 apartments.[63] That use, the appellate court held, "is undoubtedly an intrusion that rises to the level of a Fourth Amendment 'search.'"[64]

Privacy of Communications

When used to intercept communications, including conversations and text messages, a cell-site simulator implicates a second privacy interest protected by the Fourth Amendment—one's expectation that the government will not electronically eavesdrop on private conversations.

Charles Katz was convicted of illegal gambling over 50 years ago.[65] To obtain that conviction, the government placed an electronic recording device on the outside of a public telephone booth from which Mr. Katz placed his calls.[66] The government agents were careful to only record Mr. Katz's conversations, which occurred approximately the same time each morning.[67] The recordings obtained led to Mr. Katz's conviction.[68]

In overturning his conviction, the U.S. Supreme Court held that the electronic surveillance employed by law enforcement violated Katz's Fourth Amendment rights.[69] "The Government's activities in electronically listening to and recording the petitioner's words," Justice Potter Stewart explained, "violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[70]

So far, there have been no cases reported where a cell-site simulator has been used to intercept communications without a warrant. Use of a cell-site simulator to do so without a warrant, whether to intercept conversations or text messages, would undoubtedly be a search and seizure prohibited by the Fourth Amendment. The Executive Office of United States Attorneys acknowledges as much, advising that if law enforcement has not obtained a warrant, cell-site simulators "must be configured to disable the interception function."[71] Cell phone users, thus, are left to trust that the technician using the cell-site simulator heeds this advice.

Privacy of Data Contained on a Cell Phone

To locate a cell phone, a cell-site simulator forces all cell phones within the range of the device's operation to disclose identifying information stored on the phone, including the telephone number of each phone. This ability implicates yet another privacy interest protected by the Fourth Amendment.

In *Riley v. California*, the U.S. Supreme Court considered "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[72] The Justices answered no and held that for "searches of data on cell phone . . . officers must generally secure a warrant before conducting such a search."[73] The only exception to this requirement would be if "exigent circumstances" require an immediate search of the phone, for instance, if police are truly confronted with a situation where data on the phone evidencing a crime "will be the target of an imminent remote-wipe attempt."[74]

In *Riley*, the government, after detaining a suspect and his phone, searched the data on the cell phone without a warrant and revealed a telephone number identified as "my house" on a contacts list stored on the phone."[75] Using that telephone number, officers located defendant's apartment through a listing in a phone directory.[76] They then obtained a warrant to search the apartment and found 215 grams of crack cocaine and other contraband.[77] Because the evidence stemmed from the illegal search of data on defendant's cell phone, it was excluded and not allowed to be offered against him at trial.[78]

Like the illegal search in *Riley*, law enforcement's use of a cell-site simulator to search and retrieve data directly from cell phones, including the cell phone's number, implicates a privacy right protected by the Fourth Amendment. Specifically, people have a reasonable expectation that the data contained on their cell phone is and shall remain private. So when law enforcement, like it did in the Andrews case, uses a cell-site simulator to force a phone to share its data, they perform a search "subject to the warrant requirement regardless of [the cell phone's] location."[79]

The Supreme Court explained, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated" by searches of physical items like wallets or purses.[80] "[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[81] "With all they contain and

all they may reveal, they hold for many Americans 'the privacies of life,'" and "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[82]

Privacy of Real-Time Cell Phone Location Information

For a cell-site simulator to locate a person, or his cell phone, the law enforcement technician causes the device to surreptitiously force the person's cell phone to transmit its signal to the device and causes the targeted cell phone to act as a tracking device.[83] This enables law enforcement the ability both to locate *and* track the phone and its owner in real-time. This implicates yet another privacy interest protected by the Fourth Amendment.

In *U.S. v. Jones*, the U.S. Supreme Court held that installation of a GPS device on a vehicle and use of that device to monitor the vehicle's movements constitute a search under the Fourth Amendment.[84] While the majority opinion in *Jones* did not base its decision on a finding that the government had invaded a privacy interest,[85] two concurring opinions involving five of the Justices agreed that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[86]

Justice Sonia Sotomayor explained that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[87] She questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[88]

In *Andrews*, the Maryland Court of Special Appeals held that people do not expect the government to intimately watch them.[89] There, the court observed that "[c]ell site simulators, such as Hailstorm, can locate and track the movements of a cell phone and its user across both public and private spaces."[90] It admonished that "[u]nchecked, the use of this technology would allow the government to discover the private and personal habits of any [cell phone] user."[91] It therefore concluded "that people have a reasonable expectation of privacy in real-time cell phone location information."[92] Simply put, the Fourth Amendment prohibits the government from using a cell-site simulator to convert a person's cell phone into a tracking device.[93] For reasons not publicly disclosed, the state's attorney's office decided against appealing this ruling to the Maryland Court of Appeals.

Conclusion

The government's use of modern technologies to track and monitor suspects is nothing new. Telephone lines were tapped starting in 1890, soon after the telephone was invented.[94] Now cell-site simulators are being used to make cell phones communicate private information to law enforcement.

There are protections in place like those provided by the Fourth Amendment that check how far the government can go. Without a warrant, for example, the inside of a home is off limits.

As in the *Andrews* and *Lambis* cases, courts are recognizing that the government's use of cell-site simulators implicates several established privacy rights protected by the Fourth Amendment. For example, without a warrant, law enforcement may not use a

device that enables officers to explore the details of the interior of a home. This prohibition was established back in 2001 when the *Kyllo* case was decided. A cell-site simulator is such a device.

After decades of using these devices, only recently in September 2015, after numerous reports of the secret use of cell-site simulators, the U.S. Department of Justice changed course requiring that its agents "must now obtain a search warrant supported by probable cause before using a cellsite simulator."[95] This new policy, however, only concerns federal law enforcement agents, not the numerous state law enforcement agencies that have obtained cell-site simulators by signing non-disclosure agreements.

It remains to be seen whether local law enforcement agencies will follow the federal government's lead and require officers to obtain warrants before deploying cell-site simulators.

James B. Astrachan is a principal in the Astrachan Gunst Thomas, P.C. law firm in Baltimore, Maryland. He is coauthor of **The Law of Advertising**, *a six-volume treatise published by Matthew Bender LexisNexis since 1972. He is a practicing intellectual property attorney and a long-time adjunct law professor at the University of Maryland Francis King Carey School of Law and the University of Baltimore School of Law.* **Christopher J. Lyon** *is a principal in the Astrachan Gunst Thomas, P.C. law firm in Baltimore, Maryland. He is a trial attorney who counsels businesses on intellectual property and commercial disputes as well as employment matters and privacy rights.*

---

1. *Kyllo*, 533 U.S. at 34. **2.** *See, e.g.*, Hina Shamsi & Alex Abdo, *Privacy and Surveillance Post-9/11*, ABA Human Rights, Winter 2011, at 5, 17; Bob Barr, *Post-9/11 Electronic Surveillance Severely Undermining Freedom*, 41 Val. U. L. Rev. 1383 (2007). **3.** 533 U.S. at 36, 38. **4.** Using the device, law enforcement observed that the side wall of a home and the roof over the home's garage were substantially warmer than the rest of the home and neighboring homes. Law enforcement concluded that the homeowner was using halide lights to grow marijuana in his house. Based in part on the information gathered from the thermal imaging device, law enforcement obtained a warrant to search the house. *Id.* at 29–30. **5.** *Id.* at 34. **6.** Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013) (quoting Entick v. Carrington, 2 Wils. K.B.275, 291, 95 Eng. Rep. 807, 817 (K.B. 1765)). **7.** *Kyllo*, 533 U.S. at 36. **8.** *Id.* at 36 n. 3 (citing website for the National Law Enforcement and Corrections Technology Center). **9.** *Id.* at 40. **10.** U.S. v. Lambis, No. 15cf734, p. 2 (S.D.N.Y. July 12, 2016) (Cell-site simulators have been "referred to as a 'Stingray,' 'Hailstorm,' or 'TriggerFish'."). **11.** Chief Justice John Roberts of the Supreme Court observed that modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Riley v. California, 134 S. Ct. 2473, 2483 (2014). He notes one survey reporting that "nearly three-quarters of smart phone users report being within 5 feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Id.* at 2490. **12.** *See* 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, 19 (2014). **13.** *Id.* at 39–40. **14.** *See* State v. Andrews, 227 Md. App. 350 (2016) (state appellate court affirming trial court's suppression of evidence obtained from use of cell-site simulator); *U.S. v. Lambis*, No. 15cf734 (S.D.N.Y. July 12, 2016) (federal district court excluding evidence obtained from use of cell-site simulator). **15.** *Non-Disclosure Agreement*, The Baltimore Sun (July 13, 2011), http://www.baltimoresun.com/bal-police-stingray-non-disclosureagreement-20150408-htmlstory.html (http://www.baltimoresun.com/bal-police-stingray-non-disclosureagreement-20150408-htmlstory.html). **16.** *See, e.g.*, Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, The New York Times, (February 11, 2016), http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=2 (http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-

cellphone-tracking-stingrays.html?_r=2); Bruce Vielmetti, *Groups Decry Milwaukee Police's Warrantless Use of 'Stingray' Tracking*, Journal Sentinel, (February 1, 2016), http://www.jsonline.com/news/crime/groups-decry-milwaukee-polices-warrantless-use-of-stingray-tracking-b99660842z1-367246261.html (http://www.jsonline.com/news/crime/groups-decry-milwaukee-polices-warrantless-use-of-stingray-tracking-b99660842z1-367246261.html); Kyle Scott Clauss, *Boston Police Confirms It Uses Controversial 'StingRay' Cell Phone Trackers*, Boston Magazine, (November 20, 2015), http://www.bostonmagazine.com/news/blog/2015/11/20/boston-police-cell-phone-trackers/ (http://www.bostonmagazine.com/news/blog/2015/11/20/boston-police-cell-phone-trackers/); Jeremy Seth Davis, *D.C. Police Sign Non-disclosure with FBI to Keep StingRay Use Private*, SC Magazine, (October 2, 2015), http://www.scmagazine.com/fbi-dc-police-sign-agreement-over-stingray-use/article/442695/ (http://www.scmagazine.com/fbi-dc-police-sign-agreement-over-stingray-use/article/442695/); Jody Callahan & Yolanda Jones, *Memphis Police Silent on Cell Phone Eavesdropping Technology*, The Commercial Appeal (September 22, 2015), http://www.commercialappeal.com/news/crime/memphis-police-silenton- cell-phone-eavesdropping-technology-205696be-3f2f-0f31-e053-0100007ff92f-328726871.html (http://www.commercialappeal.com/news/crime/memphis-police-silenton-%20cell-phone-eavesdropping-technology-205696be-3f2f-0f31-e053-0100007ff92f-328726871.html); Glenn E. Rice, *Secret Cellphone Tracking Device Used By Police Stings Civil Libertarians*, The Kansas City Star, (September 5, 2015) http://www.kansascity.com/news/business/technology/article34185690.html (http://www.kansascity.com/news/business/technology/article34185690.html); Paul Ingram, *Feds Now Required to Get Warrants for Stingray Surveillance*, Tucson Sentinel. com (September 4, 2015, 12:05 PM), http://www.tucsonsentinel.com/local/report/090415_doj_stingray/feds-now-required-get-warrants-stingray-surveillance/ (http://www.tucsonsentinel.com/local/report/090415_doj_stingray/feds-now-required-get-warrants-stingray-surveillance/); *St. Louis Prosecutors Drop Charges Before Spy Tool Used in Arrests is Revealed in Court*, RT Question More (April 20, 2015, 7:27 PM), https://www.rt.com/usa/251345-missouri-stingray-charges-dropped/ (https://www.rt.com/usa/251345-missouri-stingray-charges-dropped/); *Judge orders Sheriff's Office in New York to Disclose Stingray Secret Surveillance Documents*, RT Question More (March 18, 2015, 5:48 PM), https://www.rt.com/usa/241937-erie-county-stingray-surveillance/ (https://www.rt.com/usa/241937-erie-county-stingray-surveillance/); Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Washington Post, (February 22, 2015), https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipmentproves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html (https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipmentproves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html); Brendan Keefe, *The Investigators: Police Could Be Secretly Tracking Your Phone*, WXIA-TV (November 5, 2014), http://phxux.11alive.com/story/news/local/investigations/2014/11/03/investigators-police-could-be-secretly-tracking-your-phone/18446075/ (http://phxux.11alive.com/story/news/local/investigations/2014/11/03/investigators-police-could-be-secretly-tracking-your-phone/18446075/); Fred Clasen-Kelly, *Charlotte Police Investigators Secretly Track Cellphones*, The News & Observer (October 18, 2014, 9:17 PM), http://www.newsobserver.com/news/local/crime/article10100405.html (http://www.newsobserver.com/news/local/crime/article10100405.html); John Anderson, *APD: Can We Please Buy Some Top-Secret "StingRays"?*, The Austin Chronicle (October 17, 2014), http://www.austinchronicle.com/news/2014-10-17/apd-can-we-please-buy-some-top-secret-stingrays/ (http://www.austinchronicle.com/news/2014-10-17/apd-can-we-please-buy-some-top-secret-stingrays/); *Fbi Forces Police Departments Across the Us to Keep Quiet About Cellphone Spying Gear*, RT Question More, (September 23, 2014, 5:48 PM), https://www.rt.com/usa/189996-fbi-fcc-nda-stingray/ (https://www.rt.com/usa/189996-fbi-fcc-nda-stingray/); Jennifer Portman, *FDLE Signed Stingray Deal*, Tallahassee Democrat, (March 30, 2014),

http://www.tallahassee.com/story/news/local/2014/03/30/fdle-signed-stingray-deal-/7073639/ (http://www.tallahassee.com/story/news/local/2014/03/30/fdle-signed-stingray-deal-/7073639/). **17.** American Civil Liberties Union, *Stingray Tracking Devices: Who's Got Them?*, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited July 21, 2016). **18.** *Non-Disclosure Agreement*, The Baltimore Sun at pp. 1–2. (July 13, 2011), http://www.baltimoresun.com/bal-police-stingray-non-disclosure-agreement-20150408-htmlstory.html (http://%20www.baltimoresun.com/bal-police-stingray-non-disclosure-agreement-20150408-htmlstory.html). **19.** *Id.* **20.** *Id.* at p. 2. **21.** *Id.* at p. 3. **22.** *See* Interim Reply of Executive Office for United States Attorneys to Request Number 07-4130 pp. 9-12, 17 (August 12, 2008), https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf). **23.** *Id.* at p. 17. **24.** *Id.* **25.** *Id.* **26.** *Id.* **27.** U.S. v. Lambis, No. 15cf734, p. 2 (S.D.N.Y. July 12, 2016). **28.** Interim Reply of Executive Office for United States Attorneys to Request Number 07-4130 pp. 10, 17 (August 12, 2008), https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf). ("the screen of the digital analyzer/cell site simulator/triggerfish would include . . . the cell site number/sector (location of the cellular telephone when the call was connected)"); U.S. v. Lambis, No. 15cf734, p. 2 (S.D.N.Y. July 12, 2016) (the cell-site simulator "calculates the strength of the 'pings' until the target phone is pinpointed"); *Andrews*, 227 Md. App. at 359 n. 4 ("True to its brand name, the Hailstorm device generates an electronic barrage that impacts all the mobile devices within its range.") **29.** Pell & Soghoian, *supra* note 12, at p. 16. **30.** Interim Reply of Executive Office for United States Attorneys to Request Number 07-4130 p. 17 (August 12, 2008), https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf. **31.** *Id.* at p. 35. **32.** Pell & Soghoian, *supra* note 12, at pp. 11–12. **33.** *See Andrews*, 227 Md. App. 350 (2016); *U.S. v. Lambis*, No. 15cf734 (S.D.N.Y. July 12, 2016). **34.** *Andrews*, 227 Md. App. at 376. **35.** *Id.* at 377. **36.** *Katz*, 389 U.S. at 350. **37.** U.S. Const. amend. IV. **38.** Stanford v. State of Tex., 379 U.S. 476, 509-510 (1965). **39.** Maryland v. Dyson, 527 U.S. 465, 466 (1999); *see also Kyllo*, 533 U.S. at 40. **40.** *Kyllo*, 533 U.S. at 32. **41.** Katz v. U.S., 389 U.S. 347, 351 (1967). **42.** *Kyllo*, 533 U.S. at 33 (citing *Katz*, 389 U.S. at 353 (Harlan, J., concurring)). **43.** *Stanford*, 379 U.S. at 510. **44.** *Id.* **45.** *Id.* **46.** *Riley*, 134 S. Ct. at 2494. **47.** *Andrews*, 227 Md. App. at 359 n. 4 (citing Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), *available at* https://www.justice/gov/opa/file/767321/download [https://perma.cc/k99L-H643]). **48.** No. 15cf734 (S.D.N.Y. July 12, 2016). **49.** *Id.* at 1. **50.** *Id.* **51.** *Id.* at 1-2. **52.** *Id.* at 2. **53.** *Id.* **54.** *Andrews*, 227 Md. App. at 359 n. 4 (citing Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), *available at* https://www.justice/gov/opa/file/767321/download [https://perma.cc/k99L-H643]). **55.** No. 15cf734, 2 (S.D.N.Y. July 12, 2016) **56.** *Id.* **57.** *Stanford, 379 U.S. at 509–510.* **58.** *No. 15cf734, p. 4 (S.D.N.Y. July 12, 2016)* **59.** *Id.* **60.** *Id. at 6, 14.* **61.** *227 Md. App. 350.* **62.** *Id. at 354.* **63.** *Id. at 359.* **64.** *Id. at 393.* **65.** *Katz v. U.S., 389 U.S. at 348.* **66.** *Id.* **67.** *Id. at 354.* **68.** *Id. at 359.* **69.** *Id. at 353.* **70.** *Id.* **71.** *Interim Reply of Executive Office for United States Attorneys to Request Number 07-4130 (August 12, 2008), https://www.aclu.org/files/pdfs/ (https://www.aclu.org/files/pdfs/) freespeech/cellfoia_release_074130_20080812.pdf, p. 17.* **72.** *134 S. Ct. 2473, 2480 (2014).* **73.** *Id. at 2485.* **74.** *Id. at 2487.* **75.** *Id. at 2481.* **76.** *Id.* **77.** *Id.* **78.** *Id. at 2495.* **79.** *Andrews, 227 Md. App. at 389 (citing Riley, 134 S.Ct. at 2489–91).* **80.** *Id. at 2488–2489.* **81.** *Id. at 2490.* **82.** *Id. at 2494–2496 (quoting Boyd v. U.S., 116 U.S. 616, 630 (1886)).* **83.** *Andrews, 227 Md. App. at 348; U.S. v. Lambis, No. 15cf734, p. 6 (S.D.N.Y. July 12, 2016).* **84.** *132 S. Ct. 945, 949 (2012).* **85.** *Instead, the majority opinion held that the government committed a trespass by placing the GPS device onto the vehicle. By trespassing, a search under the Fourth Amendment occurred because "[t]he Government physically occupied private property for the purpose of obtaining information." 132 S. Ct. at 949.* **86.** *Id. at 964 (Alito, J., concurring).* **87.** *Id. at 955 (Sotomayor, J., concurring).* **88.** *Id.* **89.** *Andrews, 227 Md. App. at 391.* **90.** *Id.* **91.** *Id.* **92.** *Id. at 393.* **93.** *Andrews, 227 Md. App. at 327 ("We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices"); U.S. v. Lambis, No. 15cf734, p. 6 (S.D.N.Y. July 12, 2016) ("[T]*

he Government may not turn a citizen's cell phone into a tracking device.") 94. William Lee Adams, Brief History: Wiretapping, Time, Oct. 11, 2010, http://content.time.com/time/magazine/article/0,9171,2022653,00.html (http://content.time.com/time/magazine/article/0,9171,2022653,00.html). 95. Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, Dep't of Justice (Sept. 3. 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators (https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators).