Volume 52
Number 3 *Spring 2018*

Spring 2018

Stinging the Stingray: The Need for Strong State-Level Anti-Surveillance Legislation

Gregory Maleska
Valparaiso University

STINGING THE STINGRAY: THE NEED FOR STRONG STATE-LEVEL ANTI-SURVEILLANCE LEGISLATION

I. INTRODUCTION

Daniel Rigmaiden, known to the Federal Bureau of Investigation (FBI) as "the Hacker," is the man who revealed the Stingray to the public.[1] For Rigmaiden, it all started in the Los Padres National Forest in California.[2] There, Rigmaiden, who had virtually no connections to the outside world, devised a tax-fraud scheme.[3] Using only his laptop and AirCard, a device that is used to get Internet service for a laptop via cellphone tower, Rigmaiden successfully filed hundreds of fraudulent tax returns from deceased Californians.[4]

Rigmaiden's only problem was accessing the money: he needed to obtain it without being traced.[5] To do this, he set up debit card accounts using fake identities.[6] He resided in a hotel room in the city to make it

---

1 *See* Cale Guthrie Weismann, *How An Obsessive Recluse Blew The Lid Off the Secret Technology Authorities Use to Spy On Peoples' Cellphones*, BUSINESS INSIDER (June 19, 2015), http://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6 [https://perma.cc/6SZF-FGN8] (detailing Daniel Rigmaiden's story about how he was able to uncover a device that was before completely hidden from the public); *American Greed: Hack Me if You Can* [hereinafter *Hack Me if You Can*] (NBC television broadcast Aug. 25, 2016) (providing the FBI's account of the investigation that eventually led to the arrest of Daniel Rigmaiden, who at the time was so well-hidden that the police referred to him only as "the Hacker.").

2 *See Note to Self: When Your Conspiracy Theory is True*, WNYC PUBLIC RADIO (June 19, 2015) (recording available at http://www.wnyc.org/story/stingray-conspiracy-theory-daniel-rigmaiden-radiolab/) [hereinafter *When Your Conspiracy Theory is True*] (explaining how Rigmaiden's anti-government tendencies and computer savvy led him to setting up the scheme).

3 *See* Rebecca McCray, *From Con Artist to Government Combatant: A Recluse Comes Out of Hiding*, TAKEPART (Feb. 4, 2016), http://www.takepart.com/article/2016/02/04/daniel-rigmaiden-stingray-truth-and-power [https://perma.cc/9BCT-AUKP] (addressing Rigmaiden's reclusive behavior, his tax-fraud scheme, and how he used these to his advantage).

4 *See When Your Conspiracy Theory is True*, *supra* note 2 (stating that the tax-fraud scheme to take from hundreds of Californians was working very well at the outset). *See also Hack Me if You Can*, *supra* note 1 (explaining that, to the Federal Bureau of Investigation FBI the system that Daniel Rigmaiden had set up was nearly untraceable); Melanie Pinola, *What Is an Aircard? Mobile Office Technology*, LIFEWIRE (Oct. 12, 2016), https://www.lifewire.com/what-is-an-aircard-2377410 [https://perma.cc/2AZK-HEQ6] (describing the functionality of an AirCard, which is generally a small card that plugs into a USB and connects a remote laptop to nearby cell towers to connect the laptop to the internet).

5 *See Hack Me if You Can*, *supra* note 1 (pointing out that the best way to accomplish the feat of withdrawing money without being traced is to use debit cards).

6 *See* Weismann, *supra* note 1 (describing that Rigmaiden was able to accomplish this with relative ease because of the fact he created numerous fake ID's and was completely out of the public eye). *See also Hack Me if You Can*, *supra* note 1 (explaining the meticulous care that

easier to withdraw money from ATMs, but to maintain his anonymity he needed to spread out his withdrawals and set up accounts at several different banks.[7] Eventually, he realized that with the help of accomplices, he could withdraw enough money to leave the country and start a new life.[8] Thus, he turned to anonymous internet message boards to recruit people willing to withdraw the money from the IRS to put onto debit cards.[9]

Rigmaiden, using only his laptop computer and Aircard, knew that with current technology he was untraceable, so he had a false-sense of security.[10] Soon, however, the FBI was able to track down one of his accomplices, and the police narrowed his general location to Palo Alto, California.[11] At that time, the police officers conducted a sweep search using a Stingray—which was completely shielded from the public at the time—and found Rigmaiden using the International Mobile Subscriber Identity (IMSI) number that matched Rigmaiden's AirCard.[12]

In a radio interview, Rigmaiden described the moment of his arrest, "when I was laying on the sidewalk getting handcuffs put on me, I instantly knew that they had tracked the AirCard down, . . . it was the only weak link in the operation." [13] While in prison, Rigmaiden spent his days tirelessly trying to uncover the device that pinpointed his location by going through thousands of Freedom of Information Act (FOIA)

Rigmaiden took to not get caught throughout the scheme, even going so far as to sign his signature on bank papers by palming the pen in such a way as to not give up finger prints).

7 *See Hack Me if You Can*, *supra* note 1 (illustrating that Rigmaiden was living a secluded lifestyle while in his hotel room, and most of his day was spent walking to random ATMs to take out modest withdrawals so as not to trigger suspicion).

8 *See When Your Conspiracy Theory is True*, *supra* note 2 (stating his own account of the plan, Rigmaiden believed that this was going to give him enough money to get out while he was ahead).

9 *See Hack Me if You Can*, *supra* note 1 (reminiscing the investigation, the FBI agents working the case believed that the main flaw in Rigmaiden's scheme was when he reached out for accomplices).

10 *See id.* (detailing how investigators were able to find one of Rigmaiden's accomplices with a tip from a post office worker in Arizona who discovered suspicious mailings going to a particular address, all being identical but addressed to different names).

11 *See When Your Conspiracy Theory is True*, *supra* note 2 (explaining that once the police had Rigmaiden's general area the investigation was far from over because they had no way of tracing Rigmaiden using traditional investigatory techniques).

12 *See id.* (describing the government's use of the secretive Stingray-device to find Rigmaiden, which would not have been possible otherwise). *See also infra* Part II.A.2 (explaining the basics of Stingray technology); sources cited *infra* note 45 (explaining that an International Mobile Subscriber number, IMSI number, is an individualized number given to each cellphone or AirCard that identifies the device).

13 *See id.* (recalling the thoughts going through Rigmaiden's mind at the time of arrest).

documents until discovering enough evidence to blow the lid off the Stingray, which turned out to be a tightly-held government secret. [14]

This Note recommends that states should continue enacting or amending statutes that control the use of the Stingray by both police officers and private citizens by proposing a three-fold approach that state legislators should consider.[15] Part II explains the technology of the Stingray, the history of the device, and various legal standards that apply to police searches under the Fourth Amendment.[16] Next, Part III argues that the third-party doctrine is inapplicable to the Stingray, analyzes state and federal law, and concludes that the current federal standards do not fit well with the various capabilities of the Stingray.[17] Finally, Part IV proposes that states should consider a threefold approach when enacting or amending Stingray legislation.[18]

II. BACKGROUND

First, Part II.A explains what the Stingray is and how it functions.[19] Then, Part II.B discusses how the federal government went to extreme measures to keep the Stingray from public disclosure.[20] Next, Part II.C discusses applicable Supreme Court jurisprudence regarding the use of the Stingray.[21] Finally, Part II.D explores potential sources of federal law and developing state statutes that apply to the Stingray.[22]

A. Dissecting the Stingray

This section provides background information about what the Stingray is and how it functions, which is essential to understanding what

---

14 *See* McCray, *supra* note 3 (noting that the government handed over 14,000 pages of evidence that they used to prosecute Rigmaiden).

15 *See infra* Part IV (offering the author's proposed legislative approach).

16 *See infra* Part II (providing background information relating to the Stingray and potential legal standards that may apply to police use of the device).

17 *See infra* Part III.B (analyzing various federal standards including the Pen Register statute and the Wiretap Act).

18 *See infra* Part IV (arguing that the best approach legislatures can take involves a combination of strict warrant requirements, deterrence, and judicial oversight).

19 *See infra* Section II.A (exploring the basic functions of cellphone technology and then describing how the Stingray can manipulate the technology to access communications, location, and device information of the cellphone).

20 *See infra* Section II.B.1 (discussing the coordinated secrecy between the FBI and state governments to keep the Stingray away from the public eye by requiring non-disclosure agreements).

21 *See infra* Section II.C (explaining pertinent Supreme Court cases that have analyzed the Fourth Amendment's reasonable expectation of privacy).

22 *See infra* Section II.D (addressing several sources of federal law regarding communication interception and more recent initiatives to limit the use of the Stingray).

standards should be enacted for use of the Stingray.[23] First, Part II.A.1 gives background information on how cellphones connect to cell towers and how the technology has evolved over the years.[24] Then, Part II.A.2 explains how the Stingray manipulates cellphone technology.[25]

1. The Basics of Cellphone Technology

Before understanding the Stingray, it is useful to understand that cellular telephones ("cellphones") send and receive radio waves, which are inherently interceptable.[26] The cellphone is merely a sophisticated version of a two-way radio.[27] Cellphones emit a low-powered radio frequency that sends and receives information by connecting to a nearby cellphone tower.[28] Similar to a radio, close proximity to the cell tower will generally lead to better reception unless the signal is obstructed.[29] Cellphones connect to the approximately 215,000 cell towers in the United States.[30] These cell towers are all subject to licensing requirements by the Federal Communication Commission (FCC).[31]

---

[23] *See infra* Part II (giving necessary information into the inner-workings of the Stingray).

[24] *See infra* Part II.A (explaining how basic cellphone technology works similar to a radio, and that all cellphones within range will automatically connect to towers around them).

[25] *See infra* Part II.B (discussing the way in which the Stingray is able to act as a fake tower and manipulate the auto-connectivity of cellphones to cell towers).

[26] *See infra* Part II.A.1 (providing background information on how cellular technology works).

[27] *See* Rong Wang, *How Do Cell Phones Work?*, PONG BLOG (Dec. 20, 2014), http://www.pongcase.com/blog/cell-phones-work/ [https://perma.cc/QAB4-96AT] (comparing current cellphone technology with that of a two-way radio and explaining how the technology developed to its current form).

[28] *See id.* (discussing how cellphones use a transmitter and a receiver to connect with cell towers). *See also* Michael Miller, *How Mobile Networks Work*, QUE (Mar. 14, 2013), http://www.quepublishing.com/articles/article.aspx?p=2021961 [http://perma.cc/TA43-AXLV] (explaining the use of very low powered radio frequency transmissions to contact nearby cell towers, or "base stations"). These base stations are geographically located in hexagonal areas with minor overlap to ensure the best cell reception to all cellphones within range. *Id*.

[29] *See* Wang, *supra* note 27 (noting that certain "impediments" can weaken signal strength). *See also* Ken Perkins, *The Top 5 Surprising Things You Didn't Know Could Block Your Cell Signal*, WEBOOST BLOG (Apr. 6, 2016), https://blog.weboost.com/news/blog/the-top-5-surprising-things-you-didnt-know-could-block-your-cell-signal/ [https://perma.cc/H25Q-8Z5F] (stating that some common cellphone weakening factors can include far proximity from the cell tower, the type of terrain, buildings, bridges, cars, foliage, and varying conditions in the atmosphere).

[30] *See Cell Phone Tower Statistics*, (June 12, 2016), http://www.statisticbrain.com/cell-phone-tower-statistics/ [https://perma.cc/324K-6ZBR] (providing that 215,000 cell towers are located in the United States, each of which has a maximum range of 21.7 miles).

[31] *See Tower and Antenna Setting*, (Sept. 20, 2016), https://www.fcc.gov/general/tower-and-antenna-siting [https://perma.cc/B2CU-GH7T] (explaining the FCC requirements for cell phone towers). *See also* Jason Norman, *Taking the Sting out of the Stingray: The Dangers of*

Cellphone technology is categorized by four generations.[32] The same basic radio technology is used for each generation, but cell data has evolved mostly from the technological development of frequency waves.[33] During the First Generation of cellphone technology ("1G"), cellphones sent out only analogue data that gave the user the ability to make phone calls.[34] As the technology developed, service providers turned to more-sophisticated data transmissions using digital transmissions as opposed to analogue transmissions.[35] The digital-to-analog development is what signified the Second Generation ("2G"), which gave rise to the ability to send text messages and slow, but usable, web browsing capabilities.[36] The Third Generation ("3G") focused on faster Internet usage for smartphones that drastically increased the speed of digital communication.[37] Currently, cellphone technology is still in the Fourth Generation ("4G").[38] The 4G

Cell-Site Simulator Use and the Role of the Federal Communications Commission in Protecting Privacy & Security, 68 FED. COMM. L.J. 139, 176–77 (2016) (positing that FCC could hold police agencies subject to encryption regulations by creating an administrative rule under Title II of the Federal Communications Act, which allows the FCC to regulate encryption).

32 *See* Dan Cudjoe, *Review of Generations and Physics of Cellphone Technology*, 4 INT'L J. OF INFO. SCI. 1, 2 (discussing the history and four generations of cellular technology, including the outlook for the fifth generation of cellular technology).

33 *See id*. (noting the existence of radio technology even after the technological jumps from each generation). *See also* Miller, *supra* note 28 (detailing that the evolution of frequency band technology was key to increasing the speed and capabilities of cellular networks).

34 *See* Miller, *supra* note 28 (providing that the first generation of cellular technology relied on analogue data).

35 *See* Miller, *supra* note 28 (distinguishing between the first and second generation based on the development of digital transmissions and stating that Second Generation internet usage is "painfully slow"). *Compare Digital Technology*, *Dictionary of American History* (2003) ("Digitized information is recorded in binary code of combinations of the digits 0 and 1, also called bits, which represent words and images.") *with analogue, vocabulary.com* (2016) ("Analog is the opposite of digital . . . [a]ny technology, such as vinyl records or clocks with hands and faces, that doesn't break everything down into binary code to work is analog").

36 *See* Miller, *supra* note 28 (explaining that the advent of digitized information in cell technology also brought the capability to transfer text messages or even access the internet, although usable internet was more of a focus for the Third Generation of cellular technology).

37 *See* Miller, *supra* note 28 (emphasizing that the Third Generation is geared towards enabling smartphone capabilities). *See also* Chris Woodford, *Mobile Broadband* (June 9, 2016), http://www.explainthatstuff.com/mobilebroadband.html [https://perma.cc/FP2W-2WX3] (explaining that the reason for much higher speeds was due to the fact that multiple phones could be using the same radio frequency simultaneously, which allows for data transfer similar to the way the internet works).

38 *See* Cudjoe, *supra* note 32 (noting that cellphone technology currently still in the Fourth Generation, but that the Fifth Generation of wireless cellular technology is expected to arrive by 2020).

network is considerably faster because it connects users to a high-speed mobile broadband network.[39]

2. A Brief Overview of the Capabilities of Stingray Technology

"Stingray" is the brand name of one of the more popular devices in the family of IMSI catchers, but for this Note all mentions of the various types of IMSI catchers will be referred to as "Stingray."[40] The Stingray was produced by the Harris Company, which has gone through great lengths to keep the technology from being publicly disclosed.[41] As discussed previously, cellphones work by automatically connecting to the closest cell tower.[42] The Stingray manipulates a cellphone's automatic-connectivity by serving as a fake tower.[43] With this capability, it gathers not only the information from the target cellphone, but all cellphones within its range and then targets a particular device to glean even more user information from the target.[44]

---

[39] *See* Woodford, *supra* note 37 (suggesting that the Fourth Generation of cellular technology further allows for multiple users on the same frequency by using Orthogonal Frequency-Division Multiple Access technology).

[40] *See* Notice of Acceptance of § 8 Declaration and § 9, Renewal (Apr. 24, 2013), http://tsdr.uspto.gov/documentviewer?caseId=sn76303503&docId=SPE20130404144554#docIndex=0&page=1 [https://perma.cc/998M-VWAH] (accepting the Harris Corporation's Trademark for the Stingray). *See also Government Cellphone Surveillance Catalogue*, (Dec. 17, 2015), https://theintercept.com/document/2015/12/16/government-cellphone-surveillance-catalogue/ [https://perma.cc/2DB9-HMD5] (exposing the various types of IMSI-catchers, including new devices that are specially designed to circumvent 4G security features).

[41] *See* Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, INTERCEPT (Sept. 12, 2016), https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/ [https://perma.cc/5B3L-A2NX] (detailing the efforts that Harris has made in maintaining secrecy of their owners' manuals by claiming that it could hurt their competitive interests and allow for criminals to have access to the information).

[42] *See* Miller, *supra* note 28 (describing how cellphones automatically connect to cell towers by using a low-powered transmitter).

[43] *See Stingray Tracking Devices*, ACLU (2015), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices [https://perma.cc/D4KT-T6DT] (defining the key capabilities of Stingrays by stating that "Stingrays . . . are invasive cell phone surveillance devices that mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information.").

[44] *See* Kate Klonick, *Stingrays: Not Just for Feds!*, SLATE (Nov. 10, 2014), http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.html [https://perma.cc/5R3C-XAXY] (providing that all cellphones within range of the tower will automatically connect to the Stingray).

First, Stingrays are able to gather certain device information.[45] For instance, one key piece of user information that the Stingray gathers is the IMSI number.[46] The IMSI can identify the mobile subscriber because it is a user-specific identification number.[47] The Stingray can also gather other information about the device, including the device's serial number, and Mobile Identity Number (MIN), if the target sends or receives a text message.[48] Beyond just device information, police officers can view whom the user is currently contacting.[49] These communications can include either voice calls or text messages.[50] Not only can the Stingray user view the cellphone information, but officers can also log this information on an accompanying software program.[51] These software programs can show the devices that have communicated with each other within the Stingray's radius.[52]

---

45 *See infra* notes 59–66 and accompanying text (explaining the types of device information that is taken when a cellular device is targeted by the Stingray).

46 *See Gemini Quick Start Guide* (Sept. 22, 2014), https://www.documentcloud.org/documents/3105793-Gemini-3-3-Quick-Start-Guide.html [https://perma.cc/F2DZ-HXF5] at 13 (instructing users about how to collect the IMSI from all cellular devices within range).

47 *See International Mobile Subscriber Identity*, TECHOPEDIA (Oct. 23, 2016), https://www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi [https://perma.cc/TK7F-TJ6N] (defining the IMSI number as "a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users . . . [t]he IMSI is a unique number identifying a GSM subscriber.").

48 *See Gemini Quick Start Guide*, *supra* note 46, at 13 (providing that the serial number is one of the pieces of identifying information that can be gathered from a subscriber who connects to the Stingray). *See also* Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, WIRED (Sept. 28, 2015), https://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/ (relying on documents from the American Civil Liberties Union (ACLU) that give guidelines for police officers and provide that the target's phone number can be gathered after the target has connected to the Stingray if the target sends or receives a phone call or text message).

49 *See Gemini Quick Start Guide*, *supra* note 46, at 26 (describing how the logging process can be completed by the Stingray user). *See also* United States v. Tutis, Crim. No. 14-699, 2016 WL 6136577 at *2 (D.N.J. Oct. 20, 2016) (referring to a government wiretap request that specifically stated that the IMSI catcher was only going to be used to determine the location of the data, and "not to obtain any written or oral communications," indicating that the IMSI catcher has the ability to determine location).

50 *See* Klonick, *supra* note 44 (stating that all devices connected to the Stingray furnish their outgoing calls and texts).

51 *See generally Gemini Quick Start Guide*, *supra* note 46 (enabling users to easily use the technology on PC-based computer platforms).

52 *See Gemini Quick Start Guide*, *supra* note 46 (explaining how the Stingray shows devices who have communicated with each other by viewing the incoming and outgoing messages and matching it to the other cell numbers within the vicinity).

Second, Stingrays have the ability to actively intercept or block voice and text communications.[53] They send a signal to the selected cellphone asking it to respond with communication data.[54] Acting as a celltower, the Stingray can copy the unencrypted digital data and the user, presumably a police officer, can view the Short Message Service (SMS) message, or listen to the phone call in real-time.[55] The Stingray can also accomplish phone and text interception by knocking the cell connection from 3G, 4G or Long-Term Evolution (LTE) down to the less-secure 2G.[56]

Finally, the Stingray has the ability to triangulate cellphone users' coordinates similar to a Global Positioning System (GPS), or the "Find my Friends" app.[57] In fact, the Stingray user manual shows that the software allows for a Google Earth plug-in.[58] Police can view all the cellphone users within its radius, and target any user's location based on their device's information.[59]

---

[53] *See* Zetter, *supra* note 48 (citing documents released by California law enforcement that show police officers have the ability to listen to voice calls and view texts with the Stingray and gives the legal guidelines police officers should follow while using the device). *See also* Robert Kolker, *What Happens When the Surveillance State Becomes an Affordable Gadget*, BLOOMBERG (Mar. 10, 2016), http://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget [http://perma.cc/MBZ6-W64Q] (describing the procedure that Stingray devices or more-advanced IMSI catchers can use to infiltrate text messages and calls of 3G and 4G networks).

[54] *See* Jason Hernandez, *How IMSI Catchers Work*, NORTH STAR POST (Dec. 16, 2015), https://www.nstarpost.com/news/how-imsi-catchers-work/ [https://perma.cc/5KXD-,HY57] (diagramming the process that the Stingray uses as acting as a fake cell tower, and showing that cell towers have a fair amount of discretion in instructing cellphones how to operate).

[55] *See id.* (explaining how the Stingray deploys the "man-in-the-middle" attack and can furnish information from the unsuspecting cellphone user).

[56] *See* Biddle, *supra* note 51 (detailing the procedure that police officers can use to accomplish the "knocking" procedure using a Stingray). *See also* Kolker, *supra* note 53 (explaining that although it was originally assumed that Stingrays were incapable of intercepting calls and texts, it has been proven that the knocking process has already been deployed by the Hailstorm, which is a type of IMSI catcher).

[57] *See* Hernandez, *supra* note 54 (describing that once connected to the cellphone, the Stingray—acting as a fake cell tower—can instruct the cellphone to reconnect too frequently and thus turn the cellphone into a "beacon" of the users location). *See also About Find my Friends*, APPLE (2016), https://support.apple.com/en-gb/HT201493 [https://perma.cc/manage/create] (explaining the iPhone application that allows users to permit location access to other users).

[58] *See iDen Transceiver Operations Manual* 93 (2013) https://www.documentcloud.org/documents/3105641-iDEN-2-4-Operator-Manual.html [https://perma.cc/2CDL-FR7F] [hereinafter *Operations Manual*] (giving the Stingray operator the directions on how to download a Google-earth plug-in to use with the software).

[59] *See id.* (detailing how the map plugin can monitor multiple cellphone subscribers within the device's radius). To accomplish this, the user manual states:

> Map Router is capable of calculating Location Finding estimates for multiple subscribers. Current Location Finding estimates for each

B. From Warzones to Squad Cars: The Pandemic Rise of the Stingray in Policing Agencies

On August 21, 2001, the Harris Corporation filed a United States trademark registration form for the name "Stingray."[60] At the outset, Stingrays were developed for the Central Intelligence Agency (CIA) as a spying tool to circumvent international cellphone companies that would not give the CIA access to their phone records.[61] But soon, the Harris Corporation had created a market for the Stingray outside of the federal intelligence community, and other administrative agencies bought the device.[62] Like any other market, the devices and software developed, so that intelligence agencies would buy newer models and sell the older models to lower-level agencies.[63]

Presently, it is generally understood that police use the Stingray in four types of scenarios: (1) identifying cellular devices in use by an identified suspect; (2) more precisely locating devices when a phone carrier is incapable; (3) electively blocking devices or dialed numbers; and

---

> enabled subscriber are sent to all enabled map outputs. Results for all subscribers are retained until the results are manually changed or the input to Map Router is changed.

Id.

60 *See Stingray Trademark Information*, TRADEMARKIA (Oct. 27, 2016), http://www.trademarkia.com/stingray-76303503.html [https://perma.cc/5XP5-K2CX] (providing the dates of the Stingray's copyright, as well as additional information about the copyrighted material).

61 *See* Larry Greenemeier, *What Is the Big Secret Surrounding Stingray Surveillance?*, SCIENTIFIC AMERICAN (June 25, 2015), https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/ [https://perma.cc/9TA4-FLQT] (explaining the history of how Stingrays came into existence).

62 *See id.* (discussing the "trickle-down" effect, whereby the device started in the hands of military and intelligence agencies and eventually landed in the hands of local police officers). *See also Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them?redirect=maps/stingray-tracking-devices-whos-got-them [https://perma.cc/E84E-RY5D] [hereinafter *Who's Got Them?*] (providing that the federal agencies known to use the Stingray, including: the FBI, the Drug Enforcement Administration, the United States Secret Service, Immigration and Customs Enforcement, the United States Marshal Service, the Bureau of Alcohol, Firearms, and Explosives, the Internal Revenue Service, the United States Army, the United States Navy, the United States Marine Corps, the United States National Guard, the United States Special Operations Command, and the National Security Agency).

63 *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J. L. & TECH. 1, 76 (2014–2015) (discussing the how the market for the Stingray expanded from the FBI, to state and local governments, and now is so widespread that citizens have access to the device). *See also Who's Got Them?*, *supra* note 62 (noting that twenty-four states and the District of Columbia are now known to be using the technology with either the state or local police forces).

(4) military and foreign intelligence.[64] Although these scenarios suggest that the police uses are potentially limited, it has been reported that some police agencies use the Stingray routinely during drug, burglary, and murder investigations.[65]

In an effort to shield the inner-workings of the Stingray from the public—especially from terrorists or criminals who could potentially harm the public—the FBI required state and local police agencies to sign non-disclosure agreements as a condition to buying the device.[66] Indeed, the FBI-mandated non-disclosure technique successfully kept the device completely shielded from the public eye, until two notable cases helped uncover the truth.[67]

In 2012, Daniel Rigmaiden appealed his case on several grounds in the pre-trial stages of his prosecution.[68] Rigmaiden challenged the constitutionality of the search as violating his legitimate expectation of privacy and by obtaining historical records from his AirCard.[69]

---

[64] *See* Pell & Soghoian, *supra* note 63, at 17–18 (explaining that first situation is implemented by using sweep searches that look through phones in local areas where the suspect is likely to be located). The second situation occurs in situations where a cellphone provider is unable to "ping" the location data of the cellphone. *Id.* The third situation allows police to target a device or group of devices and cut off all wireless capabilities to the affected cellular devices. *Id.* The final situation occurs in war zones, and was the original use of the Stingray's capabilities. *Id. See also In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 747 (S.D. Tex. 2012) (exemplifying the second situation, whereby law enforcement used a Pen Register application seeking to track the suspect using a police vehicle and Stingray in order to determine the suspects telephone number).

[65] *See* John Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, LA WEEKLY (Jan. 24, 2013), http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739 [https://perma.cc/F7PL-C3RQ] (exposing the widespread use of the Stingray by the LAPD, using the device over twenty-one times in a four-month period for seemingly routine investigations).

[66] *See* Pell & Soghoian, *supra* note 63, at 38 (discussing at length how police enforcement agencies used the non-disclosure agreements for years to use the Stingray and how they masked the actual capabilities of the technology from judges).

[67] *See infra* Section II.A–B (explaining revelations made during Daniel Rigmaiden's pre-trial legal proceedings, as well as a judge's denial of a request of a Pen Register order to use a Stingray).

[68] *See* United States v. Rigmaiden, 844 F. Supp. 2d 982, 988–99 (D. Ariz. 2012) (providing the many appeals that Rigmaiden lodged regarding civil rights violations made by the government in attaining his personal information and tracking him down). These appeals included challenges to warrants based on probable cause, particularity, and exceeding the scope of the warrants. *Id.*

[69] *See* United States v. Rigmaiden, CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013) (explaining that in issuing his decision the Judge presiding over Rigmaiden's trial made a finding of probable cause). The judge found that "the use and monitoring of a mobile tracking device" would "lead to evidence of" several specific crimes, including conspiracy to defraud the government, fraud relating to identity information, aggravated identity theft, and wire fraud, "as well as to the identification of individuals who are engaged

Interestingly, the prosecution conceded that use of the Stingray, which was not explicitly named in the case, constituted a Fourth Amendment search.[70] However, the judge still found that all of the numerous Fourth Amendment challenges were satisfied.[71]

Luckily for Rigmaiden, the prosecution saw another side of him during the nearly six-year-long legal battle after his arrest.[72] In fact, the prosecution urged the judge to circumvent federal sentencing guidelines.[73] Rigmaiden ultimately pled guilty to four felonies, and in return he was given time-served, community service, and required to return the stolen tax money.[74]

During the final stage of the Rigmaiden prosecution, a magistrate opinion from Texas discussed the Stingray.[75] In this case, the Drug Enforcement Agency (DEA) attempted to track a suspect believed to be using a burner phone by filing for a pen register application, but the judge denied the request on two grounds.[76] First, the Stingray could gather

---

in the commission of these offenses." *Id.* The judge also found that Rigmaiden did not have a legitimate expectation of privacy in his AirCard, laptop, or apartment specifically because they were "procured through fraud." *Id* at *8.

70 *See Rigmaiden*, 2013 WL 1932800, at *15 (stipulating to the fact that the search with the Stingray qualified as a Fourth Amendment search and seizure of information); *infra* Part II.C (discussing the Supreme Court's constitutional interpretations of the Fourth Amendment).

71 *See Rigmaiden*, 844 F. Supp. 2d at 995–96 (finding that "[f]or purposes of Defendant's Fourth Amendment arguments, that the search for the aircard was a search within the meaning of the Fourth Amendment"). Notably, in one proceeding where Rigmaiden wanted disclosure of additional discovery related to the Stingray that was concealed from the public at the time the Judge stated that the government had reason to suppress the techniques it used because "[the government's] disclosure would therefore seriously hamper future law enforcement efforts." *Id.* at 988.

72 *See* Dennis Wagner, *Tax Scammer Rigmaiden Pleads Guilty, Gets Time Served,* ARIZONA REPUBLIC (Apr. 8, 2014), http://www.azcentral.com/story/news/politics/2014/04/07/rigmaiden-tax-scammer-pleads-guilty/7448151/ [https://perma.cc/D9CD-GAF3] (explaining to the Court that he believed the defendant had turned over a new leaf, the prosecutor stated that, "I honestly believe the defendant has made a decision to enter society and become a law-abiding member.").

73 *See id.* (discussing the judge's predisposition that he would dismiss the defendant's appeal, but that he respected the wishes of the prosecution).

74 *See id.* (detailing the plea deal that the prosecution reached with Rigmaiden after a sixty-eight month pre-trial battle).

75 *See In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012) (referring to the word "stingray" in reference to an IMSI-catcher for the first time in any judicial proceeding).

76 *See id.* at 748 (describing that the target was previously using a different telephone and was believed to have switched to a new one that the DEA did not know). *See also* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 204 (2014) (explaining the planned police procedure to track the suspected narcotics trafficker). Specifically, the police did not have the cellphone number of the defendant, so

cellphone information from unintended targets, and the requesting agent did not seem to know what would become of the information from the unintended cellphone user information that might get swept up in the Stingray search.[77] The judge relied in part on the *Rigmaiden* proceedings, whereby the government conceded that the use of a cell-site simulator was a justifiable search for purposes of the Fourth Amendment.[78]

Second, the judge denied the request because the Federal Pen Register Statute requires that the government "have a telephone number or some similar identifier before issuing an order."[79] Therefore, because the Federal Pen Register Statute requires information that the DEA was unable to provide before conducting the search, the judge found that the request was not adequate.[80] Because the Federal Pen Register Statute requires a lower showing than a warrant, the court held that the pen register was not sufficient for the diverse capabilities of the Stingray.[81]

---

they planned to follow the suspect in a police vehicle while using the Stingray to determine his cellphone number. *Id.*

77 *See* Owsley, *supra* note 76, at 204 (stating that the record on such devices was very limited, and that in the only other comparable case, the government had procured a warrant rather than a Pen Register order).

78 *See In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747 at 748 (describing the use of the Pen and Trace order as not being adequate considering the government's concession that a cell site simulator required a warrant). *See also supra* note 70 and accompanying text (analyzing the concession made by the government that the cell-site simulator indeed required a warrant to satisfy the Fourth Amendment).

79 *See In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747 at 751 (referring to the pen register application statutory language, which requires digital identifying information about the target is who is sought). *See also infra* notes 153–71 and accompanying text (discussing the exceedingly low requirements for issuance of a pen register order); *Pen Register*, BLACK'S LAW DICTIONARY (10th ed. 2014):

> An electronic device that tracks and records all the numbers dialed from a particular telephone line, as well as all the routing, addressing, or signaling information transmitted by other means of electronic communications. [] Because a pen register does not record the contents of any communication, it may not constitute a Fourth Amendment search requiring a search warrant though it does need a court order.

Id. (internal citation omitted).

80 *See In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 751 (S.D. Tex. 2012) (holding that the DEA lacked the specificity that is required for a pen register request). *See also* Owsley, *supra* note 76, at 205 (explaining that the pen register statute required more information than the suspect's telephone number because "given the absence of a known cell phone number target, neither case law nor statutory language supported the applicability of the pen register statute to an application for a cell-site simulator").

81 *See infra* Part II.C (analyzing the use of the pen register statute in light of the various capabilities of the Stingray).

C. *Supreme Court Jurisprudence on the Fourth Amendment's Protection from Electronic Surveillance*

The Fourth Amendment of the U.S. Constitution states: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[82] To determine how the Fourth Amendment applies to the government's use of the Stingray, it is useful to think of the Stingray's capabilities separately, as follows: (1) the ability to view incoming and outgoing telephone numbers; (2) the ability to track the location of the device; and (3) the ability to intercept communications.[83] Due to government secrecy, courts have recently faced evidentiary admissibility questions about the unwarranted use of the Stingray.[84] Because no statute directly addresses the admissibility of such evidence in these states, the courts relied on the analogous Supreme Court case law in ruling that Stingray-acquired evidence requires a warrant.[85]

In 1967, the Supreme Court decided its first landmark case regarding police surveillance of a phone line.[86] The Court held that every citizen has a reasonable right to privacy under the Fourth Amendment.[87] However,

---

82 U.S. CONST. amend IV.

83 *See supra* Part II.A (describing how the Stingray can glean user information, intercept texts and calls, and track cell phones). *See also* U.S. v. Lambis, 197 F.Supp.3d 606, 606–11 (S.D.N.Y. July 12, 2016) (exploring the Fourth Amendment considerations of the ability to triangulate user identification); *In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d at 747, 752 (determining that the pen register statute did not cover the government's request to glean device information that would pinpoint a suspected drug trafficker).

84 *See* Maryland v. Andrews, 134 A.3d 324, 353 (Md. Spec. App. 2016) (holding that the unwarranted use of a Stingray-like device violated the defendant's reasonable expectation of privacy); *Lambis*, 197 F.Supp.3d at 616 (denying admission of evidence gathered from a Stingray); United States v. Tutis, CR 14-699 (JBS), 2016 WL 6136577, at *6 (D.N.J. Oct. 20, 2016) (holding that a wiretap order satisfied the Fourth Amendment's particularity requirement whereby the government needs to show that the warrant has a particular description of property that is to be seized).

85 *See infra* Part III.C (discussing states that have enacted statutes); *Andrews*, 134 A.3d at 336–37 (analyzing the Supreme Court decisions regarding the Fourth Amendment search); *Lambis*, 197 F.Supp.3d 606, at 606–11 (relying on several Supreme Court rulings in determining that Stingray-acquired evidence requires a warrant).

86 *See* Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966), *rev'd*, 389 U.S. 347 (1967) (holding that the FBI was required to get a warrant before listening into and recording phone calls of the defendant). After an FBI Agent overheard Charles Katz's conversation regarding a potential violation of federal gambling law, the agent placed a microphone outside of a public phone booth that recorded Katz's phone call. *Id.* at 131.

87 *See* Katz v. United States, 389 U.S. 347, 350 (1967) (creating the precedential 'reasonable expectation of privacy' standard). Specifically, the Court recognized that the officers were required to get a warrant *before* placing the microphone, and the search could not be

the *Katz v. United States* decision left the door open for future litigation by stating "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[88] This language would eventually become the basis for what is known as the third-party doctrine.[89]

The third-party doctrine is a major exception to the reasonable expectation of privacy and gives no Fourth Amendment protection to information divulged to the public.[90] In *Smith v. Maryland*, the Supreme Court held that law enforcement officers were within their Constitutional rights when viewing incoming and outgoing telephone calls stored in a pen register.[91] Such a device, the Court said, was not subject to an expectation of privacy because the digits of the telephone number were voluntarily given over to the telephone company when making the phone call.[92]

Another exception is the "good faith" exception to the exclusionary rule.[93] This exception applies in situations where the government has

---

considered reasonable even if the police were able to establish probable cause after they had already installed the microphone. *Id.* at 356 (emphasis added).

88 *Id.* at 351. *See also* Steven M. Bellovin & Matt Blaze, *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 3 (2016) (explaining how the *Katz* decision only addressed the specific content of the phone call, not the non-content information such as the numbers dialed).

89 *See* United States v. Thomas, 2015 WL 10634507, at *5 (E.D. Pa. 2015) (discussing the Constitutional basis of the "third-party doctrine"). *See also Third-Party Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("The principle that one has no reasonable expectation of privacy in information that one has voluntarily disclosed to one or more third parties").

90 *See* Simon Stern, *The Third-Party Doctrine and the Third Person*, 16 NEW CRIM. L. REV. 364, 365 (2013) (detailing how the third-party doctrine defines the reasonableness of the privacy expectation under the Fourth Amendment). The distinction can be made between public and private information, and if the government gleans information that falls into the former category, it is not subject to a reasonable expectation of privacy. *Id.* This exception will even apply if there has not been an affirmative consideration that the information is meant to be public. *Id.*

91 *See* 442 U.S. 735, 736 (1979) (holding that using information from a pen register was not a Fourth Amendment search). The petitioner, who was found to have robbed a home, began making threatening phone calls to the victim. *Id.* at 737. Police gathered the personal information of the petitioner, and installed a pen register without a warrant to determine whether he was making the phone calls to the victim. *Id.* After the prosecution used the unwarranted pen register evidence, the petitioner argued that the installation of a pen register required a warrant. *Id.*

92 *See id.* at 735–36 ("When petitioner voluntarily conveyed numerical information to the phone company . . . he assumed the risk that the company would reveal the information to the police.").

93 *See* United States v. Leon, 468 U.S. 897, 890 (1984) (providing another exception to the warrant requirement, which allows police officers acting in good faith to be excused from minor defects in the warrant process). In this landmark case, the police officer gathered information from an informant and subsequently procured a judge-issued search warrant. *Id.* The search turned up evidence that the suspect was indeed involved in a drug dealing

attempted to fulfill the warrant process, but some type of a defect in the warrant process has occurred.[94] In general, the rationale for this rule is that an officer who has relied on a judge's approval of a warrant should not be penalized by having the evidence excluded for trial due to a warrant defect.[95]

The Supreme Court has also had occasion to rule on the Constitutionality of unwarranted location tracking.[96] In *Kyllo v. United States*, the Court held that unwarranted location tracking inside the home is a violation of the Fourth Amendment.[97] In this case, the Court narrowly found that law enforcement agencies did not have the right to use infrared sensors to track a suspect's location inside his home without a warrant.[98] However, the case left some ambiguity as to the privacy individuals should expect in public areas because Justice Scalia relied heavily on the fact that the home has a heightened expectation of privacy.[99]

The Court partially addressed this ambiguity in *United States v. Jones*, where it held that an unwarranted use of a GPS tracking device violated

---

operation, but the warrant was found to be lacking probable cause after the search had already occurred. *Id.* at 923. *See also* Edna F. Ball, *Good Faith and the Fourth Amendment: The Reasonable Exception to the Exclusionary Rule*, 69 J. CRIM. L. & CRIMINOLOGY 635, 658 (1978) (explaining that two common scenarios exist whereby the good faith exception to the exclusionary rule may be permitted under Fourth Amendment jurisprudence). The first such scenario occurs where a police officer makes a mistake in judgment when determining whether probable cause exists to support a warrant. *Id.* The second situation occurs where an officer relies on a mistake in fact, for example relying on a defected warrant. *Id.*

94 *See Leon*, 468 U.S. at 922 ("[T]he marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion.").

95 *See id.* at 923 (distinguishing that this exclusion will not always apply even if a warrant has been issued, and holding that a baseline analysis of reasonableness needs to be determined on a case-by-case basis).

96 *See* Hernandez, *supra* note 54 (explaining the Stingray's ability to track cellphones by acting as a fake cell tower and requesting the phone's location information). *See also* Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 14 (2008) (arguing that the *Kyllo v. United States* decision reinforced that the home has a high degree of privacy that would not be experienced in more public places).

97 *See* 533 U.S. 27, 44 (2001) (finding an unwarranted search had occurred after police used infrared heat sensors to analyze heat radiations emitted from a suspect's home without first getting a warrant). The information gathered from the device led to the police being granted a search warrant based on probable cause that the heat radiations signified a likelihood that the suspect was growing marijuana inside the home. *Id.* at 30, 40.

98 *See id.* at 40 (holding that law enforcement must get a warrant before using thermal imaging equipment that can look through the walls of a suspect's home).

99 *See id.* at 33 (distinguishing this case from a past case that held that aerial photography of an industrial complex was not a search chiefly because of the special sanctity of the home). *See also* U.S. CONST. amend IV (making specific mention to "houses" in the prefatory language of the Fourth Amendment).

the Fourth Amendment's prohibition on unreasonable searches.[100] The Court relied on the common law trespass doctrine in finding that attaching a GPS device to a vehicle constituted a search under the Fourth Amendment.[101] Thus, under the *Jones* reasoning, the physical attachment itself was enough to trigger Fourth Amendment protection because a trespass had been traditionally linked with the protection from government intrusion.[102]

Notably, the Supreme Court denied *certiorari* to review an Eleventh Circuit decision, where law enforcement agents gathered cellphone location data from a cellphone service provider with a court order rather than a warrant.[103] The government gathered the location of the petitioner in relation to the cell tower during incoming and outgoing calls.[104] The Eleventh Circuit found that cellphone location data gathered from a cell service provider—a third party—is not subject to the Fourth Amendment.[105] The Fourth Circuit ruled similarly and relied on the third-party doctrine in holding that the defendant had no expectation of privacy in the cellphone location data that was gathered by the phone company

---

100 *See* 132 S. Ct. 945, 948 (2012) (holding that the installation of a GPS on a suspect's vehicle constitutes a search under the Fourth Amendment).

101 *See id*. at 949 (describing the historical connection between the tort trespass doctrine and Fourth Amendment searches). *See also* Brittany Boatman, United States v. Jones*: The Foolish Revival of the Trespass Doctrine in Addressing GPS Technology and the Fourth Amendment*, 47 VAL. U. L. REV. 677, 683–84 (2013) (explaining that Justice Scalia's majority opinion in the Jones decision "revived" the trespass doctrine and extended the word "effect" from Fourth Amendment to include a person's vehicle); *supra* note 82 and accompanying text (providing the relevant text of the Fourth Amendment).

102 *See* 132 S. Ct. at 949 (relying on historical arguments that the founders created the Fourth Amendment to protect the citizenry from physical intrusion).

103 *See* United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) (denying certiorari to hear appeal). The defense wanted evidence related to cellphone records to be discarded. *Id.* They argued that the procurement of evidence from the phone company by court order was in violation of the Fourth Amendment because the government had not made a requisite showing of probable cause. *Id.*

104 *See* United States v. Davis, 754 F.3d 1205 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 Fed. Appx. 925 (11th Cir. 2014) (unpublished), *and on reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) (stating that the prosecution relied on the cell location data in its case in chief). *See also* Dana Kerr, *Court Rules Police Need Warrant for Cell Phone Location Tracking*, CNET (June 11, 2014), https://www.cnet.com/news/court-police-need-warrant-for-cell-phone-location-tracking/ [https://perma.cc/K7VB-GSQV] (providing detailed relevant facts of the *Davis* case). Specifically, the defendant was charged with several counts of robbery of gas stations and restaurants and that the cell tower location data put the defendant in close proximity to all of the crimes at the times when they occurred. *Id.*

105 *See Davis*, 785 F.3d at 518 (holding that the ultimate test for a Fourth Amendment was reasonableness and that the government had conducted a reasonable search).

and obtained by the government. [106] However, despite very limited case law regarding the Stingray, courts have not extended these decisions to location data gathered by the Stingray.[107]

D. Federal and State Legislative and Administrative Standards Applicable to the Stingray

Several sources of state and federal law and policy are potentially applicable to the Stingray.[108] Among the most important sources are the federal pen register and trace statute, the "Wiretap Act," a proposed federal Stingray Act, state-level Stingray legislation, and a Department of Justice (DOJ) policy.[109]

1. The Federal Pen Register and Trace Statute

The Constitutional standard that applies to law enforcement oversight of incoming and outgoing calls is a low bar due to the previously discussed *Smith v. Maryland* Supreme Court decision that held that pen register use falls under the third-party doctrine.[110] In an attempt to create some statuary guidance, Congress enacted the pen register and Trace Statute ("Section 3123"), which requires judges to issue an order allowing the use of the pen register.[111] Under this statute, a law enforcement officer or prosecutor is required to name the identity of the person making the

---

[106] *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (finding that historical cellphone location data falls within the third-party doctrine and is thus not subject to warrant requirement). *See also* Jeremy Derman, *Constitutional Law – Maryland District Court Finds Government's Acquisition of Historical Cell Site Data Immune from Fourth Amendment* – United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012)*, 46 SUFFOLK U. L. REV. 297, 298 (2013) (explaining that the District Court granted a court order under the Stored Communications Act based off of a "specific and articulable facts" standard, but this standard did not rise to the typical Fourth Amendment warrant requirement of probable cause).

[107] *See* Maryland v. Andrews, 134 A.3d 324, 353 (Md. Spec. App. 2016) (holding that the unwarranted use of a Stingray-like device violated the defendant's reasonable expectation of privacy). *See also* United States v. Lambis, 197 F.Supp.3d 606, 615 (S.D.N.Y. July 12, 2016) (distinguishing Stingray technology from cell tower location data from the service provider because the user does not *voluntarily* allow the Stingray to intercept the connection to the cell tower).

[108] *See supra* Part II.C (addressing the Federal Pen Register and Trace Statute, the Wiretap Act, and the proposed Stingray Privacy Act).

[109] *See infra* Part D.1–3 (analyzing the federal statutory sources that are currently enacted, as well as proposed federal legislation and DOJ policy).

[110] *See supra* notes 90–92 and accompanying text (explaining how information gathered by a pen register falls under the third-party doctrine).

[111] *See* 18 U.S.C. § 3121 (2012) ("no person may install or use a pen register or a trap and trace device without first obtaining a court order [pursuant to the application procedure in the statute]").

request and to certify that the information gathered is relevant to an ongoing police investigation.[112]

The 1986 statute allowed for no judicial oversight for similar online information because the statute was set up specifically for landline telephone communications.[113] To remedy this lack of statutory coverage, the Patriot Act of 2001 amended and broadened the 1986 definition of "pen register" so it could protect online communications with the same modest privacy protections.[114] The amended definitions are much more expansive and not telephone-specific.[115]

In fact, it is now believed that the Federal Pen Register Statute is exactly what local and federal law enforcement agents may have been, or may still be, using before conducting a search with the Stingray.[116] The

---

[112] *See id.* (setting the judicial standard for reviewing the application for a Pen/Trace order). The application process is made pursuant to 18 U.S.C. § 3122, which states:

> [The contents of the application shall include] . . . [b](1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and . . . [b](2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Id.

[113] *See generally* U.S.C. § 3127 (2016) (lacking definitions to the chapter that would apply to electronic communications over Internet or cellphone platforms).

[114] *See id.* (expanding the definitions of "wire communication," "trap and trace device," and "pen register").

[115] *See id.* (providing the new definitions for the procedure). In full these provisions define the terms "pen register" and "trap and trace device," as follows:

> [T]he term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business . . . [T]he term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that *such information shall not include the contents of any communication*.

Id. § (3)–(4) (emphasis added).

[116] *See* Ryan Gallagher, *Feds Accused of Hiding Information From Judges about Covert Cellphone Tracking Tool*, SLATE (Mar. 28, 2013), http://www.slate.com/blogs/future_tense/2013/03/28/stingray_surveillance_technology_used_without_proper_approval_report.html

question then, is whether the Stingray, which is capable of much more than a traditional pen register, is subject to the standard court order or requires a warrant.[117] At this time, the question remains unanswered, and judges are forced to grapple with the problem on Constitutional rather than statutory grounds.[118]

2. The Federal "Wiretap Act" Provides Recourse For Victims of Electronic Privacy Invasion

Another potentially-applicable statute is the Omnibus Crime Control and Safe Streets Act ("Wiretap Act").[119] A claim brought against a private citizen and a law enforcement officer can be distinguished under this Act.[120] If private citizens are alleged to have used surveillance technology to eavesdrop on a third party, they may be subject to harsh criminal and civil penalties.[121] However, in many circuits the statute is interpreted as giving qualified immunity to law enforcement officers.[122] In other

---

[https://perma.cc/NV8L-CW3Q] (explaining that the pen/trace application applies to "a type of surveillance that does not usually require a search warrant because it records only metadata—the who, where, and when of a communication but not the content"). The article states that local and federal law enforcement agencies likely used the Pen/Trace statute to get court permission to use the Stingray, relying on documents gathered by the ACLU. *Id*. *See also* Jenna McLaughlin, *How Chicago Police Convinced Courts to Let Them Track Cellphones Without a Warrant*, INTERCEPT (Oct. 18, 2016), https://theintercept.com/2016/10/18/how-chicago-police-convinced-courts-to-let-them-track-cellphones-without-a-warrant/ [https://perma.cc/MD63-KYYQ] (examining the recently-released pen register applications that the Chicago police department used before requesting to use the Stingray, most of which only referred to the Stingray as a "digital analyzer" having the capability to gather signal emissions from a targeted cellphone).

117 *See* Greenemeier, *supra* note 61 (arguing that the pen register standard is too low of a bar for the Stingray's capabilities).

118 *See* Grace Vandemark, *Stingray Tracking Technology*, SURVEILLANCE IN AMERICA: AN ENCYCLOPEDIA OF HISTORY, POLITICS, AND THE LAW (ABC-CLIO 2016) (explaining that in the limited amount of cases involving the Stingray, courts have been split as to whether they require a warrant).

119 *See generally* 18 U.S.C. § 2511 (2012) (detailing various unlawful activities relating to intercepting electronic information); Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U. L. REV. 1481, 1516 (2007) (arguing that the Wiretap Act as well as a miscellany of other federal privacy statutes have failed to keep up with the ever-developing technology in the age of the internet).

120 *See* 18 U.S.C. § 2551 (setting different standards for private citizens and those "acting under the color of law").

121 *See id.* § 2511(4)–(5) (providing that violators can be subject to fines, civil liability and up to five years of imprisonment).

122 *See id.* § 2511(2)(c) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."). *See also* Brian L. Porto, Annotation, *Qualified Immunity as*

jurisdictions, immunity for law enforcement can still exist depending on varying definitions of the good-faith defense.[123] Regardless, it would be difficult for a private citizen to actually prove that a police officer was using the technology irresponsibly.[124]

Notably, one recent case faced the issue of whether a wiretap warrant issued for a Stingray complied with the Fourth Amendment.[125] The Court held that the wiretap warrant was sufficient because it was based on probable cause and it adequately detailed the scope of the search so as to comply with the Fourth Amendment's particularity requirement.[126] Furthermore, the Court held that even if the warrant were invalid, it would have fallen within the "good faith" exception.[127]

3. The Proposed "Stingray Privacy Act of 2015," State-Based Stingray Legislation, and A New DOJ Policy Seek To Monitor the Stingray

Due to these issues, legislators on Capitol Hill have taken notice of privacy concerns of the Stingray.[128] On November 2, 2015, "The Stingray

---

Defense in Suit under Federal Wiretap Act, 178 A.L.R. Fed. 1 (Originally published in 2002) (discussing the different approaches by circuits regarding the good-faith defense and qualified immunity).

123 *See* Porto, *supra* note 122 (analyzing federal cases where the qualified immunity defense has been invoked).

124 *See* Hernandez, *supra* note 54 (demonstrating that users have no idea that the Stingray has connected to their cellphone). *But see* Lilly Hay Newman, *Now There's an App For Detecting Government Stingray Cell Phone Trackers*, SLATE (Dec. 31, 2014), http://www.slate.com/blogs/future_tense/2014/12/31/snoopsnitch_is_an_app_by_the_german_srlabs_that_detects_imsi_catchers_stingrays.html [https://perma.cc/5GNB-3DNL] (detailing a promising new app called "SnoopSnitch," which claims to be able to tell a user if a Stingray has connected to their phone).

125 *See* United States v. Tutis, Crim. No. 14-699, 2016 WL 6136577, at *3 (D.N.J. Oct. 20, 2016) (holding that under the circumstances the warrant requirement was fulfilled). In this case, the suspect in a drug trafficking conspiracy was allegedly cycling through several cellphones with the purpose of thwarting law enforcement. *Id.* at *2. To streamline the investigation, the officers applied for a wiretap order to use a Stingray-like device for the sole purpose of determining which cellphone belonged to the user, and the warrant was granted. *Id.*

126 *See id.* at *5 (finding that probable cause was satisfied by evidence of known drug trafficking activities and the constant switching of cellphones). The judge also found that even though the government did not specifically say that a Stingray was going to be used, the fact that the device's capabilities to the extent that it would determine his cellphone number was adequate for purposes of the wiretap order. *Id.*

127 *See id.* at *8 (holding that the good faith requirement would have been satisfied even if the wiretap order did not satisfy the Fourth Amendment because a police officer acting upon the issuance of the wiretap order would have reasonable belief that the order satisfied the Fourth Amendment). *See also* Ball, *supra* note 93, at 635–36 (explaining the doctrine of good faith as it relates to the Fourth Amendment).

128 *See* Dennis Romboy, *Chaffetz Aims to Restrict Police Use of "Stingrays" to Capture Cellphone Info*, DESERTNEWS (Nov. 3, 2015), http://www.deseretnews.com/article/865640580/Chaffetz-aims-to-restrict-police-use-of-stingrays-to-capture-cellphone-info.html?pg=all

Privacy Act of 2015" was introduced into the House of Representatives.[129] According to Representative Jason Chaffetz, a co-sponsor of the Stingray

---

[https://perma.cc/FT9M-PC79] (reporting Representative Jason Chaffetz's concerns about unwarranted Stingray use).

[129] *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015) (detailing a warrant procedure and criminalizing citizen-use of the Stingray). In full the act provides:

> (a) Prohibition Of Use.—Except as provided in subsection (d), anyone who knowingly uses a cell-site simulator shall be punished as provided in subsection (b).
> (b) Penalty.—The punishment for an offense under subsection (a) is a fine under this title or imprisonment for not more than 10 years, or both.
> (c) Prohibition Of Use As Evidence.—No information acquired through the use of a cell-site simulator in violation of subsection (a), and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.
> (d) Exceptions.—Subsection (a) does not apply to the following:
> (1) Warrant—Use of a cell-site simulator by a governmental entity under a warrant issued under the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued under State warrant procedures) by a court of competent jurisdiction.
> (2) FOREIGN INTELLIGENCE SURVEILLANCE.—Use of a cell-site simulator by a governmental entity to conduct electronic surveillance under the Foreign Intelligence Service Act of 1978 (50 U.S.C. 1801 et seq.).
> (3) Emergency—Subject to subsection (e), use of a cell-site simulator by a governmental entity, if—
> (A) such governmental entity reasonably determines an emergency exists that—
> (i) involves—
> (I) immediate danger of death or serious physical injury to any person;
> (II) conspiratorial activities threatening the national security interest; or
> (III) conspiratorial activities characteristic of organized crime; and
> (ii) requires use of a cell-site simulator before a warrant can, with due diligence, be obtained;
> (B) there are grounds upon which a warrant could be entered to authorize such use; and
> (C) such governmental entity applies for a warrant approving such use not later than 48 hours after such use begins.
> (e) Termination Of Emergency Use.—
> (1) IN GENERAL.—A governmental entity shall immediately terminate use of a cell-site simulator under subsection (d)(3) when the information sought is obtained or when the application for a warrant is denied, whichever is earlier.

Protection Act, "[t]he abuse of stingrays and other cell site simulators by individuals, including law enforcement, could enable gross violations of privacy."[130]

The Stingray is not just in the hands of federal agencies.[131] Currently twenty-three states are known to have access to the Stingray.[132] Widespread police possession has caused state lawmakers across the country to enact legislation.[133] Amid major criticism from privacy advocates, the DOJ created a policy that purportedly requires federal agents to get a warrant before using the Stingray.[134] Still, the question

> (2) PROHIBITION ON USE AS EVIDENCE.—If an application for a warrant under subsection (d)(3) is denied, any information or evidence derived from use of the cell-site simulator shall be subject to subsection (c) and an inventory shall be served on each person named in the application.

Id.

130 *See* Romboy, *supra* note 128 (explaining Representative Jason Chaffetz's policy position regarding the Stingray device).

131 *See Who's Got Them?*, *supra* note 62 (providing the federal agencies known to use the Stingray, include: the Federal Bureau of Investigations, the Drug Enforcement Administration, the United States Secret Service, Immigration and Customs Enforcement, the United States Marshal Service, the Bureau of Alcohol, Firearms, and Explosives, the Internal Revenue Service, the United States Army, the United States Navy, the United States Marine Corps, the United States National Guard, the United States Special Operations Command, and the National Security Agency).

132 *See id.* (illustrating in a fifty-state survey all of the state and local law enforcement agencies known to use the Stingray, including: Alaska, Arizona, California, Washington D.C., Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Missouri, New York, North Carolina, Oklahoma, Pennsylvania, Tennessee, Texas, Virginia, Washington, and Wisconsin).

133 Several states have enacted legislation that sets out some guidelines for Stingrays, however some of the legislative aim is in response to attachment of only GPS devices. *See* CAL. PENAL CODE § 1546.1 (2016) (providing in-depth warrant requirements before police interception, but with some exceptions); IND. CODE § 35-33-5-12 (2015) (setting a standard that police need to gain a warrant, but allowing potentially broad exceptions); MINN. STAT. § 626A.42 (2014) (providing that evidence for warrantless gathering of location data will be inadmissible with some exceptions); MONT. CODE § 46-5-110 (2015) (enacting standard that applies to any police tracking of wireless devices); TENN. CODE § 39-13-610 (2014) (requiring police to get a warrant, but allowing several exceptions); UTAH CODE § 77-23c-102 (2014) (disallowing warrantless location evidence but providing judicial discretion in allowing evidence); VA. CODE § 19.2-56.2 (2012) (providing that police must get a warrant before using tracking location with exceptions); LA. STAT. § 14:222.3 (2016); H.B. No. 1440, Wash. Sixty-Fourth Leg., First Spec. Sess. (Wash. 2015) (speaking directly to inadmissibility of evidence gathered by a cell-simulator device); Ill. Legis. Serv. P.A. 99-622 (S.B. 2343) (2016) (requiring that police quash any evidence not related to the investigation provided in the search warrant).

134 *See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [https://perma.cc/7CEA-KEP9] (providing a warrant procedure for all federal employees seeking to use a Stingray).

remains how the states and federal government will deal with the ever-advancing technology.[135] This Note proposes a three-pronged approach that states can use to deter use of unwarranted Stingray searches.[136]

III. ANALYSIS

Several of the aforementioned constitutional and statutory standards likely apply, at least to some degree, to the Stingray.[137] This section explores how these various legal standards may apply to the warrantless use of the Stingray.[138] First, Part III.A analyzes the underlying constitutional questions regarding the third-party doctrine and weighs its applicability to police use of the Stingray, concluding that the third-party doctrine is inappropriate for police data gathered by the Stingray.[139] Then, Part III.B examines various federal statutory standards that may apply to the use of the Stingray, and concludes that federal law is not currently equipped to deal with the Stingray's capabilities.[140] Finally, Part III.C shows that the state legislatures have enacted statutes that are effectively filling in the gaps left from the lack of federal statutes.[141]

A. The Third-Party Doctrine Is Inappropriate for the Stingray

The third-party doctrine helps define the meaning of a "reasonable" search under the Fourth Amendment.[142] Well before the Stingray was discovered, there was significant scholarly debate about the usefulness of the third-party doctrine in general.[143] Proponents of the third-party

---

135 *See infra* Part III (analyzing the existing federal guidance, including the Wiretap Act and the Pen Register Statute, as well as a Department of Justice Policy, and a flood of state-level Stingray legislation).

136 *See infra* Part IV (proposing that states should introduce a three-pronged approach to combat unwarranted use of the Stingray).

137 *See supra* Part III.C–D (providing information regarding Supreme Court cases involving the unwarranted use of the Stingray, and discussing legislative and policy guidance).

138 *See infra* Part III (analyzing how current legal standards may apply to the unwarranted use of the Stingray by police officers).

139 *See infra* Part III.A (addressing the potential applicability of the third-party doctrine to the Stingray).

140 *See infra* Part III.B (determining that the federal "Wiretap Act," and pen register statute are not equipped to deal with the multiple capabilities of the Stingray).

141 *See infra* Part III.C (assessing the strengths and weaknesses of currently-enacted statutes from states that have enacted laws pertaining to Stingrays).

142 *See supra* Part II.A (describing the key components of the third-party doctrine). *See also* Stern, *supra* note 90, at 364 (explaining that people have no reasonable expectation of privacy to information shared with bank, phone carrier, or credit card company).

143 *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107(4) MICH. L. REV. 561, 563 (2009) (arguing in favor of the third-party doctrine on public policy grounds). *But see, e.g.*, Erin Murphy, *The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*,

doctrine say that in the absence of the rule, criminals would use the Fourth Amendment as a shield to an otherwise-public act.[144] This argument relies on the premise that Fourth Amendment protections are inapplicable in public places, and instead the Fourth Amendment is only surmised to protect privacy in inherently private places.[145] It also relies on the idea that a criminal actor could then take advantage of the third-party doctrine by essentially using only third-party platforms.[146] But if the Stingray is able to make sweeping searches of the entire public, nowhere can truly be considered a private place if the user owns a cellphone.[147] Furthermore, the reliance on the argument that criminal actors can take advantage of their cellphones to perform criminal tasks is not well taken because police still have the ability to use the Stingray, but simply must get a warrant based on probable cause.[148] Thus, a sweeping search of cellphone data and contents, with no probable cause, does not serve either of the major arguments in favor of the third-party doctrine.[149]

The traditional arguments against the third-party doctrine further undermine this argument in two ways.[150] The first argument is that most people have an expectation of privacy in information given voluntarily to third-parties.[151] Currently, phone records collected from the phone carrier

---

24 BERKELEY TECH. L.J. 1239, 1240–41 (2009) (refuting arguments by Kerr that public policy favors the third-party doctrine).

144 *See* Kerr, *supra* note 143, at 561 (outlining primary arguments in favor of the third-party doctrine). *See also* United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012) (detailing that in the *Rigmaiden* proceeding the judge denied the defendant's advanced discovery requests in part because the requested information would advantage criminals).

145 *See* Kerr, *supra* note 143, at 574 (arguing that the Fourth Amendment allows police to make practical investigations in public places to gather evidence that may lead to establish the probable cause that allows for a warrant).

146 *See* Kerr, *supra* note 143, at 581 (explaining that the Fourth Amendment should keep the third-party doctrine alive even in the face of developing technology, the absence of which would essentially give criminals the upper hand).

147 *See* Murphy, *supra* note 143, at 1249 (arguing that the public domain is not always expected to be an area that is inherently subject to no privacy protections).

148 *See supra* Part II.C (explaining the traditional warrant requirements). *See also* Eric M. Yesner, *Government Surveillance through New Technology: Rethinking the Third-Party Doctrine's Implications on the Fourth Amendment*, 19 HOLY CROSS J.L. & PUB. POL'Y 135, 140 (2015) (positing that the evolution of new technology has unequivocally been tilted toward heightened citizen surveillance, and that government spying has become much easier with an antiquated third-party doctrine).

149 *See supra* notes 143–46 and accompanying text (analyzing the capabilities of the Stingray in light of arguments in favor of the third-party doctrine).

150 *See* Kerr, *supra* note 143, at 562 (detailing the two main arguments against the third-party doctrine).

151 *See* Kerr, *supra* note 143, at 563 (providing the first argument given by opponents of the third-party doctrine, and refuting the argument).

are generally not subject to a warrant.[152] However, the Stingray goes beyond specific data collected against a particular person because it has the ability to gather and receive location, user identifying information, and communications of several users instantly and proactively.[153]

The second argument is that with the presence of the third-party doctrine, police power becomes too far-reaching.[154] The Stingray is the perfect example of how the police power can become too far-reaching with developing technology.[155] The Stingray allows sweep searches, and although the use of a cellphone may be voluntary, the expectation of privacy that each individual has when using their cellphone seems to outweigh the interest the police may have in using the Stingray for public safety.[156]

Furthermore, the Stingray likely does not conform to the traditional third-party doctrine as set forth in *Smith v. Maryland*.[157] Regardless of the position taken on the third-party doctrine, the Stingray goes beyond what could be considered information given *voluntarily* to a third-party.[158] One of the first Stingray cases to hit the federal circuit, *United States v. Lambis*, addressed this issue.[159] The court, in ruling against the application of the third-party doctrine, stated:

---

[152] *Compare* United States v. Graham, 824 F.3d 421, 436 (4th Cir. 2016) (finding that historical cellphone location data falls within the third-party doctrine and is thus not subject to warrant requirement) *with* U.S. v. Davis, 754 F.3d 1205, 1210 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 Fed. Appx. 925 (11th Cir. 2014) (unpublished), *and on reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) (holding in part that the third-party doctrine is applicable to historical cellphone data gathered by a law enforcement agency and thus upholding a conviction despite Fourth Amendment challenges to the issued court order).

[153] *See supra* Part II.A.2 (explaining the various capabilities of the Stingray and how police can search the contents of any cellphone within its radius).

[154] *See* Kerr, *supra* note 143, at 583–84 (refuting the argument that police power is too strong under the third-party doctrine by pointing out that other doctrines, such as entrapment, are used to promote a less-far-reaching police state).

[155] *See* Owsley, *supra* note 76, at 192–93 (explaining the way in which police can circumvent typical privacy expectations when using the Stingray).

[156] *See* Owsley, *supra* note 76, at 227, 230 (weighing the privacy interests of individuals in the use of their cellphones and explaining how the Stingray goes beyond the amount of privacy that is expected by the Fourth Amendment).

[157] *See* United States v. Lambis, 197 F.Supp.3d 606, 615–16 (S.D.N.Y. July 12, 2016) (finding that the Stingray does not fit within the third-party doctrine).

[158] *Compare* Smith v. Md., 442 U.S. 735, 736 (1979) (relying heavily on the fact that the user of a telephone gives information over to a third party *voluntarily* in justifying no Fourth Amendment protection from the use of a pen register) (emphasis added) *with Lambis,* 197 F.Supp.3d at 615 (finding that the user of a cellphone has not voluntarily surrendered cellphone information when law enforcement uses a Stingray tracking device).

[159] *See Lambis,* 197 F.Supp.3d at 614 (holding that a Stingray has different capabilities and thus should be distinguished from the pen register device used in *Smith*).

> For instance, in *Smith*, the Supreme Court found that pen register information is subject to the third party doctrine because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." However, the location information detected by a cell-site simulator is different in kind from pen register information: *it is neither initiated by the user nor sent to a third party*.[160]

The final sentence makes two very important arguments.[161] First, the Stingray "is not initiated by the user."[162] Recall that the Stingray works by deploying a "man-in-the-middle attack."[163] The Stingray actively connects to users' cellphones without their knowledge.[164] Thus, although cellphone users may have voluntarily sent information to the cellphone service provider, they have not given any information voluntarily to the Stingray user.[165]

The second argument is "nor [is the user's cellphone information] sent to a third party."[166] The government's use of the Stingray can be contrasted to a situation like the one in *United States v. Davis*, where the government gathered the information directly from the third party (i.e., the phone carrier).[167] With the Stingray, the user is not technically sending the information to a third party at all.[168] Instead, the Stingray is

---

160 *Id.* (internal citations omitted and italics added for emphasis).

161 *See id.* ("[h]owever, the location information detected by a cell-site simulator is different in kind from pen register information: *it is neither initiated by the user nor sent to a third party*" (emphasis added)).

162 *See id.* (providing that the cellphone user does not voluntarily send over information to a third-party).

163 *See* Kolker, *supra* note 53 and accompanying text (detailing how the Stingray gathers information from a user's cellular telephone without the user or the third-party telephone provider's knowledge).

164 *See id.* (explaining how users have no indication that a Stingray has connected to their cellphone).

165 *See Lambis*, 197 F.Supp.3d 606 at 615 (detailing the difference between the voluntariness of sending the information to a cell service provider rather than directly to a cell-site simulator).

166 *Id.*

167 *See id.* (analyzing the arguments advanced by the varying circuits about whether cellphone information given voluntarily to a third-party phone carrier falls under the third-party doctrine, but concluding *arguendo* that even if it does qualify, the data gathered from a Stingray goes beyond because the third-party phone carrier is completely uninvolved).

168 *See supra* notes 51–53 and accompanying text (explaining that the Stingray actively intercepts data from third parties, and does not involve the third-party in gleaning the information).

intercepting the message directly.[169] Thus, the "third-party" link is completely broken because the government has interacted directly with the user's cellphone.[170]

B. The Federal Law Is Beyond the Curve with the Stingray

At the federal level, privacy law is arguably behind the curve in many respects.[171] This Part deals with federal laws that may be specifically applicable to the Stingray, and demonstrates that the laws are not designed to keep up with technology such as the Stingray.[172] First, Part III.B.1 analyzes U.S.C. § 3123 ("the Federal Pen Register Statute") and explains why the statute is too low of a bar for the Stingray.[173] Then, Part III.B.2 discusses why the Wiretap Act is also not well-suited to provide a legislative standard for the Stingray.[174] Finally, Part III.B.3 discusses the proposed Stingray Privacy Act of 2015.[175]

1. U.S.C. § 3123 Is Too Low of a Standard for the Stingray

As it applies to the Stingray's ability to view call records, the broad discretion of law enforcement under United States Code § 3123 would permit Stingray use by police, but only if viewing call records was the device's sole capability.[176] Recall that this statute—originally enacted for landlines—gives police only two requirements before gaining access to the information: (1) police officers or prosecutors must state their identity, and (2) make a showing that the information requested is relevant to an

---

169 *See* Hernandez, *supra* note 54 and accompanying text (clarifying that the Stingray acts exclusively as a fake tower to intercept the information).

170 *See* Klonick, *supra* note 44 (explaining that the police have the ability to connect to the devices of several users within the radius of the Stingray without consent of the user or service provider).

171 *But cf.* Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

172 *See infra* Part III.B.1 (discussing the Wiretap Act, the pen register statute, and proposed legislation to limit Stingrays).

173 *See infra* Part III.B.1 (explaining why U.S.C. § 3123 does not adequately provide for the multiple intrusive uses of the Stingray).

174 *See infra* Part III.B.2 (analyzing the Wiretap Act and concluding that the Act only applies to intercepted communications while leaving broad immunity to anyone acting "under the color of law.").

175 *See infra* Part III.B.3 (addressing the proposed Federal Stingray legislation, including some of its strengths and weaknesses).

176 *See supra* note 112 (providing the statutory language and relevant provisions of the application procedure under § 3123).

ongoing criminal investigation.[177] Additionally, this statute does not have an exclusionary rule, so evidence acquired from botching this procedure will not be thrown out by a judge.[178]

The New York Police Department (NYPD) gives a practical example of how low the bar is under § 3123.[179] The common practice of the NYPD is to simply subpoena a phone carrier to gain access to a cellphone user's call information in cases where a cellphone has been stolen.[180] The issue is that, with no exclusionary rule and not constitutionally establishing a search under the Fourth Amendment, law enforcement agencies have an almost unchecked ability to catalogue phone records of limitless people with no judicial oversight.[181]

2. The Wiretap Act Is Ill-Suited To Regulate the Stingray Because the Stingray Is Untraceable and Can Intercept Multiple Users' Communications at One Time

One argument is that if the technology were to be used indiscriminately to intercept communications, the Wiretap Act could be triggered.[182] The Wiretap Act requires that police officers have probable cause and go through all the typical procedures for getting a warrant.[183] For instance, assume that verifiable evidence exists that a police officer used intercepted communication with the Stingray without a warrant, even though the suspect was completely free of guilt.[184] Under these

---

177 *See* 18 U.S.C. § 3122 (b)(1)–(2) (2016) (detailing the procedure by which police officers and prosecutors can be granted a pen register).

178 *See generally* 18 U.S.C. § 3123 (2016) (lacking any exclusionary rule in the statutory language).

179 *See* Joseph Goldstein, *City is Amassing Trove of Cellphone Logs*, NEW YORK TIMES (Nov. 26, 2012) http://www.nytimes.com/2012/11/27/nyregion/new-york-city-police-amassing-a-trove-of-cellphone-logs.html?hpw&_r=1 [https://perma.cc/JD9T-ZNQK] (illustrating how it is commonplace for the NYPD to subpoena phone carriers and collect massive amounts of information without getting a warrant).

180 *See id.* (describing the large database of information that the New York Police Department has acquired from the practice of subpoenaing the phone companies, with no questions asked by the companies when they furnish the information).

181 *See id.* (explaining that T-Mobile handed over cellphone numbers from 297 police subpoenas in a single month without hesitation).

182 *See* Christopher Izant, Note, *Stingray Surveillance: Legal Rules by Statute or Subsumption,* HARV. L. NAT'L SEC. J. (July 15, 2016) http://harvardnsj.org/2016/07/stingray-surveillance-legal-rules-by-statute-or-subsumption/ [https://perma.cc/X9LT-WP2Q] (arguing that under the Wiretap Act, any content collected by the Stingray would be subjected to the more-stringent record keeping and time limit rules as promulgated in the statute).

183 *See* 18 U.S.C. § 2515 (2012) (providing that police officers get a warrant before using evidence obtained by interception of wire or oral communications, with any evidence being acquired without a warrant being excluded from use in the courtroom).

184 Hypothetical situation posed by the author.

circumstances, could a suspect sue the government for violating his privacy rights?[185] As mentioned earlier, the Wiretap Act gives wide-ranging immunity to police officers "acting under the color of law."[186] Therefore, in some cases, police officers may receive qualified immunity if they neglected to get a warrant before intercepting communications.[187] Another difficulty in typical regulation is that a citizen has no way of knowing if a police officer has used the Stingray, as the user has no indication that a Stingray was connected to or disconnected from their cellphone.[188]

The Stingray has the ability to track location and to intercept communications, both of which go much further than viewing call logs.[189] These capabilities may qualify as a Fourth Amendment search based on Supreme Court interpretations of the Fourth Amendment, which would require a warrant.[190] Furthermore, the Stingray has the capability of intercepting multiple users' communications with one use.[191]

---

185 It is possible that a citizen could file a *Bivens* action in such a case. In any case, one can only imagine the difficulty in first, knowing that a Stingray in fact connected to your cellphone, and second, proving that a particular officer violated your constitutional rights in using the particular technology. *See* Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971).

186 *See* Porto, *supra* note 122 (explaining how some circuits have interpreted the Wiretap Act as giving police officers qualified immunity).

187 *See supra* notes 120–24 and accompanying text (distinguishing between causes of action brought against citizens and those brought against police officers).

188 *See supra* notes 53–4 (providing background information on how the Stingray can be used without the cellphone user having any knowledge).

189 *See* Hernandez, *supra* note 54 (describing how Stingrays can track all users' location within range without the users' knowledge). *See also* Zetter, *supra* note 53 (explaining that the Stingray has the ability to intercept text messages and phone calls).

190 *See* Maryland v. Andrews, 134 A.3d 324, 353 (Md. Spec. App. 2016) (holding that the unwarranted use of a Stingray-like device violated the defendant's reasonable expectation of privacy). *See also* United States v. Lambis, 197 F.Supp.3d 606, at 606–11 (S.D.N.Y. July 12, 2016) (denying admission of evidence gathered from a Stingray on Constitutional grounds). *But see* U.S. v. Davis, 754 F.3d 1205, 1210 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 Fed. Appx. 925 (11th Cir. 2014) (unpublished), *and on reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) (allowing the government to gather cellphone data directly from the service provider under an interpretation of constitutional reasonableness).

191 *See In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012) (denying issuance of a pen register, citing to the fact that "[the government] did not address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment").

3. Federal Legislation Is a Slow, Dubious Process and the Currently-Proposed Federal Legislation Does Not Go Far Enough

The Stingray Privacy Act of 2015 is currently in committee in the United States House of Representatives.[192] The bill closely resembles the DOJ's policy that requires federal agents to get a warrant before deploying the device; however, the bill, unlike the DOJ's policy, is actually legally enforceable if it gets passed.[193] Facially, the proposed law grapples with some of the problems brought forth by the Stingray and fills in some gaps of federal statutory coverage.[194]

The bill has a "prohibition of use" clause.[195] This clause criminalizes the use of the Stingray by either an indeterminate fine or up to ten years imprisonment.[196] The bill's cosponsor has said that this clause would serve as a method of specific deterrence for police wishing to abuse the Stingray.[197] However, the clause also addresses another concern, in that members of the public have gained increased access to the Stingray.[198]

Section (c) of the proposed Stingray Protection Act of 2015 introduces an evidence-inadmissibility rule.[199] The rule provides that any evidence gathered by a Stingray without a warrant is inadmissible, subject to some

---

192 *See generally* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015), full text at *supra* note 129 (proposing new standards for use of the Stingray).

193 *See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, DOJ (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators (providing a warrant procedure for all federal employees seeking to use a Stingray). *See also* Izant, *supra* note 182 (stating that the DOJ's policy is only policy and thus not legally enforceable).

194 *See supra* Part III.B (discussing the holes in the current federal law as it relates to controlling police use of the Stingray).

195 *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (a) (2015), full text at *supra* note 129 (providing that knowingly using a cell-site simulator is prohibited and punishable by law, and any evidence gathered from unwarranted police use will be discarded subject to exceptions).

196 *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (b) (2015), full text at *supra* note 129 (exacting a penalty of up to ten years imprisonment for violation of the prohibition of use clause).

197 *See* Steven Nelson, *Bill: Give Cops up to 10 Years in Prison for Warrantless Phone Tracking*, U.S. NEWS (Nov. 3, 2015), http://www.usnews.com/news/articles/2015/11/03/congressmen-cops-should-face-10-years-in-prison-for-warrantless-phone-tracking [https://perma.cc/533K-CVAW] (according to Representative Peter Welch, "the penalty is there as a deterrent").

198 *See* Pell & Soghoian, *supra* note 63, at 75 (explaining that the market for the Stingray has made the devices available to the public). *See also* Kolker, *supra* note 53 (revealing that the price to buy less-sophisticated versions of the Stingray device are as low as $1,800 on foreign websites).

199 *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (c) (2015), full text at *supra* note 129 (establishing that all evidence gathered without a warrant will be inadmissible in a courtroom).

potentially problematic exceptions.[200] The first questionable exception to the inadmissibility rule is "an emergency . . . that is reasonably determined to involve . . . conspiratorial activities characteristic of organized crime."[201] The problem with this exception is that "organized crime" can be broadly defined.[202] Furthermore, the Stingray is mainly used for serious situations involving crime that could be reasonably considered organized.[203]

Second, an additional exception applies during an emergency that is reasonably determined to involve "conspiratorial activities threatening the national security interest."[204] This exception is also broadly defined.[205] The clause lacks clarity as to whether certain agencies, such as the Central Intelligence Agency, National Security Administration, Federal Bureau of Investigation, or the Department of Homeland Security would ever be subject to a warrant requirement because those agencies are designed specifically to protect national security interests.[206]

Finally, perhaps the most problematic exception of all states that "[the warrant-requirement does not apply] . . . [and] there are grounds upon which a warrant could be entered to authorize such use."[207] The main concern with this exception is that it directly contradicts the Fourth Amendment as interpreted in *Katz*.[208] The Supreme Court expressly rejected the government's claim that evidence from electronic surveillance

---

[200] *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (c) (2015), full text at *supra* note 129 (proving several broad exceptions to the rule).

[201] Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (b) (2015), full text at *supra* note 129.

[202] *See Organized Crime*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining organized crime as: "1. Widespread criminal activities that are coordinated and controlled through a central syndicate . . . 2. Persons involved in these criminal activities; a syndicate of criminals who rely on their unlawful activities for income.").

[203] *See supra* note 64 and accompanying text (describing situations where the Stingray is generally deployed by police officers). *But see* John Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, LA WEEKLY (Jan. 24, 2013), http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739 [https://perma.cc/F7PL-C3RQ] (exposing the widespread use of the Stingray by the LAPD, using the device over twenty-one times in a four month period for seemingly routine investigations).

[204] Stingray Privacy Act of 2015, H.R. 3871(d)(3)(A)(II) (2015), full text at *supra* note 129.

[205] *See generally* Stingray Privacy Act of 2015, H.R. 3871 (2015), full text at *supra* note 129 (offering no definitions for the terms within the chapter).

[206] *See Who's Got Them?*, *supra* note 62 (providing that the NSA, FBI, and CIA all have access to the devices).

[207] H.R. 3871 (d)(3)(B) (2015).

[208] *See* Katz v. United States, 389 U.S. 347, 357 (1967) (explaining that getting a warrant based on probable cause is a necessary prerequisite, the absence of which will create a *per se* unreasonable search under the Fourth Amendment, subject only to few narrow exceptions). The Court further explains that electronic surveillance is not, by its very nature, one of the exceptions to the rule. *Id.*

could be granted upon probable cause *after* the evidence had already been procured.[209] Thus, in light of *Katz*, this portion of the statute, if enacted, may be challenged as violative of the Constitution.[210]

C. State-Level Legislation Is Filling in the Gaps

The main advantage of state-level legislation is that states are much more productive than Congress.[211] In fact, thirty-eight states enacted more legislation than Congress did last year.[212] Furthermore, while lawmakers on Capitol Hill only saw four percent of bills turned into law, state lawmakers saw twenty-five percent.[213] Since Rigmaiden's case shed light on the previously undisclosed use of the Stingray, a flurry of states have enacted privacy legislation to control police use of the Stingray.[214]

All of these state laws address evidentiary concerns, but offer little to no deterrence for police officers in violation.[215] The laws prevent warrantless Stingray-acquired evidence from entering courtrooms.[216] However, states have also allowed exceptions that will allow evidence in some circumstances.[217] One issue with some of the earlier enacted statutes

---

[209] *See id.* at 358 (explaining that allowing such evidence "bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment").

[210] *Compare id.* (providing precedent that electronic surveillance does not fall within the warrant exception) *with* Stingray Privacy Act of 2015, H.R. 3871 (d)(3)(B) (2015) (stating that an exception to the warrant requirement can exist where "a warrant could be entered to authorize such use.").

[211] *See* Glen Justice, *States Six Times More Productive Than Congress*, CQ ROLL CALL (Jan. 27, 2015), http://cqrollcall.com/statetrackers/states-six-times-more-productive-than-congress/ [https://perma.cc/K6T6-5KMJ] (providing data that shows that even many smaller populated states, such as West Virginia, North Dakota and Rhode Island, are much quicker and more effective at enacting legislation than the United States Congress).

[212] *See id.* (illustrating that the average bill passage rate for United States Congress is four percent, whereas the national average for state legislatures is twenty-five percent). The study also explains that part of the reason that states are more effective is because state-level legislatures have issues that are sometimes more pressing, which can cost the state congressmen their jobs if they do not pass resolutions to state and local issues. *Id.*

[213] *See id.* (demonstrating that the state-level legislatures are much more likely to pass proposed legislation than legislators on Capitol Hill).

[214] *See supra* Part I (detailing the story of Daniel Rigmaiden).

[215] *See supra* note 133 and accompanying text (demonstrating that all state laws to this point have been evidence-focused). *See, e.g.*, MONT. CODE § 46-5-110 (2015) (providing that police officers need a warrant before tracking the location of a wireless device, subjecting a violator to a fifty-dollar penalty for breaking the statute).

[216] *See supra* note 133 and accompanying text (detailing that every state law currently in place bars evidence from Stingray devices that has been obtained without a warrant, subject to some exceptions).

[217] *See, e.g.*, TENN. CODE § 39-13-610(c) (2014) (allowing seven exceptions to the warrant requirement). The exceptions to Tennessee's Stingray law exceptions are as follows:

is that they may have been enacted before the full abilities of the Stingray were known to the state legislatures.[218]

Although these laws are a step in the right direction, they do not completely remedy the holes in the federal law.[219] Take California's Stingray law, for example, which is considered to be one of the most stringent.[220] First, it covers situations where a law enforcement agency wishes to gather electronic information from a service provider.[221] In California, the policing agency must get a warrant, a wiretap order, or an order for electronic reader records before making any service provider hand over user information or access to a user's device.[222] This provision grants privacy rights beyond the constitutional protections under the Fourth Amendment as interpreted in *Smith v. Maryland*.[223]

Another strength of California's law is that it goes into very specific warrant mandates relating to the use of Stingrays or other similar

---

(1) If the electronic device is reported stolen by the owner;
(2) If necessary to respond to the user's call for emergency services;
(3) To prevent imminent danger to the life of the owner or user;
(4) To prevent imminent danger to the public;
(5) With the informed, affirmative consent of the owner or user of the electronic device;
(6) If the user has posted the user's location within the last twenty-four (24) hours on a social media web site; or
(7) If exigent circumstances justify obtaining location information for the electronic device without a warrant.

Id.

218 *See supra* Part I.A.2 (explaining the various capabilities of the Stingray, including the ability to intercept/block communications, the ability to gather device information, and the ability to target location). *See*, *e.g.*, VA. CODE § 19.2-56.2 (2014) (referring only to the technology as "tracking devices," but failing to address admissibility of information that is intercepted or device information that is gathered by the device).

219 *See supra* Part II.C (analyzing constitutional and federal statutory law that pertains to the Stingray).

220 *See generally* CAL. PENAL CODE § 1546.1 (2016) (providing strict warrant requirements and allowing for judicial oversight of Stingray evidence). *See also In Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communications Privacy Act into Law*, ACLU (Oct. 8, 2015), https://www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy [https://perma.cc/HLY2-2Y3M] (explaining the ACLU's position that the enacted California Stingray legislation should set a model for the rest of the nation).

221 *See* CAL. PENAL CODE § 1546.1(a)(1) ("a government entity shall not . . . [c]ompel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.")

222 *See* CAL. PENAL CODE § 1546.1(b) (detailing the ways in which police can access the electronic information).

223 *Compare* CAL. PENAL CODE § 1546.1 (providing strict judicial oversight for user call log information) *with* Smith v. Maryland, 442 U.S. 735, 736 (1979) (allowing law enforcement to install a pen register to record incoming and outgoing caller information because it falls under the third-party doctrine).

equipment.[224] The law also gives the issuing judge the authority to appoint a special master (a qualified attorney) to ensure that only the information sought in the warrant is pursued by law enforcement, and that any additional unrelated information be destroyed.[225]

Washington passed a bill in 2015, which was the first of its kind to mention "cell-site simulator device" directly.[226] The law bans all use of Stingray-acquired evidence unless the law enforcement agency has a warrant based on probable cause, has the device user's informed consent, or "[acts] in accordance with a legally recognized exception to the warrant requirements."[227] The allowance of exceptions may be one of the law's greatest strengths because it only allows exceptions that would otherwise be recognized by the judge.[228]

Some other state laws speak exactly to what exceptions the legislature has in mind.[229] One of these exceptions could be generally classified as the "emergency exception."[230] Although states define the exception

---

[224] *See* CAL. PENAL CODE § 1546.1(a)(3) (2014) ("a government entity shall not . . . [a]ccess electronic device information by means of physical interaction or electronic communication with the electronic device.").

[225] *See* CAL. PENAL CODE § 1546.1(e)(1)–(2) (2014) (granting the Court discretion over the process by which the law enforcement gathers the evidence). The full text of this provision states:

> (e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following:
>
> (1) Appoint a special master . . . charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.
>
> (2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

Id. See also CAL. PENAL CODE § 1524(e) (2016) (providing the procedure by which a police officer can appoint a special master). The statute states that a special master is "a member in good standing of the California State Bar and who has been selected from a list of qualified attorneys that is maintained by the State Bar particularly for the purposes of conducting the searches." *Id.* § 1524(d)(1). The statute considers the special master to be a public employee. *Id.* The court is to make an effort to ensure that the special master has no relationship to any of the parties involved in the issuance of the search warrant. *Id.* Furthermore, any information that is obtained using a special master is confidential and only subject to be divulged by judicial inquiry. *Id.*

[226] *See* H.B. No. 1440, Wash. Sixty-Fourth Leg., First Spec. Sess. (Wash. 2015) (stating that the purpose of the law is to prohibit the use of cell site simulators without a warrant).

[227] *See id.* (providing the standard for all cell-site simulators by which law enforcement officers must comply).

[228] *See id.* (allowing judicially-recognized exceptions to the warrant requirement).

[229] *See* statutes cited *supra* note 133 (describing several exceptions to state Stingray laws).

[230] *See, e.g.*, IND. CODE § 35-33-5-12 (2016) ("[police must obtain a warrant] unless . . . exigent circumstances exist that necessitate using the tracking instrument without

differently, the notion is that if a police officer believes that a person's life is in danger, the officer can circumvent the typical warrant requirement.[231]

Another common exception is the good faith exception.[232] The good faith exception is a constitutionally recognized exception to the exclusionary rule.[233] The problem with allowing a good faith exception to apply to Stingray evidence is that it could potentially provide disincentives to police from using a high-degree of due diligence with the Stingray.[234] Unlike a typical police warrant to search personal property, the use of a Stingray can subject numerous citizens to a search at a single time.[235] With the highly-intrusive capabilities of the Stingray, there may need to be added measures that ensure the police are not abusing the Stingrays capabilities.[236] On the other hand, *United States v. Leon* provides a valuable rule, in that police officers that comply with substantially all of the warrant requirements in good faith, but discover a procedural defect after the fact, should not be punished.[237] However, the advantage of creating a very narrow good faith exception for the Stingray is that the police officers would be on notice that using the device is exceptional and requires a very high degree of due diligence.[238]

---

first obtaining a court order.); MINN. STAT. § 626A.42 (d) (2016) ("A government entity may obtain location information without a tracking warrant . . . in an emergency situation that involves the risk of death or serious physical harm to a person who possesses an electronic communications device"); MONT. CODE § 46-5-110(1)(b)(iv) (2016) ("A government entity may obtain location information of an electronic device [if] . . . there exists a life-threatening situation"); UTAH CODE § 77-23c-102 (2014) (providing that a separate statute allows police to gather cell location information in emergency situations).

231 *See* MONT. CODE § 46-5-110(1)(b)(iv) (2016) (allowing evidence to be admissible in life or death situations or if a person is in risk of being harmed physically).

232 *See* Ball, *supra* note 93 (describing the good faith exception and its common applicability to searches under the Fourth Amendment). *See also* Maryland v. Andrews, 134 A.3d 324, 364 (Md. Spec. App. 2016) (explaining that the good faith exception to the exclusionary rule will generally exist in situations where no officer-error exists).

233 *See id*. at 365 (citing Supreme Court precedent regarding the exclusionary rule). *See also* United States v. Leon, 468 U.S. 897, 890 (1984) (holding that the good faith exception is applicable in situations where the police officer relied on a warrant even if the probable cause upon which the warrant is granted is later found to be deficient as a matter of law).

234 *See Andrews*, 134 A.3d at 365 (refusing to allow the defendant to invoke the good faith exception to the exclusionary rule because the police had made warrant errors).

235 *See* Hernandez, *supra* note 54 (explaining that the Stingray can search through any cellphone within its radius without the user having knowledge).

236 *See supra* Part II.A.2 (providing that the Stingray has the ability to intercept/block communications, triangulate users' location, and gather information from all cellphones within range of the Stingray, all without the users or service provider having any knowledge that the search has occurred).

237 *See Leon*, 468 U.S. at 890 (holding that the exclusionary rule is subject to the good faith exception if the warrant has a minor defect).

238 *See* William J. Mertens & Silas Wasserstrom, *The Good Faith Exception to the Exclusionary Rule: Deregulating the Police and Derailing the Law*, 70 GEO. L.J. 365, 463 (1981) (explaining the

In conclusion, states have been enacting legislation in an effort to protect the privacy rights of their citizens.[239] Thus far, several states have enacted statutes, and still others are in the beginning stages of proposal.[240] However, some of these laws are currently too relaxed, and require added protections to ensure public privacy.[241]

IV. CONTRIBUTION

Legislators, both state and federal, are starting to address the alarming privacy concern associated with Stingray use.[242] Stingrays have the ability to gather communication and location data from all devices in radius, which potentially causes Fourth Amendment concerns.[243] In crafting anti-surveillance legislation or amending older laws, legislators should look at the capabilities of the Stingray holistically, which is currently lacking in some states.[244]

This Part will propose a three-pronged approach that legislators should consider when they are in the process of enacting Stingray privacy legislation.[245] First, Part IV.A.1 provides that legislators should make strict warrant requirements for police use of the Stingray.[246] Then, Part IV.A.2 proposes that legislatures should provide a deterrent for misuse of the Stingray, both for private citizens as well as law enforcement.[247] Finally, Part IV.A.3 argues that legislators should give discretionary

---

downfalls of the exclusionary rule, especially that it weakens the Fourth Amendment and fails to deter police from carelessly committing police misconduct).

239 *See* statutes cited *supra* note 133 (providing the states that have enacted legislation thus far). *See also supra* note 129 (providing the full text of the proposed Stingray Privacy Act of 2015).

240 *See* statues cited *supra* note 133 (illustrating that many states have already enacted legislation to deal with the Stingray).

241 *See, e.g.*, TENN. CODE § 39-13-610(c) (2014) (allowing several broadly defined exceptions that allow the Stingray evidence to be admissible).

242 *See* statutes cited *supra* note 133 (providing all the states that have adopted legislation for the Stingray).

243 *See supra* section II.A (explaining how Stingray technology creates privacy concerns for the public as a whole because it potentially can access the information of not only the target, but all of the persons within the Stingray's radius).

244 *See, e.g.*, VA. CODE § 19.2-56.2 (accessing only the capability of the Stingray to determine the location information of a device).

245 *See infra* Part IV.A (proposing a three-pronged approach that legislators can use when making standards applicable to Stingray technology).

246 *See infra* Part IV.A.1 (explaining how strict warrant requirements, like those in Washington, will help keep potentially invasive information out of the courtroom).

247 *See infra* Part IV.A.2 (arguing that some sort of criminal penalty should be imposed on those who abuse the capabilities of the Stingray).

powers to judges to use special procedures when issuing a warrant for the Stingray to ensure that public privacy is not hindered.[248]

A. Proposals

1. Make Strict Warrant Requirements For Police Use Of The Stingray

Legislators should keep in mind that the Stingray has very powerful capabilities and opens up real privacy concerns for the general public.[249] For this reason, legislatures should enact a standard that does not allow for broad exceptions.[250] However, because the technology is new, it may be best to grant more power to judges to adopt standards that are consistent with typical exclusionary rules.[251]

Washington's law provides a strong example of a state law that both requires a warrant, and allows the judiciary to apply legally recognized exclusions to the warrant requirement, except that it does not clearly state that information exchanged between cellphone and cell site simulator is not voluntary.[252] As a result, model language for an anti-surveillance clause on warrant requirements should follow Washington's standard, but with added language, which reads:

> The state and its political subdivisions shall not, by means of a cell site simulator device, collect or use a person's electronic data or metadata without:
>
> (1) that person's informed consent,
>
> (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized, or
>
> (3) acting in accordance with a legally recognized exception to the warrant requirements, *insofar as any data transmitted to or from a cellular device to or from a*

---

248 *See infra* Part IV.A.3 (promoting California's legislation, which allows the judge to appoint special masters and to quash any evidence not related to the investigation that may be gathered by a Stingray).

249 *See supra* Part II.A (discussing the various capabilities of the Stingray).

250 *See, e.g.*, Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015), full text at *supra* note 129 (allowing many exceptions that police can use to circumvent the typical warrant requirement).

251 *See* H.B. No. 1440, Wash. Sixty-Fourth Leg., First Spec. Sess. (Wash. 2015) (delegating to the judge the ability to determine whether Stingray-acquired evidence falls within typical judicially-recognized standards).

252 *See id.* (giving discretionary power to the judge to make evidentiary findings, while still mandating a warrant procedure).

> *cell site simulator device shall not be considered voluntarily rendered by the user to a third-party*.[253]

This provision is appropriately flexible to fit within the confines of recognized exceptions to the warrant requirement, but at the same time informs law enforcement that the warrant procedure must be followed notwithstanding any challenges with the third-party doctrine.[254]

2. Create a Deterrent for Both Police Misuse and Private Citizen Use of the Stingray

Currently, no state offers a criminal or civil penalty for violation of its Stingray Law.[255] However, as provided in the Stingray Protection Act of 2015, violation of the law will lead to punishment by fine or imprisonment.[256] Both private use of the Stingray, as well as unwarranted police use, should be explicitly a criminal act.[257]

One benefit of writing in a criminal penalty is that it will strongly deter privacy invasions.[258] Thus, future legislation should follow the federal standard, and model legislation should state, "[a]nyone who knowingly uses a cell site simulator [not in accordance to the warrant procedure] shall be punished by a fine or imprisonment for not more than 10 years, or both."[259] In sum, the possibility of a penalty is needed and the above provision works well as a deterrent.[260]

---

253 H.B. No. 1440 § 1, Wash. Sixty-Fourth Leg., 1st Spec. Sess. (Wash. 2015) (additional italicized text added by author).

254 *See id.* (providing strict language for a warrant).

255 *See* statues cited *supra* note 133 (outlining all the states that currently have enacted Stingray legislation). *But see* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (b) (2015), full text at *supra* note 129 (demonstrating that anyone in violation of the proposed law can be fined or imprisoned up to ten years).

256 *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (b) (2015), full text at *supra* note 129 (creating a specific deterrence in the statute by imposing penalties to those in violation).

257 *See id.* (criminalizing breaking the proposed federal statute). *See also* Pell & Soghoian, *supra* note 63 (addressing the fact that the Stingray is no longer just in the hands of police, and is now available to the public).

258 *See* Romboy, *supra* note 128 (explaining that the Stingray Privacy Act of 2015's co-sponsor Jason Chaffetz intended for the penalties to serve as a deterrent).

259 *See* Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. § (b) (2015), full text at *supra* note 129 (creating a penalty for violators).

260 *See id.* (proposing a fine or imprisonment up to ten years for knowing violators of the Act).

3. Judicial Discretion for Special Masters and Evidence Destruction

California is the only state that has enacted legislation that allows judges to have the discretionary ability to appoint a special master (court-appointed attorney) who will oversee the use of the Stingray.[261] This procedure helps ensure citizens' privacy by ensuring that the requirements of the warrant that are judicially proscribed are actually followed by the enforcing officers.[262] Additionally, the oversight of a special master adds credibility to law enforcement's case if and when the evidence procured needs to go to trial.[263]

California also gives judges discretionary power to destroy evidence not related to the warrant or investigation.[264] Given the fact that the Stingray can acquire evidence from unintended third-party users, this standard also helps ensure privacy of the public at large.[265] As such, a judicial oversight model clause for a Stingray should mimic the language of the California statute.[266] In sum, the judicial oversight provision appropriately allows for judges to oversee the warrant procedure to ensure that the Stingray is not misused during the search and that all data unrelated to the warrant is destroyed after the evidence has been gathered.[267]

B. Commentary

Some have argued that data sent through the air has no reasonable expectation of privacy because the cellphone user is sending the

---

[261] *See supra* note 225 (providing the text of the statutory provision that gives judges discretionary power to appoint a special master).

[262] *See* CAL. PENAL CODE § 1546 (establishing that the purpose of the statute is to better define current privacy interests and ensuring that electronic device information is private to the extent that it requires a warrant based off of probable cause before a search may be conducted).

[263] *See, e.g.*, *In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012) (holding that the pen register warrant was declined in part because the agent seeking the request did not have valid answers for exactly how the technology was going to be used in the investigation).

[264] *See supra* note 225 (providing the text of the statutory provision that gives judges discretionary power to destroy evidence that is unrelated to the purpose of the warrant).

[265] *See In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d at 748 (ruling by magistrate judge that the pen register warrant was denied due to concerns for other users' data who could be compromised as a result of the investigation).

[266] *See supra* note 225 (providing the full relevant statutory text that is advocated by the author).

[267] *See supra* note 225 (giving judges the ability to enforce the issuance of a warrant to use a Stingray).

information voluntarily to a third party (the phone company).[268] Therefore, under the third-party doctrine, police have a right to ensure public safety interests, which would otherwise be violations of individual privacy interests.[269] This argument concludes that, because cellphone data falls within the third-party doctrine, it should not be subject to probable cause and warrant requirements under the Fourth Amendment.[270] However, this argument misses the point because society has evolved to the point where the cellphone is oftentimes intrinsically connected to the user, with highly-personal content which requires added legal protection.[271]

Another argument is that promoting a standard that criminalizes police misuse of the device is going too far.[272] The argument states that the inability to use evidence gathered by the Stingray would be enough of a deterrent for police officers.[273] However, this argument fails to recognize the Stingray's invasive nature, in that if it is used carelessly, the Stingray has the potential to expose intimate secrets of virtually limitless unsuspecting users without any potential for recourse.[274]

Finally, an argument could be made that the judicial power to issue a warrant is the only power the judge should have in overseeing the

---

[268] *See supra* notes 144–48 and accompanying text (discussing the argument in favor of the third-party doctrine being applied to electronic data communications).

[269] *See supra* note 148 and accompanying text (explaining that in the absence of the third-party doctrine, criminal actors would use the Fourth Amendment as a shield to otherwise publicly-discoverable information).

[270] *See supra* notes 146–48 and accompanying text (providing the third-party doctrine advocates arguments, which are often advanced by the government, that cellphone data does not have a reasonable expectation of privacy because it is freely disseminated to third-parties).

[271] *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (ruling that police cannot go through the physical contents of their cellphone unless they have been issued a warrant). Writing for the majority in *Riley*, Chief Justice Roberts wrote:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life, []. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.

Id. (internal citation omitted).

[272] *See* Nelson, *supra* note 197 (questioning whether the Bill would go too far in acting as a deterrent for police officers).

[273] *See, e.g.*, MINN. STAT. § 626A.42(d) (2014) (providing no penalties for police officers who use the Stingray without a warrant, except that the evidence will be thrown out).

[274] *See supra* section II.A.2 (explaining the capabilities of the Stingray). *See also In re* the Application of the U.S. for an Or. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012) (ruling by judge that the concern of unintended user data to be compromised weighed against the issuance of a Pen Register order).

executive powers of the policing agency.[275] Again, this is a misunderstanding of the Stingray's capabilities.[276] With the appointment of a special master the judge can ensure that the device is only used for the capability that is stated in the warrant, which is a real concern, considering the Stingray's capabilities.[277] Additionally, the ability to destroy other evidence grants the judge the authority to ensure that data from private citizens is not inadvertently stored in a police database.[278] Thus, both of these judicial powers give a valid check on the police power of the law enforcement agency.[279]

V. CONCLUSION

For years, the FBI kept the use of the Stingray out of the public eye. Now, the Stingray's use by both state and federal law enforcement agencies is widely known. The Stingray is able to manipulate cell networks by acting as a fake tower, and in the process it can gather incoming and outgoing call information, intercept communications, and track locations of unsuspecting parties. Unfortunately, the Stingray does not fit well with any current federal privacy legislation. Indeed, neither the Federal Pen Register Statute, nor the Wiretap Act contain statutory language that directly encompasses all the abilities of the Stingray. To remedy this problem, state legislators across the country have enacted statutes. However, many states remain without legislation to guide the courts and police on the use of the Stingray. To best address the abilities of the Stingray, new legislation should include a threefold approach. First, the legislation should include strict warrant requirements that are flexible enough to conform to existing laws of evidence. Second, legislatures should consider enacting legislation that deters warrantless use of the Stingray, including both police and private citizens. Finally, legislators should consider enacting statutes that give judicial oversight of warranted use of the Stingray to best assure that public privacy is not undermined. In conclusion, the technology of Stingrays is developing, and the state

---

275 *See* U.S. CONST. art. I (granting police powers to the executive branch of government).

276 *See supra* section II.A.2 (explaining Stingray's abilities to intercept, locate devices, and take user information).

277 *Cf. supra* note 225 (providing the statutory language that gives the judge the discretionary ability to appoint a special master to oversee the use of the Stingray).

278 *See* Goldstein, *supra* note 179 (explaining how police in New York have created a database of phone information by subpoenaing phone carriers for information).

279 *See supra* notes 275–78 and accompanying text (detailing the arguments both for and against judicial use of the special master and the ability to quash unrelated evidence that turns up in a Stingray investigation).

legislatures have the unique opportunity to shape the future of information privacy in the United States.

Gregory Maleska[*]

[*] J.D. Candidate, Valparaiso University Law School (2018); B.A., Political Science, University of Minnesota-Morris (2014). I owe many thanks to my executive board, if only our government could work as smoothly as the editors of Volume 52. I also owe a great thanks to Kirsten Myers, Editor in Chief of Volume 51, your guidance was more helpful to me than you could possibly imagine. Last but not least, I'd like to thank my family and my fiancé for your love and support throughout my time in Law School.