

# StingRay Devices Usher in a New Fourth Amendment Battleground

On a clear day in March 2014, just after noon, an unmarked police van was parked near the 3800 block of Chatham Avenue in West Baltimore.

The officers inside the van were focused on a large yellow house, which was cut up into several separate apartment units. The police believed that one of the units was the home of the man they were after: a suspect in a murder-for-hire plot. The problem was, they did not know which apartment was his.

Rather than obtain a warrant, or knock on each of the doors in sequence, the officers in the van did something much more convenient. They flipped the switch of an electronic device, roughly the size of a briefcase, and watched the results on a computer screen.

The device, known as a cell site simulator, emitted a radio signal that penetrated the walls of the house and activated the suspect's phone. The phone was essentially tricked into thinking it was communicating with a cellular tower. The phone then sent a signal back to the cell site simulator, revealing to police critical information: the phone number, the phone's serial number, and, most importantly on this day, the precise location of the phone inside the building.

Now able to pinpoint their suspect, the police entered the house, went directly to apartment number four, and arrested the man they had been tracking. That man now resides in a Bureau of Prisons facility.

## A New Battleground

Arguably, there is no police technology that is more commonly used — while at the same time more shrouded in mystery — than the technology that is employed in a cell site simulator. Manufactured by the Harris Corporation under the name "StingRay," these devices occupy the latest battleground in the struggle between police investigatory tactics and the Fourth Amendment. While few courts have thoroughly explored the legal implications of cell site simulators, it seems inevitable that they will be the subject of extensive litigation in the coming years.

At least 52 law enforcement agencies around the country are using the devices, which cost roughly $100,000 per unit, according to the ACLU, which is closely monitoring and litigating the use of cell site simulators.[1] Anecdotally, their use is pervasive in metropolitan areas, where police have special technology units that use the devices in investigations ranging from stolen cell phones to murders. In Baltimore, the extent of the use of cell site simulators was secret until last month, when a detective testified that Baltimore City police officers have used the device over 4,300 times since 2007.[2]

BY C. JUSTIN BROWN AND KASHA M. LEESE

The 4,300 figure is staggering compared to the numbers released by other jurisdictions: the Florida Department of Law Enforcement said its officers have used the device approximately 1,800 times; police in Baltimore County, Md., said that they have used it 622 times; police in Tallahassee, Fla., said that they have used it more than 250 times; and police in Tacoma, Wash., said that they have used it about 170 times.[3]

According to Jeanine Meckler, a public defender in Baltimore who has litigated a StingRay case, the devices started popping up in criminal cases around 2011. Today, she said, "they're using it far more than we realize."

Cell site simulators should be troubling to defense attorneys, and civil libertarians, for multiple reasons. First, without proper authorization, they likely amount to a Fourth Amendment search of an individual's person, phone, and possibly home. Second, cell site simulators do not engage only target phones; they engage every phone within a certain radius of the device, whether intended or not. And finally, the use of this technology is often justified by confusing pen register and trap-and-trace orders, which most judges do not understand, and which really should not apply to StingRays.

Making matters worse, law enforcement officers — both federal and local — are going to great lengths to keep the use of these devices secret. Just a few months ago in a Baltimore City Circuit Court robbery trial, a police officer refused to answer defense counsel's questions about a cell site simulator and how it led to the recovery of a stolen phone. The judge seemed to be furious and threw out the evidence — the cell phone. The exclusion of the phone was a major factor in obtaining a hung jury for the defendant. The exchange, at a suppression hearing, went as follows:

> **Defense:** Officer, what information did you have?
>
> **Police Officer:** Ma'am?
>
> **Prosecutor:** Your Honor, this goes to the State's motion *in limine*.
>
> **The Court:** No, this goes to why he was stopped. It's a simple question. Why was he stopped? What was the, it was a warrantless arrest. Why was he stopped? That's the question she's asked. He can answer the question. Why did you stop him?
>
> **Police Officer:** This kind of goes into Homeland Security issues, Your Honor.
>
> **The Court:** Okay, if it goes into Homeland Security issues, then the phone doesn't come in. Okay. Step down, thank you. I mean this is simple. You can't just stop someone and not give me a reason, State, and you know that. …[4]

While the officer quoted above indicated that his secret was a matter of national security, more commonly police are hiding behind nondisclosure agreements that the manufacturers require. According to the *New York Times*, a journalist in Tucson recently obtained a copy of a nondisclosure agreement, and it stated that the city "shall not discuss, publish, release, or disclose any information pertaining to the product … [w]ithout the prior written consent of Harris."[5] In April 2015, the Baltimore Police Department's nondisclosure agreement was presented for the first time in court.[6] The agreement prohibits disclosure of the existence of the technology to the public, judges and lawmakers, and directs the state to dismiss cases at the request of the FBI, in lieu of providing information about cell site simulators.[7] In the agreement, the FBI claims that disclosure about the technology would render it essentially useless for criminal and national security investigations.[8] In some instances, even the actual nondisclosure agreements are kept secret.

Before defense attorneys can fight cell site simulators in court, they must be able to recognize that one was used by law enforcement. This can be a challenge because one thing is sure: nobody is going to volunteer this information. Rather, a defense attorney will have to develop a full understanding of how law enforcement located the defendant, and eliminate alternative methods. Doing this requires knowledge of how cell site simulator technology works.

## How It Works

To understand how a cell site simulator works — and to be able to identify whether law enforcement used one in a particular case — it is necessary to have a basic understanding of other types of cellphone tracking, specifically cell tower tracking and GPS tracking.

Cell tower tracking (cell site location information) is commonly used by law enforcement. It allows officers to subpoena historical phone records from third-party carriers (usually without a warrant) and use those records to approximate where a cell phone was located, as long as the phone was turned on. All cellphones communicate periodically with base towers by sending pulses — usually to the closest tower emitting the strongest signal. As the phone moves, and as signal strength varies, the phone uses different cell towers. By plotting the locations of these different cell towers, it is possible to learn an approximate location of an individual (as long as the individual was in possession of the cellphone). The most obvious weakness of this system is that it is imprecise — at best it can locate within roughly 50 yards.

Global Positioning System (GPS) tracking is a superior type of tracking. The system works through GPS satellites in space and can track a device with great precision. The problem with GPS, from the perspective of law enforcement, is that it generally requires a warrant, and it requires the planting of a device on a target (such as a car). Although most modern cellphones come with GPS capability, police generally do not have access to this.

A cell site simulator, also known as a StingRay, KingFish, IMSI catcher,[9] triggerfish, or digital analyzer,[10] is a technology that can locate the source of a cellular signal without going through the wireless carrier. The technology mimics a carrier's cellphone towers and measures the strength of the cellular signal from several locations. Essentially, it masquerades as a wireless carrier's base station and electronically forces all cellphones in the area to communicate with it as if it were the carrier's base station.[11] By using cell site simulators, police can locate, interfere with, and intercept communications from cellphones and other wireless devices.[12]

The Department of Justice Electronic Surveillance Manual describes the capabilities of cell site simulators:

> The equipment includes an antenna, an electronic device that processes the signals transmitted on cellphone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360-degree display) and signal strength of a particular cellphone while the user is making a call. By shifting the location of the device,

> the operator can determine the phone's location more precisely using triangulation.[13]

The Manual also explains the various benefits to law enforcement agencies of using cell site simulators:

> If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected). … [Cell site simulators] and similar devices may be capable of intercepting the contents of communications[.][14]

Police can also use cell site simulators to determine a phone's location if they know the target cellphone's IMSI. The IMSI is programmed into the cell site simulator, which then sorts through the signaling data (including location) of cellphones in the area until it finds a match.

Cell site simulators vary from carrier requests in at least two important ways. First, cell site simulators can typically be used without carrier assistance. With carrier-assisted surveillance, the carrier necessarily has knowledge that the surveillance is taking place and has copies of the records it discloses at the request of law enforcement pursuant to a traditional pen register/trap and trace order. By bypassing the carrier and using a cell site simulator, only the operator of the device (i.e., law enforcement) has knowledge that an interception ever took place and has access to the intercepted information. To the extent that carriers may be able to act as a proxy for their customers' privacy interests and push back against some law enforcement requests, no such advocates exist when a cell site simulator is used.

Second, cell site simulators produce extremely precise location information, in some cases within an accuracy of approximately six feet.[15] In one federal case, the government conceded that the cell site simulator located the defendant's wireless device precisely within a specific apartment in an apartment complex.[16] In Florida, Tallahassee police testified that by "using portable equipment" and going to "every door and window" in a large apartment complex, they were able to identify the "particular area of the apartment that the handset was emanating from."[17]

Cell site simulators can perform many different functions; some are capable of capturing the content of communications, such as voice calls and text messages, although law enforcement officials maintain that they disable these functions.[18] As discussed above, the full scope of capabilities is unknown because manufacturers have vigilantly guarded their products' specifications through nondisclosure agreements.

## Fourth Amendment Concerns

Although no court has specifically reached this question, it is likely that the use of a cell site simulator constitutes a Fourth Amendment search. This is rooted in some old Supreme Court law — *United States v. Karo*[19] — and some new Supreme Court law — *Kyllo v. United States*,[20] *United States v. Jones*,[21] and *Riley v. California*.[22] Depending on how the device is used, it could amount to a search of a person, a person's cellular phone, or a person's home.

### a. The Search of a Home

The Supreme Court addressed electronic monitoring inside a home in *Karo* and found that it was unconstitutional without a warrant.[23] Government agents had installed a beeper in a container of ether that was delivered to the defendant. They then used the beeper monitor to determine that the ether was in the defendant's residence, and they used this information to obtain a warrant to search the residence.[24] The Court explained that, while the agents' monitoring of the beeper was less intrusive than a full-scale search of the home, it did "reveal a critical fact about the interior of the premises that the government is extremely interested in knowing and that it could not have obtained without a warrant[:]" that the ether was actually located in the defendant's house.[25]

Further, in deciding that the government was required to obtain a warrant to monitor the beeper, the Court rejected several arguments by the government:

> [We] reject the government's contention that it would be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime … will be committed[.] … If agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, the government argues, for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises. The argument that a warrant requirement would oblige the government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.[26]

Nearly two decades later, in *Kyllo*, the Court held that law enforcement could not technologically invade the home from afar by use of a thermal imaging device without a warrant.[27] There, law enforcement suspected the defendant of growing marijuana plants inside of his home. Agents sat outside of the residence in their vehicle and used a thermal imaging device to scan the interior of the home, which took only a few minutes. The reading from the device showed that high levels of heat were emanating from a certain area of the home. Agents obtained a warrant to search the home based, in part, on this information.[28]

The Court held that, when the government "uses a device that is not in general public use" to permeate the walls of the home and find out details that previously would not have been known without physical intrusion, the surveillance is a Fourth Amendment search and requires a warrant.[29] It reasoned that the Fourth Amendment draws a line at the entrance of the house, and the line "must be not only firm but also bright — which requires clear specification of those methods of surveillance that require a warrant."[30]

Accordingly, if the searches in *Karo* and *Kyllo* were in violation of the Fourth Amendment, so too would be the use of a cell site simulator to track a cellphone inside a person's home. Thus, the location of the target phone will be critical to any challenge of a search utilizing StingRay technology.

### b. The Search of a Phone

It is also likely that the use of the StingRay constitutes a search of the target's phone (not to mention every other

phone that happens to be collaterally captured). This notion is supported by *Jones* and *Riley*.

First, in *Jones*, the Court held that the government's attachment of a GPS tracking device to the defendant's vehicle, and its use of that device to monitor the vehicle's movements, constituted a Fourth Amendment search requiring a warrant.[31] The Court addressed the issue under the theory of a governmental trespass (a "physical intrusion") onto the defendant's effect (the vehicle).[32] Although use of a cell site simulator is an electronic, rather than a physical, intrusion, the Supreme Court made no references in *Jones* that would differentiate between the two types of searches. Because *Jones* did not require an analysis regarding electronic intrusion, the Court purposely dodged that question, but left a strong hint that may be relevant to a cell site simulator search: "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy[.]"[33]

In a StingRay scenario, the police search the phone when they send signals to it and force it to respond. This is by nature an intrusive act — the simulator makes the phone do something that it would not otherwise do. This switch from inactive monitoring (i.e., obtaining records) to active monitoring (i.e., using the cell site simulator) is akin to the switch from traditional visual surveillance to GPS tracking in *Jones*; it causes the search to require a warrant.

Also of significance, the owner of the phone has no idea what is happening. The search is clandestine. This differs from using cell tower records because, with cell tower records, one can plausibly assume that the phone user is on notice that he is sending a signal to the third-party carrier, to whom he pays a monthly fee.

The Supreme Court's holding in *Riley* also supports the notion that the use of a StingRay amounts to a Fourth Amendment search of a phone. In *Riley*, the Supreme Court unanimously enunciated that a phone is more similar to a house, as in *Karo*, than a car, as in *Jones*, and held that a search of a phone requires a warrant.[34] It explained, "[i]ndeed, a cellphone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form — unless the phone is."[35]



Applying this principle to the use of a cell site simulator, it would seem that the invasive interaction with the phone is akin to a police officer scrolling through a phone's records. With a StingRay, the search may be more remote, and it may be generally less intrusive, but it is still a search.

phones most of the time, with 12 percent admitting that they even use their phones in the shower."[37]

Thus, assuming that most people keep their cellphones on their bodies, it is by no means illogical to analogize tracking a phone to tracking the movement of a person. By using devices like cell site simulators, the government is able to tell

**Law enforcement officers are going to great lengths to keep the use of StingRay devices a secret.**

### c. The Search of a Person

Finally, the government's use of the cell site simulator may constitute the search of a person.

The Supreme Court's analysis in *Riley* strongly supports this view. For example, the Court stated 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 the human anatomy."[36] The Court cited a study that found that "nearly three-quarters of smartphone users report being within five feet of their

where the person is with great precision. In some ways, it is akin to secretly planting a GPS device on someone and tracking their movement (as in *Jones*).

This becomes even more problematic if, for example, people were having a meeting in a house. By using a StingRay, the government could tell who is at the meeting (by reading the phones' IMSI signals), what is being discussed (by reading the content of messages), and even who left to use the restroom (by tracking a phone's movement). The potential for intrusion of this type is

unbounded — and all the more reason it is a Fourth Amendment search for which a warrant should be required.

## Warrants

One of the most troubling facts surrounding the use of StingRay devices is the manner in which law enforcement is seeking authorization from judges. It seems to be a general practice that they are using modified pen register or trap-and-trace orders as quasi warrants to circumvent Fourth Amendment concerns. In most instances this is disingenuous, as these statutory orders were not intended to justify privacy intrusions on this scale. Making matters worse, in some instances law enforcement is burying confusing cell site simulator jargon — which no judge could possibly understand — into the text of the orders to modify the document.

The following is an example of the language that was buried within a standard pen register/trap-and-trace order that was recently signed by the same Baltimore City judge mentioned earlier who excluded a stolen cellphone from trial. Note that, when subsequently litigating this order in federal court, the government argued that this language was a fair and accurate description that it was seeking authorization to use a cell site simulator:

> ORDERED, that the Agencies shall complete the necessary installation of the Pen Register / Trap & Trace and Cellular Tracking Device, utilizing AT&T; Sprint / Nextel; Virgin Mobile / T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc.; and / or any other Telecommunication service provider providing services for the above listed telephone number, facilities, technical information and equipment, if required. The Agencies are authorized to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register / Trap & Trace and Cellular Tracking Device, unobtrusively and with a minimum of interference to the service of subscriber(s) of the aforesaid telephone, and shall initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available, Global Positioning System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), Precision Locations and any and all locations, and such provider shall initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent / agencies serving the Order.[38]

It is easy to imagine that a judge would easily gloss over this paragraph and be confused. The language does not mention "cell site simulator" or StingRay or anything with which the judge might be familiar. The language refers to "service providers," which makes it seem as if this is a standard cell tower authorization. There is conveniently no mention that all cellphones within a certain area are subject to be tracked, or that the target phones can be tracked inside a home. What is arguably most confusing is that the order and application are both captioned as pen register/trap and trace documents under the state law that authorizes such investigate techniques.

In Tacoma, Wash., when judges were queried by the local newspaper about whether they understood that approximately 200 orders they had signed were being used to authorize cell site simulators, they responded that they had never even heard of the devices. In response, the judges started requiring new disclosures by police seeking such authorization.[39]

In an apparent attempt to fortify these pen register/trap-and-trace orders, police are sometimes adding brief statements of probable case. This appears to be done so that the government can later argue that the order is, essentially, a warrant, thereby giving it broader effect than a pen register order. But this too is misleading. Because a pen register or trap-and-trace application does not require a showing of probable cause, it is unlikely that a judge considering the application would scrutinize the assertion of probable cause.[40]

## Attacking the Order

Because it is likely a court would consider the use of a cell site simulator to be a Fourth Amendment search, the key to challenging this device is defeating the pen register order — which the government will argue is effectively a

warrant. The following are a few arguments for doing so:

### a. Challenge the 'Warrant' as Misleading to the Court

Defense counsel should first argue that the application (or affidavit) for the order was intentionally misleading, thereby meriting a hearing pursuant to *Franks v. Delaware*.[41] Under *Franks*, the defendant "must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit."[42] The defendant must also show that the offending information was material to the issuance of the warrant (or order).[43]

The false statement is the omission of language that would actually allow the judge to understand what was going on. Rather than openly tell the judge they are seeking authorization for the use of a "StingRay" or "cell site simulator" — one will probably not see these words in the application or order — the government has most likely cloaked its true intention with technical jargon. The description may omit critical facts about the technology, such as the fact that it will capture telephone information from innocent third-party phone users. The description may omit the fact that the tracking is focused on a home — where privacy concerns are greater. Without divulging this information, it would likely be impossible for the judge to understand what the affiant really wanted to do.

How does one prove that this misrepresentation was intentional? Simple. The police and/or prosecutor will openly admit it. It is precisely their goal to conceal this information — based on their concerns about nondisclosure agreements with the manufacturers, or national security, or both. The last thing they want is to put the true nature of the device in a document that they know will someday have to be turned over to a defense attorney. Even the most obstreperous police witness, when questioned under oath, would be hard pressed to deny that there was an intent to conceal certain information about the cell site simulator.

### b. Fighting the Good Faith Exception

The argument under *Franks* dovetails with the argument defense counsel can use to overcome the good faith exception, which will likely be the government's first line of defense.[44] Two exceptions to the good faith doctrine may be present in the case of a cell site simulator: (1) when the affiant knowingly or recklessly misled the magistrate with false information or material omissions and (2) when the warrant is facially deficient in its description of the place to be searched or the things to be seized.[45]

First, it is likely that the very same team of officers who created the application and the order also used the cell site simulator. As such, they would have known that the order was based on a facially insufficient application — in which the true nature of the device was concealed from the magistrate.

Second, if the government is arguing that the pen register order is actually a warrant (because it includes a statement of probable cause), it is likely that the order authorized an overly broad search. The order may be overly broad if it did not impose geographical limitations on where the officers could use the cell site simulator. The order may also be overly broad because it implicitly authorizes the search not only of the target phone, but of all other phones in the surrounding area.

Finally, defense counsel should emphasize that the order is invalid as a warrant because it relies on a statute that authorizes only pen register or trap and trace devices. This argument is bolstered by the fact that, under federal law, a pen register may not be used to collect "any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[46] In contrast, cell site simulators collect information that discloses the physical location of the telephone and its user — and that is precisely the reason law enforcement is using them.

### c. Technical Grounds

It is also possible for defense counsel to challenge the order on technical grounds that would make it facially invalid. State and federal statutes authorizing warrants to search a person, property or electronically stored information require execution within 14 days; tracking device warrants must be executed within 45 days.[47] These requirements are important because, when the time period expires, the government must submit a new application with a new statement of probable cause.

Under the federal pen register statute, 18 U.S.C. § 3123, an order for a pen register lasts up to 60 days. This makes some sense because a pen register is less invasive than a warrant or a tracking device authorization. If law enforcement is arguing, however, that the pen register (including a statement of probable cause) is effectively a warrant, it would follow that the authori-

zation should only last for 14 days. The government should not be able to circumvent this temporal requirement by proceeding under the pen register statute. If a warrant with a 60-day term is facially invalid, the same can be said about a pen register order that is being used as a warrant.

#### d. Distinguish *United States v. Rigmaiden*

The government may try to rely upon *United States v. Rigmaiden,*[48] one of the few published opinions on this issue, to prop up its so-called warrant. But this case can be distinguished. In *Rigmaiden*, a federal court upheld the use of a cell site simulator when it was supported by a tracking warrant. The application for that warrant, however, was far more explicit than the pen register applications that are typically being used today. The *Rigmaiden* court reasonably could have understood what it was authorizing from the relatively detailed language of the application. The *Rigmaiden* order was further bolstered by the inclusion of limiting provisions.

Because the court had been informed that the use of the cell site simulator would likely intrude upon private areas, it "specifically required the government to 'expunge all of the data' at the conclusion of the tracking mission."[49] It also limited the duration of the tracking period to 30 days, and it "ordered that monitoring of transmissions related to the [target] aircard were 'limited to transmissions needed to ascertain the physical location of the aircard.'"[50] These specifics are simply not present in pen register applications.

One federal court, the Southern District of Texas, has already distinguished *Rigmaiden* and held that a pen register order does not apply to the use of a StingRay device.[51] This is obviously an evolving area of law, and practitioners litigating this issue must continually look for new opinions.

#### e. Distinguish *United States v. Karo*

The government may also rely on a passage from *Karo* to argue that an order satisfies a warrant's particularity requirement — even if it does not specify that the phone will be tracked inside of a home, or elsewhere. *Karo*, considering a beeper installed in a container of ether, states that "it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is required. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance."[52] This could be interpreted to imply that an application for authorization to track a phone need not contain any specific geographical information about where the tracking will take place.

This dicta from *Karo*, however, should not apply to cell site simulators. *Karo* involved a beeper, which was attached to and monitored one specific item identified in the warrant. A cell site simulator, on the other hand, is not attached to anything and monitors infinite items (i.e., all of the phones in the vicinity). The beeper in *Karo* was a single physical device that was installed and tracked by police over a radio frequency particular to that device. In contrast, cell site simulators interact with and gather information from all bystanders' phones within a certain radius of the cell site simulator. The cell site simulator, unlike the beeper, is not placed "into" an object. Rather, it interferes with objects.

Finally, the object in *Karo* was a can of ether, which was, in the circumstances of the case, contraband. Thus, anyone who possessed the ether was arguably engaging in criminal conduct. The objects here are all of the phones within a certain radius of the cell site simulator. These phones are not contraband. As the Supreme Court explained in *Riley*,[53] cellphones are the opposite of contraband — they are an essential tool of modern society. And, unlike the can of ether in *Karo*, cellphones carry a "cache of sensitive personal information,"[54] from which one may "reconstruct an individual's private life[.]"[55]

## Conclusion

If a defense attorney can identify that a StingRay was used, it is likely that a good result will follow. The more the attorney can discover and litigate, the more the government will be forced into an uncomfortable position. If a motions hearing is set, for example, and subpoenas are served on individuals with knowledge of the StingRay device, it is likely that the prosecutor will be spending late nights with his superiors trying to figure out what to do.

One possibility is that the government will decide it would rather lose its case than risk a disclosure about its StingRay device. Whatever the prosecutor's concern may be — national security, secrecy, or a nondisclosure clause — that concern will likely overshadow the importance of a single criminal case. Thus, the prosecutor may proceed without a particular piece of evidence, even if that piece of evidence could cost him the case.[56]

Another possibility is that the recognition of a StingRay issue will be enough to generate a beneficial plea deal. In a Florida armed robbery prosecution, a judge ordered the state to show the cell site simulator to the defense. Rather than do this, the state obtained a guilty plea by reducing the charges from armed robbery to petty theft.[57]

Similarly, in the case described at the beginning of this article, related to the search of a residence in West Baltimore, the parties settled on the morning the case was set for a suppression hearing. As the parties inched closer to the hearing, the plea offer improved. Finally, it was too good to refuse, and the defendant decided that a short prison sentence was better than the uncertainty of trial.

## Notes

1. American Civil Liberties Union, Stingray Tracking Devices: Who's Got Them?, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.

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

3. *Id.*; Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, The Baltimore Sun (April 9, 2015), http://www.baltimoresun.com/news/maryland/crime/blog/bs-md-co-county-stingray-20150409-story.html.

4. *Maryland v. Batty*, Case No. 2B02204540, Transcript of Motions Hearing (Sept. 16, 2014).

5. Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times (March 15, 2015), *available at* http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html.

6. Fenton, *supra* note 2.

7. *Baltimore Police StingRay nondisclosure agreement*, The Baltimore Sun (April 8, 2015), http://www.baltimoresun.com/bal-police-stingray-non-disclosure-agreement-20150408-htmlstory.html.

8. *Id.*

9. IMSI is the acronym for "international mobile subscriber identity," which is a cell-

phone's unique identifier.

10. *See* DOJ Electronic Surveillance Manual (Jan. 2, 2008), *included in* DOJ's Response to ACLU's FOIA Request, at 17 (Aug. 12, 2008), *available at* https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (hereinafter "DOJ Electronic Surveillance Manual," with reference to the pagination of the FOIA Request Response PDF).

11. *Id.* at 41 ("A cell site simulator (CSS) electronically 'forces' a cellular telephone to autonomously register its MIN and ESN when the target telephone is turned on but is not being used.").

12. *See* Electronic Privacy Information Center ("EPIC"), *Epic v. FBI — StingRay / Cell Site Simulator*, http://epic.org/foia/fbi/stingray/.

13. DOJ Electronic Surveillance Manual at 9.

14. *Id.* at 17.

15. *See, e.g.,* PKI Electronic Intelligence, GSM Cellular Monitoring System (product brochure) at 12, http:// docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEM (noting that the device can "locat[e] … a target mobile phone with an accuracy of 2 m[eters]").

16. *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 996 (D. Ariz. 2012).

17. Hearing on Motion to Suppress, *Florida v. Thomas*, No. 2008-CF-3350A (Fla., Leon Co. Cir. Ct., Aug. 23, 2010), *available at* https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

18. *See* DOJ Electronic Surveillance Manual at 17. The devices used by the federal government are likely configured to disable the content-interception function, as the DOJ has acknowledged that a wiretap order under the heightened Title III standard (18 U.S.C. § 2518) would otherwise be necessary. *See id.*

19. *United States v. Karo*, 468 U.S. 705 (1984).

20. *Kyllo v. United States*, 533 U.S. 27 (2001).

21. *United States v. Jones*, 132 S. Ct. 945 (2012).

22. *Riley v. California*, 134 S. Ct. 2473 (2014).

23. 468 U.S. 705.

24. *Id.* at 707–10.

25. *Id.* at 716; *see also id.* at 719.

26. *Id.* at 717–18.

27. 533 U.S. 27.

28. *Id.* at 29–31.

29. *Id.* at 40.

30. *Id.*

31. 132 S. Ct. at 949.

32. *Id.* The expectation-of-privacy line of Supreme Court cases also supports the conclusion that the cell site simulator search is a trespass. For example, in *Katz v. United States*, 389 U.S. 347 (1967), the Court found a violation of the Fourth Amendment where the government was eavesdropping on a conversation in a public telephone booth.

33. 132 S. Ct. at 954.

34. 134 S. Ct. 2473.

35. *Id.* at 2491 (emphasis in original).

36. *Id.* at 2484.

37. *Id.* at 2490.

38. Somewhat ironically, this Order was signed by the same Baltimore City Circuit Court judge who, as mentioned in this article, granted the suppression of a cellphone when the police officer refused to answer questions about his use of the cell site simulator in *State v. Batty*.

39. Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, The News Tribune (Tacoma) (November 15, 2014), *available at* http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?sp=/99/289/&rh=1.

40. Unlike the probable cause required to obtain a warrant, a pen register/trap and trace order requires only a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. 18 U.S.C. § 3122(b)(2).

41. *Franks v. Delaware*, 438 U.S. 154 (1978).

42. *Id.* at 155–56.

43. *Id.*

44. The good faith exception is derived from *United States v. Leon*, 468 U.S. 897 (1984), in which the Supreme Court held that when an officer acts "in the objectively reasonable belief that [his] conduct did not violate the Fourth Amendment," evidence seized under the authority of a search warrant that is later invalidated should not be suppressed. *Id.* at 918.

45. *Id.* at 923.

46. 47 U.S.C. § 1002(a)(2).

47. Fed. R. Crim. P. 41(e)(2)(A)–(C).

48. *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013).

49. *Id.* at *22 (quoting the warrant).

50. *Id.* at *14 (quoting the warrant).

51. *In the Matter of The Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012).

52. *United States v. Karo*, 468 U.S. 705, 718 (1984).

53. 134 S. Ct. 2473 (2014).

54. *Id.* at 2490.

55. *Id* at 2489.

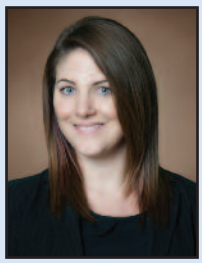
56. *See, e.g.,* Adam Lynn, *Defendant Challenges Use of Secret 'StingRay' Cell Device*, The News Tribune (Tacoma) (April 26, 2015), http://www.thenewstribune.com/2015/04/26/3759932/defendant-challenges-use-of-secret.html (discussing a case in Tacoma, Wash., where authorities refused to publicly disclose details about the StingRay, citing a nondisclosure agreement, and prosecutors did not fight defense counsel's efforts to have evidence gained by use of the StingRay excluded).

57. *See* Ellen Nakahima, *Secrecy Around Police Surveillance Proves a Case's Undoing*, Wash. Post (Feb. 22, 2015), *available at* http:// washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html. ■

## About the Authors

C. Justin Brown's practice is focused on white collar, federal criminal defense, and civil matters. He currently represents Adnan Syed, the subject of the podcast "Serial." Prior to entering the legal profession, he was a print journalist who worked for several national publications, including the *New York Times* and *Newsweek*.

**C. Justin Brown**
Law Offices of C. Justin Brown
231 E. Baltimore Street
Suite 1102
Baltimore, MD 21202
410-244-5444
Fax: 410-934-3208
E-mail brown@cjbrownlaw.com



A 2013 graduate of the University of Miami School of Law, Kasha M. Leese concentrates her practice on civil litigation and criminal defense cases.

**Kasha M. Leese**
Law Offices of C. Justin Brown
231 E. Baltimore Street
Suite 1102
Baltimore, MD 21202
410-244-5444
Fax: 410-934-3208
E-mail kasha@cjbrownlaw.com