THE BRAVE NEW WORLD OF CELL-SITE SIMULATORS

Heath Hardman[·]

INTRODUCTION

How do you catch a hacker that has stolen thousands of dollars, stolen multiple identities, and evaded capture for years? If you're the Federal Bureau of Investigation (FBI), you use a Stingray, of course. If you're puzzled right now, you probably also have an expectation of privacy within your home and it has never occurred to you that the FBI could use a device to cause your phone to emit a signal, without your knowledge, for the purpose of locating it—and you. That device is the Stingray—a cell-site simulator—and the story of the hacker is not a fictional one. Technology constantly adapts, updates, and changes, and with it so does the law and society. Once again, we are faced with an emerging technology that the legal community must deal with. First, however, the legal community must understand the technology in order to spot the issues, argue causes, and apply analogous law until laws that are on-point are developed.

This article will cover the public awareness concerning cell-site simulators in section I. In section II, pertinent elements of cellular network technology will be discussed, which will be crucial to the legal community's ability to apply the law and create new laws. Section III will merge the technological information and other information publicly available to outline possible methods that have been, or could be, used. Finally, section IV will point to certain legal issues raised by cell-site simulator technology and the need for possible legislation or regulation. The

· J.D., Albany Law School, 2014; Editor-in-Chief, *Albany Government Law Review*, 2013–2014; B.S. Philosophy, Empire State College. The author served in the United States Marine Corps from 1998–2009 and served twice in Iraq and twice in Afghanistan. During the author's military service, he completed the three-year Military COMINT Signals Analyst Program at the National Security Agency. The author has used, and is familiar with, multiple cell-site simulators. Much of the author's experience is classified, so only unclassified publicly available sources are used here. The views expressed in this writing are those of the author and in no way reflect the position or views of the National Security Agency or the United States Government or Military.

technology explained, and the legal issues raised, will enable following efforts to explore the brave new world of cell-site simulators.

I. PUBLIC AWARENESS

A. Cell-Site Simulators in the Media

In 2010, Chris Paget made news when he debuted a device that spoofed a GSM base station and eavesdropped on calls made by AT&T subscribers in front of a crowd at a Defcon security conference.[1] As far as the subscribers' cellphones were concerned, Paget's device was "indistinguishable from AT&T."[2] In fact, Paget used a voice-over-internet program to connect the calls while recording them on a USB stick.[3] Mike Tassey and Richard Perkins, in 2011, built a "flying, unmanned, automated password-cracking, Wi-Fi sniffing, cell-phone eavesdropping spy drone."[4] "The drone can mimic GSM cell phone towers to trick targeted phones in a certain area into connecting to the plane's antenna rather than its usual carrier, allowing the drone to record phone calls and text messages which it then stores on a thirty-two gigabyte hard drive."[5]

In 2011, news agencies also began reporting on the FBI's use of a cell-site simulator—the Stingray.[6] The media's and public's awareness was aroused by the case of Daniel David Rigmaiden, a "Hacker" captured by the FBI and facing fraud charges in the U.S. District Court

---

[1] Andy Greenberg, *Despite FCC "Scare Tactics," Researcher Demos AT&T Eavesdropping*, THE FIREWALL, FORBES.COM, (July 31, 2010, 5:35 pm), http://www.forbes.com/sites/firewall/2010/07/31/despite-fcc-scare-tactics-researcher-demos-att-eavesdropping/. *See also* Kim Zetter, *Hacker Spoofs Cell Phone Tower to Intercept Calls*, THREAT LEVEL, WIRED.COM (July 31, 2010, 7:57 pm), http://www.wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/.

[2] Greenberg, *supra* note 1.

[3] *Id.*

[4] Andy Greenberg, *Flying Drone Can Crack Wi-Fi Networks, Snoop On Cell Phones*, SECURITY, FORBES.COM, (July 28, 2011, 2:11 pm), http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/. *See also Eavesdropping Drone: New Drone Listens in on Cell Phone Calls and Hacks Wi-Fi Networks*, Homeland Security News Wire (Aug. 5, 2011), http://www.homelandsecuritynewswire.com/new-drone-listens-cell-phone-calls-and-hacks-wi-fi-networks.

[5] Greenberg, *supra* note 4.

[6] *See, e.g.*, Jennifer Valentino-DeVries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, Wall Street Journal, Sept. 22, 2011, at A1.

of Arizona, Judge David G. Campbell.[7] Regarding the Stingray, the Wall Street Journal reported:

> A stingray works by mimicking a cellphone tower, getting a phone to connect to it and measuring signals from the phone. It lets the stingray operator "ping," or send a signal to, a phone and locate it as long as it is powered on, according to documents reviewed by the Journal. The device has various uses, including helping police locate suspects and aiding search-and-rescue teams in finding people lost in remote areas or buried in rubble after an accident.[8]

Additionally, the Wall Street Journal reported that the "U.S. armed forces also use stingrays or similar devices," and "local law enforcement in Minnesota, Arizona, Miami and Durham, N.C., also either possess the devices or have considered buying them."[9] According to Sgt. Jesse Spurgin, the Maricopa County Sherriff's Department, in Arizona, uses the equipment on a monthly basis, for location only, but not to listen to conversations.[10]

The American Civil Liberties Union (ACLU) and Electronic Frontier Foundation (EFF) filed *amicus* briefs in the *Rigmaiden* case in 2012.[11] Because the *Rigmaiden* case is "the first case in the country to address the constitutional implications of a so-called 'stingray,' a little known device that can be used to track a suspect's location and engage in other types of surveillance," the ACLU and EFF "argue that if the government wants to use invasive surveillance technology like [the Stingray], it must explain the technology to the courts so they can perform their judicial oversight function as required by the Constitution."[12] Regarding the importance of this case, the ACLU stated:

---

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Linda Lye, *In Court: Uncovering Stingrays, a Troubling New Location Tracking Device*, ACLU (Oct. 22, 2012, 12:42 pm), https://www.aclu.org/blog/national-security-technology-and-liberty/court-uncovering-stingrays-troubling-new-location.
[12] *Id.*

> The case is highly significant for two reasons. First, it shows that the government is using new types of technology—not just GPS and cell site location records—to track location. Second, it shows that the government is going to great lengths to keep its surveillance practices secret. The government is hiding information about new surveillance technology not only from the public, but even from the courts. By keeping courts in the dark about new technologies, the government is essentially seeking to write its own search warrants. That's not how the Constitution works.[13]

The ACLU also highlighted three Stingray-related privacy concerns:

- First, they collect information about the devices and whereabouts of third parties, not just the targets of an investigation. []IMSI catchers mimic a wireless carrier's network equipment; in doing so, they send and receive signals to and from all mobile devices in the vicinity on the same network.
- Second, the devices can pinpoint a target with extraordinary precision. Some have an accuracy of two meters. This means that individuals can be tracked even when they are inside their homes.
- Third, although the government says the device used in Rigmaiden's case was not capable of capturing the content of communications, many IMSI catchers offered for sale by surveillance vendors offer this feature. IMSI catchers can thus be used for eavesdropping, not just location tracking.[14]

Although both the ACLU and FBI concluded that the use of the Stingray in the *Rigmaiden* case constituted a search under the Fourth Amendment, the ACLU stated that the warrant was problematic because "the papers the government submitted to get the so-called 'warrant' never told the judge that the government wanted to use a stingray (or IMSI catcher, or cell site emulator), what the device is, or how it works."[15] The ACLU further argued that "the government hid from the judge the facts that stingrays collect information about third parties, that they can pinpoint targets even within their homes, and that some models capture content, not just location."[16] Without all the information, the judge could not make a "meaningful, informed decision about whether the search the government sought to undertake was constitutional, and if

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

so, whether the court should have imposed limitations on the scope of the search."[17] Finally, the ACLU added that, "[b]ecause stingrays are indiscriminate, highly intrusive devices that obtain information from all nearby third parties on the same cellular network, and not just the target of an investigation, there is a serious question whether they can ever be used consistent with the Fourth Amendment."[18]

Another privacy issue was raised in 2012 when President Obama signed a bill that opened U.S. airspace to thousands of unmanned aircraft.[19] Concerns were voiced over safety, privacy, domestic law enforcement use, and legal policies.[20] In 2013, public awareness reached a boiling point as various media outlets reported on developments in the *Rigmaiden* case, domestic uses of surveillance drones, and the National Security Agency's use abroad.[21] According to Chris Soghoian, the ACLU's principal technologist, "'No matter how the StingRay is used—to identify, locate or intercept—they always send signals through the walls of homes,' which should trigger a warrant requirement . . . . 'The signals always penetrate a space protected by the Fourth Amendment.'"[22] On the domestic front, the Department of Homeland Security (DHS) customized its Predator drones to perform cell phone tracking, signals interception in the frequencies used by mobile phones, and added "direction finding" capabilities that can identify the location of mobile devices.[23] The DHS drones "are primarily used to patrol the United States' northern and southern borders but have been pressed into service on behalf of a growing number of law

---

[17] *Id.*
[18] *Id.*
[19] Jeff Glor, *Drone Use in the U.S. Raises Privacy Concerns*, CBSNEWS.COM (April 5, 2012, 8:09 am), http://www.cbsnews.com/8301-505263_162-57409759/drone-use-in-the-u.s-raises-privacy-concerns/.
[20] *Id.*
[21] *See, e.g.*, Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns Over Privacy*, WASHINGTON POST, at A03 (March 28, 2013); Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET.COM (March 2, 2013, 11:30 am), http://news.cnet.com/8301-13578_3-57572207-38/dhs-built-domestic-surveillance-tech-into-predator-drones/; Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASHINGTONPOST.COM (July 21, 2013), http://articles.washingtonpost.com/2013-07-21/world/40713603_1_national-security-agency-former-senior-agency-official-intelligence.
[22] Nakashima, *supra* note 21.
[23] McCullagh, *supra* note 21.

enforcement agencies including the FBI, the Secret Service, the Texas Rangers, and local police."[24] The National Security Agency's activities became a matter of public interest in 2013, as well, when the Washington Post reported an event where a Navy SEAL asked a drone operator and collector to locate a cell phone in Afghanistan.[25] According to the Washington Post, "The CIA wanted the phone as a targeting beacon to kill its owner."[26] Apparently, the motto used for one unit at NSA is, "We Track 'Em, You Whack 'Em."[27]

B. U.S. v. Rigmaiden

A central focus of the public's attention directed toward cell-site simulators is the case of *U.S. v. Rigmaiden*, involving the FBI's use of a Stingray to locate Daniel Rigmaiden.[28] At the time of this writing, the case has not gone to trial or been otherwise resolved, but numerous motions and memoranda have been filed, providing some information about the case.[29] The government alleges that, in 2007 and 2008, Daniel Rigmaiden used the identities of deceased and living individuals to e-file more than 1,200 fraudulent tax returns claiming over $3,000,000 in tax refunds.[30] Internal Revenue Service agents subpoenaed subscriber information for one of the IP addresses from which a return was filed and determined that the IP address was associated with a Verizon Wireless broadband access card, which was used to make a wireless connection between a computer and the Internet.[31]

In June and July of 2008, "the government obtained historical cell-site records from Verizon that reflected communications from the aircard" and "showed that the aircard

[24] *Id.*
[25] Priest, *supra* note 21.
[26] *Id.*
[27] *Id.*
[28] U.S. v. Rigmaiden, 2013 WL 1932800 (Dist. Ct. Arizona 2013).
[29] *Id.* at *1.
[30] *Id.*
[31] *Id.*

communicated regularly with several cell towers in the area of Santa Clara, California."[32] "Using the cell-tower information, a map, and various calculations," the government was able to narrow the location of the aircard to an area of about one-quarter of a square mile.[33] The government then obtained an order from a Federal Magistrate Judge in the Northern District of California that authorized a "trap and trace device to obtain additional cell site information, and a warrant authorizing the use of a mobile tracking device to communicate with the aircard."[34] Next, the government used this mobile device to track the aircard's location on July 16, 2008, to unit 1122 of the Domicilio apartment complex in Santa Clara, California.[35]

After determining the location of the aircard and apartment, the government obtained gate access data from the apartment's alarm company in order to ascertain the arrival and departure habits of the apartments occupant.[36] After observing the apartment, on August 3, 2012, agents saw a person matching the description of the apartment's occupant acting suspiciously.[37] After a chase, Daniel Rigmaiden was apprehended, and the keys in his pocket fit and turned the door lock to the apartment in question.[38] After obtaining a warrant, the agents entered the apartment and found false identification, the aircard, a laptop computer, and other devices that contained incriminating evidence.[39] In the end, Daniel Rigmaiden was identified by his fingerprints.[40]

---

[32] *Id.* at *3.
[33] *Id.*
[34] U.S. v. Rigmaiden, 2013 WL 1932800, at *3 (Dist. Ct. Arizona 2013).
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] U.S. v. Rigmaiden, 2013 WL 1932800, at *3 (Dist. Ct. Arizona 2013).

The technical strategy the FBI used began with the collection of the "aircard's historical cell-site, sector, and distance information for the previous 30 days."[41] Next the government tracked the "Verizon Wireless broadband access card/cellular telephone," but only for a period "not to exceed thirty (30) days" and "limited to transmissions needed to ascertain the physical location of [the aircard]."[42] Regarding the tracking, the FBI stipulated to several specific facts worth noting:

> - The mobile tracking device used by the FBI to locate the aircard functions as a *cell-site simulator*. The device *mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard.*
> - The FBI used the device in multiple locations. The FBI analyzed signals exchanged between the mobile tracking device and the aircard. *The FBI would take a reading, move to a new location, take another reading, move to another location, etc.* The FBI never used more than a single piece of equipment at any given time.
> - The device was used by government agents on foot within Defendant's apartment complex.
> - The device *generated real time data during the tracking process*.
>
> . . . .
>
> - Signals sent by the mobile tracking device to the aircard are signals that *would not have been sent to the aircard in the normal course of Verizon's operation of its cell towers*.
> - The mobile tracking device caused a *brief disruption in service to the aircard*.
> - During the tracking operation, *the FBI placed telephone calls to the aircard*.
> - The tracking operation was a Fourth Amendment search and seizure.
>
> . . . .
>
> - At the conclusion of the July 16, 2008, search efforts, the mobile tracking device had *located the aircard precisely within Defendant's apartment*.[43]

According to the FBI's own admissions, it is clear that the Stingray device is a cell-site simulator, which mimics a cell phone tower, sends and receives signals from an aircard in a manner that would not occur during normal operation, causes disruption in service, can call a

[41] *Id.* at *9.
[42] *Id.* at *14.
[43] *Id.* at *15, (emphasis added).

mobile device, and generates real-time data.[44] Furthermore, the Stingray collects third-party information from other cell phones and aircards in the area it is operating in, although the FBI claims that it deletes this information immediately after a tracking operation.[45]

Just what is a Stingray? Jennifer Valentino-DeVries of the Wall Street Journal answers that question:

Graphic 1: Stingray[46]

> The systems involve an antenna, a computer with mapping software, and a special device. The device mimics a cellphone tower and gets the phone to connect to it. It can then collect hardware numbers associated with the phone and can ping the cellphone even if the owner isn't making a call.
>
> . . . .
>
> Once a signal is found, the stingray setup measures its strength and can provide a general location on the map. The officer can then move to another location and again measure the signal strength. By collecting the signaling information from several locations, the system can triangulate the location of the phone more precisely.[47]

---

[44] *Id.* at *15.
[45] *See id.* at *20.
[46] Ken Jorgustin, *Govt. 'Stingray' Intercepting & Tracking Cell Phones*, MODERNSURVIVALBLOG.COM, (Oct. 27, 2012) http://modernsurvivalblog.com/government-gone-wild/govt-stingray-intercepting-tracking-cell-phones/.
[47] Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, DIGITS, WSJ.COM (Sept. 21, 2011, 10:33 PM), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/. *See also* Jennifer Valentino-DeVries, *How Technology is Testing the Fourth Amendment*, DIGITS, WSJ.COM (Sept. 21, 2011, 10:32 PM), http://blogs.wsj.com/digits/2011/09/21/how-technology-is-testing-the-fourth-amendment/.

Knowing the basics about what a Stingray is, and how it is used, is helpful, but a better understanding of cellular technology is needed in order frame this new technology in any legal context.

II. PRIMER ON CELLULAR TECHNOLOGY

Cellular technology, like many forms of technology, can be complicated. For the purposes of this paper, however, only three areas will be focused on: cell selection, location updating, and paging and calls. Most cellular technologies operate similarly, however there can be differences among varying standards. These differences may include different signal types, or merely different names for aspects that are nearly identical in all other aspects. For the purposes of this paper, the GSM standard will be used.[48]

A. Cell Selection

When a cellphone is active (powered on) without being in a phone call, it is deemed to be in "idle mode" and must 1) continuously stay in contact with a base station (cell tower), 2) listen to what the base station transmits in order to intercept incoming calls, and 3) monitor the radio environment in order to evaluate its quality and chose the most suitable base station.[49] Base stations broadcast important information related to the cell selection process, including the location area identity and whether the cell is barred for access or not.[50] A list of preferred networks is stored on the non-volatile memory of the Subscriber Identification Module (SIM); the most preferred is usually the home network.[51] The cellphone, while in idle mode, must choose *one* cell from which it expects to receive incoming calls from a paging channel; it is said

[48] *See* Sascha Segan, *CDMA vs. GSM: What's the Difference?*, PCMAG.COM (Aug. 22, 2012, 8:00 AM), http://www.pcmag.com/article2/0,2817,2407896,00.asp (explaining the two main types of cellular technology in the United States and their differences).
[49] MICHEL MOULY & MARIE-BERNADETTE PAUTET, THE GSM SYSTEM FOR MOBILE COMMUNICATIONS 192 (1992).
[50] *Id.* at 425.
[51] *Id.* at 449.

to be "camping" on this cell.[52] Additionally, when a cellphone wants to exchange information with the network, such as a call at the user's request, it must do so in the cell it is camping on.[53]

The "camped-on cell should also be as close as possible to the best cell in which a potential connection will be set up."[54] The criteria used to choose a cell combines the reception level of the cellphone, the maximum transmission power of the cellphone, and several other parameters depending on the cell.[55] During the cell selection process, the strength of the received signal from the base station, the maximum power of the cellphone, and cell-specific criteria are taken into account to create a value called C1.[56] "When a choice between cells has to be made, the cell of the best C1 is chosen among those equivalent for other criteria."[57] Another criteria called Cell Reselect Hysteresis (CRH) is used during the cell selection process.[58] It is a sort of handicap and sets a certain value that must be exceeded before switching from one cell to the other.[59] The new cell must have a C1 that is higher than the old cell's C1 with the CRH added—in other words, it must be significantly better, not just slightly better.[60]

In short, once a cell phone is powered on and in idle mode, it looks for the cell in its preferred network list that would allow for the best connection based on a mathematical calculation. When a cell phone is camped on one cell, it doesn't switch to a new cell until the new cell's C1 value is greater than the sum of the old cell's C1 and CRH. For a cell-site simulator operator to induce a cellphone to camp on his or her cell-site simulator (CSS), all he or she needs to do is become the strongest cell in the target cellphones preferred network.

---

[52] *Id.* at 434.
[53] *Id.* at 441.
[54] *Id.*
[55] MOULY & PAUTET, *supra* note 49, at 441.
[56] *Id.* at 453.
[57] *Id.*
[58] *Id.* at 455–56.
[59] *Id.*
[60] *Id.*

How, then, can a relatively small mobile CSS like the Stingray compete with a large and powerful cell? There are two ways: 1) move very close to the target cellphone, or 2) use Cell Reselect Offset (CRO). Moving close to the target cellphone may be difficult without a general idea of where the phone is located. Additionally, moving close to the target cellphone may not work if there is also a very strong cell nearby. However, a cell may artificially inflate its C1 value by adding Cell Reselect Offset (CRO).[61] Essentially, the cellphone is told to measure the reception of the cell (C1) and then boost the measurement by whatever amount of CRO the cell designates.[62] This new value—C1 + CRO—is designated as C2.[63] Thus, a CSS operator can artificially inflate the attractiveness of a CSS to a cellphone by adding CRO to achieve a seemingly higher signal strength than other neighboring cells.

One more factor must be taken into account—the BA list. The Broadcast Control Channel (BCCH) Allocation list, or BA list for short, consists of the six strongest neighboring cells, which the cellphone must continuously monitor along with the current serving cell.[64] These neighboring cells will be the cellphone's only candidates to camp on, should one become stronger than the cell it is currently camping on.[65] Thus, a CSS operator must configure his or her CSS to appear to be one of the cells on the BA list. Otherwise, the cellphone will not monitor for its existence or consider it as an option for selection. To estimate which cells may be on the cellphone's BA list, the CSS operator will likely need to survey the surrounding area to determine what the strongest cells are, and therefore which cells are most likely on the target cellphone's BA list.

---

[61] GSM TECHNICAL SPECIFICATION 05.08, ETSI 9, 14–15 (July 1996).
[62] *Id.*
[63] *Id.* at 14–15.
[64] *Id.* at 15–16.
[65] *Id.*

B. Location Updating

"A location area is a group of cells, each cell belonging to a single location area."[66] The identity of the location area a cell belongs to is broadcast by each cell, thus enabling cell phones to be informed of the location area they are in.[67] When a cellphone changes to a new cell, two cases may arise: either both cells are in the same location area, and the mobile station does not send any information to the network; or, the cells belong to two different location areas, and the mobile station informs the network of its change of location area.[68] This is called location updating.[69] "The status of the last registration attempt is stored in the SIM, as well as the identity of the location area."[70] Periodic location updating can occur anywhere from every six minutes to more than 24 hours, however, excessive location updating can create a heavy load on the network.[71]

A cellphone may receive location update rejections indicating that the network is not allowed or that the location area is not allowed.[72] If the network is not allowed, the subscriber has no subscription entitlement for service in the network, but if the location area is not allowed, the subscriber has no subscription entitlement for service in the location area.[73] If the cellphone is instructed that the network is forbidden, it will no longer attempt to communicate with cells of that network except on explicit request from the user.[74] Instead, the cellphone will look for a new network, and new cell.[75] Cellphones may also be instructed that roaming is not allowed, and mechanisms may be put in place to prevent further attempts in the same cells of that location

[66] MOULY & PAUTET, *supra* note 49, at 444.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.* at 472.
[72] MOULY & PAUTET, *supra* note 49, at 469.
[73] *Id.*
[74] *Id.* at 445.
[75] *Id.*

area.[76] The identities of location areas that have rejected a cellphone are stored, and will not be considered candidates for selection, but these identities are erased when the cellphone is switched off, or the SIM is removed.[77] Generally, there are three levels for the status of cellphones—the white list, grey list, and black list.[78] The white list includes cellphones that are approved; the grey list includes faulty cellphones whose faults are not important enough to justify barring; and the black list includes cellphones that are barred—either because they are stolen or because of severe malfunctions.[79] A CSS operator will need to pay careful attention to which location area he or she chooses, and which manner of rejection is used to reject non-target cellphones in order to prevent barring service to non-target cellphones.

C. Paging & Calls

When the network seeks to establish communications with a cellphone—for an incoming call, for example—it pages the cellphone.[80] Because the cellphone periodically updates its location, when an incoming call arrives, a paging message is only sent in those cells belonging to the location area where the cellphone has last performed location updating.[81] The cellphone responds, through various communications to and from the cell tower, and a channel assignment is made for the communication to occur on.[82] A full traffic channel may be used for signaling matters, rather than calls, but this wastes a lot of spectrum.[83]

When an initial channel assignment is made, the network provides the cellphone with the description of the channel, the initial timing advance to be applied, and the initial maximum

---

[76] *Id.*
[77] *Id.* at 448.
[78] MOULY & PAUTET, *supra* note 49, at 591.
[79] *Id.*
[80] *Id.* at 317–18.
[81] *Id.* at 45.
[82] *Id.* at 317–18.
[83] *Id.* at 191.

power.[84] When a cellphone is far from the cell tower, propagation delays may occur.[85] To account for this, a cellphone will advance its emission to compensate for the delay in time to transmit across the distance—a head start, so to speak.[86] The value, measured in time, is called the timing advance.[87] The timing advance can range from zero to 233 microseconds, which is sufficient to cope with cells having a radius of up to 35 km, given the speed of light.[88] The cell tower continuously measures the transmission response time and provides the cellphone with timing advance information twice every second.[89] Additionally, the network can control both the power of its own transmissions and the power of the cellphone's transmissions.[90] After preliminary channel assignments and parameters are assigned, the transmission mode is then chosen by the network, but may be changed by the network later according to the communication needs.[91] Once a traffic channel is at the cellphone's disposal—such as during a phone call—the cellphone is then in "dedicated mode."[92] In dedicated mode, a CSS operator can use the signal to locate the target cellphone.

III. Possible Methods of Locating a Cellphone with a Cell-Site Simulator

With a basic understanding of how cellphones and cellular networks interact, and using the information provided in the *Rigmaiden* case, a possible method for locating a cellphone can be established.

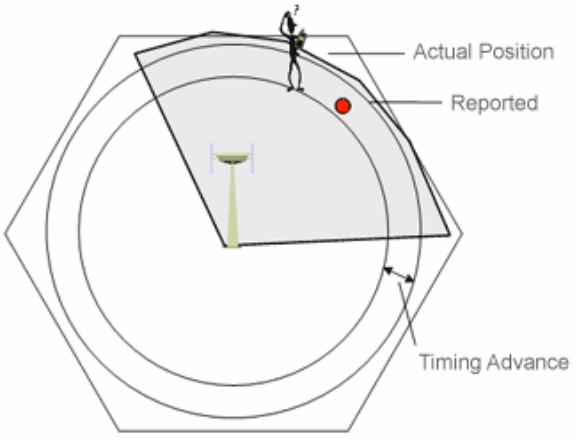
[84] Mouly & Pautet, *supra* note 49, at 375.
[85] *Id.* at 201.
[86] *Id.*
[87] *Id.*
[88] *Id.* at 346.
[89] *Id.*
[90] Mouly & Pautet, *supra* note 49, at 342–44.
[91] *Id.* at 385.
[92] *Id.* at 192.

A. Gather Historical Location Data

In the *Rigmaiden* case, the FBI obtained "historical cell-site records" that showed regular communication with several cell towers in an area of "just under one-quarter of a square mile."[93] More specifically, the FBI obtained "historical cell-site, sector, and distance information for the previous 30 days."[94] Cell sites are typically divided into three sectors.[95] If a 360-degree coverage area from a single cell-site were divided equally, each sector would be 120 degrees. Thus, determining which tower the cellphone is "camped on," along with the sector and it's directionality from the cell-site, would narrow a circular area down to what would be roughly shaped like a slice of pizza. This area could be further narrowed, however. Using the distance information—such as the timing advance data—it would be possible to determine how far into the sector, or 'slice of pizza,' the cellphone is located. This would pinpoint a cellphone inside an arc located at an approximate distance from the cell-site's center and within about a 120 degree range of directionality. Furthermore, if the cellphone camps on other cells in the area, a cross-section of two arcs may occur which would further narrow the area down to the area where the arcs overlap. Finally, the historical data would indicate where the cellphone is typically located at various times and may show a pattern of behavior—such as where the phone tends to be at night. This may be a good indication of where the target individual's home is, unless he or she works nights, etc. Any place, however, where a clear pattern of behavior indicates a cellphone is habitually located at may be a good starting point for further location efforts.

[93] U.S. v. Rigmaiden, 2013 WL 1932800, at *3 (Dist. Ct. Arizona 2013).
[94] *Id.* at *9.
[95] MOULY & PAUTET, *supra* note 49, at 611.

Graphic 2: Cell-Site, Sector, and Timing Advance[96]



B. Simulate a Cell-Site and Attract the Target Cellphone

After determining a general area that the target cellphone is located within, the next step would be to move into the area with a cell-site simulator to 'spoof' a cell-site. In the *Rigmaiden* case, the FBI used a cell-site simulator that "mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard."[97] In order to simulate a cell-site that would attract the target cellphone, the cell-site simulator (CSS) must appear to be part of the target cellphones preferred network, appear to be the strongest cell, and appear on the target cellphone's BA list.[98] If the mimicking CSS appears to be a proper candidate, and the strongest available choice, the target cellphone will likely 'camp' on it.[99] It is possible for the CSS to appear to be the strongest by moving close to the target cellphone and manipulating the Cell

[96] *What is Enhanced Cell ID?*, AT&T.COM, http://developer.att.com/developer/tier2page.jsp?passedItemId=3100150 (last visited December 20, 2013).
[97] U.S. v. Rigmaiden, 2013 WL 1932800, at *15 (Dist. Ct. Arizona 2013).
[98] *See supra* section II.
[99] *Id.*

Reselect Offset (CRO).[100] Once the target cellphone is 'camped' on the CSS, the CSS operator may initiate communication with the target cellphone.[101]

C. Page the Target Cellphone

Once the target cellphone has 'camped' on the CSS, the CSS operator may page the cellphone to initiate a traffic channel.[102] Typically, a traffic channel is used for calls, but it may be used for signaling purposes, thus the user need not be aware that the target cellphone is emitting a signal.[103] In the *Rigmaiden* case, the FBI stipulated that the Stingray sent signals that would not have been sent to the mobile device "in the normal course of Verizon's operation of its cell towers."[104] Additionally, the Stingray caused a "brief disruption in service" to the mobile device and "the FBI placed calls" to the mobile device.[105] Once the target mobile device is in a traffic channel, or phone call, the last remaining step is to locate it.

D. Locate the Target Cellphone

While the phone is emitting a signal, induced by the CSS, the cellphone's power output can be manipulated.[106] This may help to establish a stronger signal to be detected and located. In the *Rigmaiden* case, the FBI "would take a reading, move to a new location, take another reading, move to another location, etc."[107] At the conclusion of the search efforts, the Stingray located the mobile device "precisely within [Rigmaiden's] apartment."[108] While it is not clear from the *Rigmaiden* case, it is conceivable that the "readings" taken were both signal strength and signal direction. The direction would indicate where the signal was emanating from, and the

[100] *Id.*
[101] *Id.*
[102] *See supra* section II(c).
[103] *Id.*
[104] U.S. v. Rigmaiden, 2013 WL 1932800, at *15 (Dist. Ct. Arizona 2013).
[105] *Id.*
[106] *See supra* section II(c).
[107] U.S. v. Rigmaiden, 2013 WL 1932800, at *15 (Dist. Ct. Arizona 2013).
[108] *Id.*

strength may indicate an approximate distance. Furthermore, the FBI moved to new locations.[109] It is also conceivable that the FBI determined their position using GPS, and the direction from that position that the signal emanated from. By moving to a new location, the FBI could then determine their position and the direction the signal is emanating from relative to that new position. If those positions and lines of direction where overlaid on a map, they would eventually cross. That point of intersection would likely be the approximate location of the target cellphone.

Graphic 3: Position and Direction Overlaid on Map[110]

Although the target cellphone's location may be narrowed from historical cell-site data to a location determined using a vehicle or drone, it may be necessary to further narrow the location. This is especially so if police forces intend to enter a premises. In the *Rigmaiden* case, once the FBI had narrowed the location to an apartment complex, they entered on foot with the

[109] *Id.*
[110] *Direction Finding and Geolocation*, SAT.COM, http://www.sat.com/products/SigMon.php (last visited December 20, 2013).

Stingray to determine the exact apartment the target device was located within.[111] This may or may not be necessary in all cases, however.

IV. LEGAL IMPLICATIONS AND ISSUES

There are multiple legal implications raised by the existence and use of cell-site simulators. While Fourth Amendment issues may be the first that come to mind, there are others lurking below the surface. If an individual can possess and use a CSS, then he or she could essentially do that which a legitimate cell network could do—or direct a cellphone to do. With a basic understanding of cellular networks, one can begin to see potential abuses, and the possible need for legislation or regulation. In this section, the issues will be raised, but not analyzed in detail. Rather, the purpose and scope of this article is educating the legal community and raising the issues for further discussion and development.

A. Fourth Amendment Searches[112]

It is likely that courts will consider using a CSS to locate target cellphones a search under the Fourth Amendment. In fact, the FBI stipulated to this and the Court agreed in the *Rigmaiden* case.[113] There is an important distinction for lawyers and policy-makers to keep in mind with regard to the use of a CSS and expectations of privacy. There are three categories of communications emitted by a cellphone—automatic transmissions,[114] user initiated

[111] U.S. v. Rigmaiden, 2013 WL 1932800, at *15 (Dist. Ct. Arizona 2013).
[112] For an exploration on the topic of the Fourth Amendment and cellphone tracking, *see* Brittany Hampton, *From Smartphones to Stingrays: Can the First Amendment Keep up with the Twenty-First Century?*, 51 U. LOUISVILLE L. REV. 159 (2012); Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell-Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489 (2012); William Curtiss, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139 (2011). *See also*, U.S. v. Rigmaiden, 2013 WL 1932800 (Dist. Ct. Arizona 2013).
[113] U.S. v. Rigmaiden, 2013 WL 1932800, at *15 (Dist. Ct. Arizona 2013).
[114] *See supra* section II.

transmissions,[115] and third-party initiated transmissions. While a user may be said to know that his or her cellphone transmits a signal automatically and when initiated by the user, and thus not subject to a reasonable expectation of privacy, the user likely does not know that a third party—the government—can *cause* their cellphone to transmit a signal when it ordinarily would not and without the user acting to transmit the signal.

The Court, in *Rigmaiden*, analyzed the privacy objections of the defendant, and held that he did not have an objectively reasonable expectation of privacy.[116] This was in part due to his use of fraudulent identities to perpetuate other frauds.[117] Furthermore, the Court cited the third-party doctrine where "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[118] However, the Court overlooked the fact that Rigmaiden did not voluntarily transmit a signal for the purposes of revealing his location. While it is arguably correct that Rigmaiden voluntarily turned over to a third-party (Verizon) historical cell-site data in the normal usage of his mobile device through automatic and user initiated transmissions, it does not appear that he voluntarily turned over his signal to a CSS operated by the government or even initiated the signal. Instead, a third party, outside of Rigmaiden's awareness or consent, caused his mobile device to emit a signal for the purposes of locating it. The FBI even stipulated to the fact that signals that would not have been sent during the normal course of business were sent and received.[119] From the *Rigmaiden* case, at least, its seems that future challenges to historical cell-site records would likely fail under the third-party doctrine, as would claims of privacy in the commission of a fraud or within a fraudulent identity. The challenge not addressed, and most likely to succeed, is a challenge raising the issue of

[115] *Id.*
[116] U.S. v. Rigmaiden, 2013 WL 1932800, at *6 (Dist. Ct. Arizona 2013).
[117] *Id.* at 6, 9.
[118] *Id.* at *10.
[119] *Id.* at *15.

government-induced emissions used to track an individual's cellphone, rather than automatic or voluntary transmissions.

B. Intellectual Property Rights

Cell-site simulators mimic real cell-sites in commercial cellular networks. In fact, in order to work properly, the CSS must broadcast data to prospective target cellphones to indicate that it belongs to the preferred network.[120] Cellular network service providers may have a cause of action against those using a CSS that mimics their network, although it may be hard to detect. One possible method of detection, however, is through the location updating process. Cellphones store the last location area registration attempt made.[121] If a CSS is set up to reject phones that are not the desired target, the cellphones may then try to register in another location area on the network. If this generates traffic with the network, or perhaps a surge in traffic, as many phones in the area are rejected from a location area that claims to be part of the network, but is not recognized, the cellular network provider may suspect a CSS. However, it would still be difficult to determine who actually operated the CSS and, therefore, infringed upon the networks intellectual property rights.

C. Airspace and Bandwidth Management

Airspace and bandwidth are limited resources. If a CSS operator employs a drone with a CSS on board, airspace will become an issue—for both safety and resource management. Additionally, a CSS must be operated within the cellphone frequency band by necessity, as do legitimate networks. A CSS operator's intrusion into the bandwidth can wreak havoc for both the network and users trying to use their cellphones. Airspace and bandwidth allocated by the FAA or FCC, perhaps at a cost, then become hijacked by a potentially rogue CSS operator. Even

[120] *See supra* section II and III.
[121] MOULY & PAUTET, *supra* note 49, at 444.

if the CSS operator is a government actor, acting under color of law, the need to locate a cellphone, and its user, may be under short notice and send the various systems into chaos with the potential for dangerous consequences.

D. Quality of Service, Denial of Service, and Safety

Maintaining a cellular network in a state where the quality of service offered to the subscribers is acceptable is an important goal for providers.[122] Not only is the user of the target cellphone denied service for at least a short period,[123] but other users may be as well. As discussed above in section II, a cellphone can be rejected from a location area or assigned to the blacklist—effectively barring it from accessing the network until powered off and back on. If a CSS operator broadcasts the CSS as belonging to the location area that currently exists in the geographic area, users who are barred from camping on the CSS cannot rejoin the network until they move to a new location area or cycle the power on their phone.[124] This secondary effect of cell-phone tracking, when done improperly, can lead to a reduced quality of service and a denial of service, at least temporarily. In a highly populated area, it is possible that the rejected non-target phones will be rejected in high volume and seek to re-register with the legitimate network nearly simultaneously. A peak in traffic could have negative effects on the cellular network's infrastructure and servers.

Some medical alert devices work through cellular networks and could be negatively affected.[125] It is possible that an individual wearing one of these devices could be in the vicinity of an operating CSS. The device may try to register with the CSS, and be rejected from either

---

[122] MOULY & PAUTET, *supra* note 49, at 578.
[123] U.S. v. Rigmaiden, 2013 WL 1932800, at *15 (Dist. Ct. Arizona 2013).
[124] *See supra* section II.
[125] *See, e.g.*, *Mobile Alert Systems*, MEDICALALERT.COM, http://seniors.medicalalert.com/mobilesystem.html#Mobile-Alert-System (last visited December 20, 2013).

the location area or even blacklisted. Because the individual would not likely check the device for cell service or attempt to make a call and realize there is a problem beforehand, if an emergency were to happen the device may not function properly. That individual may find out too late that their device is not working. Even if they thought to turn it off and back on, it may be too late for help to arrive.

Criminals and terrorists may be able to use a CSS to further their activities. For example, an ankle tracking device that communicates through a cellular network could be manipulated by a CSS. Once the ankle tracking device has registered to the CSS, it can no longer communicate with the network to update the location of the individual wearing it. This would lead to a no communication alert, which "are not uncommon and are caused when the device cannot communicate with cell towers for a variety of reasons, such as cellular network issues."[126] A law enforcement organization may not be as concerned about a no communication report as compared to a report of movement beyond the prescribed bounds. A criminal or terrorist could also use a CSS as a means of electronic attack, or to deny communications, while committing a crime or for malicious reasons. For example, a terrorist could attack a location, while simultaneously cutting the phone lines and employing a CSS set up to blacklist users in the surrounding area. This could prevent victims of the attack, or those nearby, from calling law enforcement or emergency medical services.

E. Privacy Concerns

Some cell-site simulators are capable of more than tracking. Some can also be used to gather information or to listen to calls. In fact, the Stingray gathers third-party signals, data, and

[126] Katherine Sayre, *Tracking System Alerted Orleans Parish Sheriff's Office to Problems with Teen's Ankle Monitor, Report Says*, THE TIMES-PICAYUNE, NOLA.COM (last updated Oct. 7, 2012, 9:52 am) http://www.nola.com/crime/index.ssf/2012/10/sheriff_marlin_gusman_and_omni.html.

phone numbers from other cellphones in the area of its operation while locating a target cellphone.[127] In addition to locating cellphones and gathering data, it is possible for a CSS to actually intercept cellphone calls in order to eavesdrop and record them.[128] Whether in the hands of a private individual, or a government actor, privacy implications are raised and cell-site simulators are powerful tools that could be abused to invade the privacy of any cellphone user. In addition to the Stingray, other cell-site simulators are being made commercially available to law enforcement and government agencies. Some manufacturers are fairly transparent about the operation of the device:

Graphic 4: MicroNet GSM IMSI and IMEI Catcher[129]

[127] U.S. v. Rigmaiden, 2013 WL 1932800, at *20 (Dist. Ct. Arizona 2013); 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, 748 (S.D. Texas 2012).

[128] *See* Andy Greenberg, *Despite FCC "Scare Tactics," Researcher Demos AT&T Eavesdropping*, THE FIREWALL, FORBES.COM, (July 31, 2010, 5:35 pm), http://www.forbes.com/sites/firewall/2010/07/31/despite-fcc-scare-tactics-researcher-demos-att-eavesdropping/; Kim Zetter, *Hacker Spoofs Cell Phone Tower to Intercept Calls*, THREAT LEVEL, WIRED.COM (July 31, 2010, 7:57 pm), http://www.wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/; Andy Greenberg, *Flying Drone Can Crack Wi-Fi Networks, Snoop On Cell Phones*, SECURITY, FORBES.COM, (July 28, 2011, 2:11 pm), http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/; *Eavesdropping Drone: New Drone Listens in on Cell Phone Calls and Hacks Wi-Fi Networks*, Homeland Security News Wire (Aug. 5, 2011), http://www.homelandsecuritynewswire.com/new-drone-listens-cell-phone-calls-and-hacks-wi-fi-networks.

[129] *MicroNet GSM IMSI and IMEI Catcher*, PROXIMUS.COM, (last visited Dec. 20, 2013) http://www.proximus.com.ua/MICRONET_GSM_Catcher.html.

> MicroNet series GSM IMSI/IMEI catcher is a device used to detect mobile phones active in specific area as well as to precisely detect their location . . . .
>
> MicroNet acts as a base station and logs IMSI/IMEI identities of all the mobile stations in the selected area. It is also possible to remotely detect mobile phone type and manufacturer.
>
> MicroNet catcher operation is based on real cellular base station (with true MMC/MNC) emulation at frequency channel selected from the list of neighbouring cells in any specific area under different Local Area Code (LAC). All mobile phones within catcher coverage attempt to log into this emulated network, as the signal strength of emulating base station exceeds power levels provided by real base stations.
>
> During the registration process of new mobile devices, the catcher grabs relevant information on terminals IMEI and IMSI, as well as information on downlink signal strength at the mobile device antenna. Collected information on IMSI allows detecting which cellular operator SIM card is used. In future, this information can be used to force mobile terminal activation and enable its tracking. IMEI parameters are used to determine mobile terminal's model.
>
> In case any mobile device subject for further tracking is logged into MicroNet catcher, operator can add its IMSI (IMEI) into separate list (or folder) and use this information during target mobiles search and localization.
>
> Mobile terminal localization is being done with the use of service channel information sent by the mobile as a response to paging requests from MicroNet catcher.
>
> Mobile devices location detection is performed using directional antenna and visual real-time information on received signal strength (at mobile terminal) displayed to MicroNet catcher operator. Other mobile terminals (including those held by MicroNet operator) are not included into the active list and receive "registration failed" message from MicroNet catcher. Consequently, these terminals get registered with their own home networks according to standard authentication procedure.[130]

It is noteworthy that the product description states that the device operates under a different location area and that the non-target phones receive a "registration failed" message.[131] This is a fairly responsible tactic and avoids much of the negative impacts discussed above. It is also

[130] *Id.*
[131] *Id.*

noteworthy that the device uses a frequency from neighboring cells—i.e. from the BA list.[132] Although the capabilities are quite clear, and the privacy concerns along with them, the manufacturer only sells to qualified government and military organizations.[133]

CONCLUSION

Cell-site simulators are a relatively new technology emerging in the public consciousness as its uses, and potential abuses, are becoming increasingly publicized. As with past technological advances, policy makers, judges, lawyers, and private individuals must grapple with the new technology and its implications. Before making decisions with regard to the technology, we must first understand it. Only then, can policy makers and legislatures decide what, if any, laws or regulations are needed. Only then, can a judge rule on a warrant in a fully informed manner, a defense attorney defend against a possible unconstitutional search, and law enforcement agencies and private individuals know the permissibility of using this technology. Understanding the technology is critical to deciding who may possess and use cell-site simulators, to what extent, and for what purposes. This article is designed to be a first step in educating the legal community about cell-site simulators and cellular network technology, and raising issues that will need attention in the near future. By understanding the way cellphones and cellular networks interact, and possible methods of cellphone tracking with a cell-site simulator, we can address the brave new world of cell-site simulators.

[132] *Id.* *See also supra* section II.
[133] *Id.*