UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 78 ● Spring 2017

NOTES

CELL SITE SIMULATORS: A CALL FOR MORE PROTECTIVE FEDERAL LEGISLATION

Laura DeGeer

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

NOTES

CELL SITE SIMULATORS: A CALL FOR MORE PROTECTIVE FEDERAL LEGISLATION

Laura DeGeer*

I. INTRODUCTION

It is unquestioned that many American citizens place great value on maintaining privacy from the spying eyes of government.[1] After the 2013 leak of classified NSA information by CIA employee Edward Snowden,[2] there has been a continuous conversation regarding the protection of technological privacy—the personal information that we store on our desktops, laptops, tablets, and phones.[3] Of these technologies, cell phones are possibly the most central to our everyday lives. We carry our phones nearly everywhere with us, usually clenched tightly in our palms. They contain our personal and work emails, text messages with loved ones, catalogs of pictures documenting the recent months and years of our lives, our banking information, and secrets that may be too private to keep where others may stumble upon them.

* Candidate for J.D., 2017, University of Pittsburgh School of Law; B.A., 2014, Honors Specialization, University of Western Ontario.

[1] *See, e.g.*, MARY MADDEN & LEE RAINIE, PEW RESEARCH CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE (2015).

[2] Jacob Stafford, Note, *Gimme Shelter: International Political Asylum in the Information Age*, 47 VAND. J. TRANSNAT'L L. 1167, 1168–71 (2014) (discussing Edward Snowden's actions and domestic and international asylum).

[3] *See* Jason M. Weinstein, William L. Drake & Nicholas P. Silverman, *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729 (2015).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

The American government and state officials are utilizing a newly developed device that directly affects this cellular privacy. These devices are called cell site simulators. With cell site simulators, officials are able to mimic cell towers and collect cellular data from any and all phones within a given geographic area.[4] This information enables officials to pinpoint where a certain cell phone is located, and they are then able to use that information in a variety of different ways.[5] The devices can be effective in narcotics investigations, tracking avalanche and kidnapping victims, as well as in other non-criminal investigations.[6] The most obvious benefit of cell site simulators is large-scale crime reduction, but at what cost?

The device is relatively new, so few states have developed legislation concerning its use, and Congress has not codified any guiding acts. There have been several Supreme Court decisions concerning personal privacy and its relation to physical searches of cell phones and the data contained therein,[7] as well as the use of technological surveillance in constitutionally protected areas.[8] However, there is yet to be a decision concerning the constitutionality of searches using cell site simulators. It is imperative that Congress draft a clear, in-depth bill enumerating when, how, and by whom a cell site simulator may be used. When drafting the bill, several considerations must be taken into account, including Supreme Court jurisprudence concerning Fourth Amendment protections against unreasonable searches and seizures and the current status of legislation in each state of the United States. These considerations are addressed and discussed in turn.

A. How They Work

Cell site simulators have been patented since at least 2002,[9] and they are used in a myriad of police investigations. The Department of Homeland Security ("DHS")

---

[4] *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185–86 (2014) ("Unfortunately, this device is capturing similar information from all the cell-phones in the surrounding area.").

[5] *Id.* at 192–94.

[6] U.S. Dep't of Justice, *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators* (Sept. 3, 2015) (mentioning some of the beneficial uses of cell-site simulators), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators; *see also* U.S. Dep't of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, https://www.justice.gov/opa/file/767321/download (last visited Oct. 20, 2016).

[7] *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014).

[8] *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001).

[9] *See* Owsley, *supra* note 4, at 186.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

often provides funding to buy and use them for regional terrorism investigations,[10] but they have also been used for generic, common criminal investigations.[11]

Cell towers are used by cellular service providers to collect information, such as "the cell tower nearest to a particular phone, the portion of that tower facing the phone, and often the signal strength of that phone."[12] Cell site simulators work by mimicking cell-towers to collect "a number of pieces of data" from phones in a given geographical area.[13]

Whenever a phone is turned on, it "registers";[14] it sends a signal seeking the closest cell tower, which then registers the phone with that cell site.[15] This registration happens approximately every seven seconds.[16] When a cell site simulator is the nearest cell site, the phone will treat the device as a cell tower and share its information.[17] This process allows the cell site simulator users to collect a plethora of information from an unknown amount of people almost instantaneously. The requirement to consistently connect with a cell tower for reception enables cell phones to be used as tracking devices.

Cell site simulators are mainly produced by the Harris Corporation, which dubs them TriggerFish and StingRays.[18] With the right knowledge and finances, however, any individual could potentially make their own.[19] This alone should necessitate federal legislation that at least criminalizes the private development and use of cell site simulators.[20]

---

[10] *Id.*

[11] *Id.* (providing examples of burglary and murder).

[12] *Id.* at 189.

[13] *Id.* at 187–88.

[14] *Id.* at 188.

[15] *Id.*

[16] *Id.* at 188–89.

[17] *Id.*

[18] *Id.* at 191.

[19] *Id.* (noting that it takes approximately $1,500.00 to purchase the components to make a cell-site simulator).

[20] Omnibus Crime Control and Safe Streets Act of 1968, 90 Pub. L. No. 351, § 2511, 82 Stat. 197, 213–14, prohibits persons from intercepting wire, oral, or electronic communication; or from using any information "obtained through the interception of a wire, oral, or electronic communication." Although

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

The use of cell site simulators developed from the government's wiretapping capabilities.[21] Federally regulated wiretapping began in 1968 with the passage of the Wiretap Act[22] in response to *Katz v. United States*,[23] but it was amended in 1986 to include updated, previously unavailable technologies.[24] Similarly here, an act that corresponds to the current technological milieu within the United States is necessary. The use of cell site simulators to secretly and seamlessly collect mass information from an unquantifiable number of citizens at one time is an invasion of personal privacy that has yet to be federally recognized or codified as such.

II. FOURTH AMENDMENT SUPREME COURT HISTORY

The Fourth Amendment provides:

> [1] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[25]

A. The "Right" to Privacy

The text of the Fourth Amendment makes clear that *reasonableness* is what determines whether a search or seizure is constitutional.[26] Thus, in the following

---

the Act prohibits using technological devices to intercept communications, it does not criminalize the personal creation of a cell site simulator. *See id.*

[21] *See* Owsley, *supra* note 4, at 194–200.

[22] 18 U.S.C. §§ 2510–2522 (2012).

[23] *See* Katz v. United States, 389 U.S. 347 (1967) (holding that telephone conversations cannot be intercepted without a search warrant).

[24] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508 (codified at 18 U.S.C. §§ 2510–2522, 2701–2709, 3121–3127) (noting that conversations are no longer solely carried through wires, as "[a] phone call can be carried by wire, by microwave or fiber optics . . . [and can be] transmitted in the form of digitized voice, data[,] or video").

[25] U.S. CONST. amend. IV.

[26] Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

analysis, reasonableness should be kept in mind as a motivating factor for the Court's decisions concerning what is afforded constitutional protection.

The Court in *Griswold v. Connecticut*[27] recognized privacy as an inherent aspect of the Constitution, holding that the constitutional "right" to privacy was implicit in the Third, Fourth, Fifth, and Ninth Amendments.[28] The Fourth Amendment right of citizens to be secure in their persons and effects is pertinent to our analysis.

The Fourth and Fifth Amendments were described in *Boyd v. United States*[29] as protections against all governmental invasions of the "sanctity of a man's home and the privacies of life."[30] Even prior to the privacy holding of Griswold, in *Mapp v. Ohio*, the Court had "referred . . . to the Fourth Amendment as creating a right to privacy, no less important than any other right carefully and particularly reserved to the people."[31] This notion of privacy, and the importance the public places on it, is what governs the reasonableness analysis of Fourth Amendment search and seizure jurisprudence.[32]

The fact that Supreme Court jurisprudence has placed such an emphasis on the right to privacy as implicit within the Constitution supports the claim that citizens would not likely be comfortable with the government discretely collecting and using their cellular data.

B. Searches and Seizures

The Supreme Court has repeatedly re-visited the question of what state actions constitute searches for Fourth Amendment purposes.[33] In doing so, the main question

---

[27] *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

[28] *Id.* at 484–85 (ruling that, because of the penumbra of the Ninth Amendment, the Constitution protects a right to privacy implicit in the Fourth Amendment right of people to be secure in their persons).

[29] Boyd v. United States, 116 U.S. 616 (1886).

[30] *Id.* at 630.

[31] *Griswold*, 381 U.S. at 484–85 (quoting Mapp v. Ohio, 367 U.S. 643, 656 (1961)).

[32] *See infra* Part II(B).

[33] *See, e.g.*, Katz v. United States, 389 U.S. 347, 360 (1967) (finding that attaching an electronic listening and recording device to a public telephone booth constituted a search and seizure); United States v. Jones, 565 U.S. 400 (2012) (finding that using a device to monitor a vehicle's movements constituted a search); Kyllo v. United States, 533 U.S. 27 (2001) (finding that using technology to obtain information from inside a home where such information could not otherwise have been obtained without physical intrusion

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

to be asked regarding searches of persons and their effects is whether the individual had a reasonable expectation of privacy in the thing being searched.[34] The general rule is that where an individual has a subjective expectation of privacy, and that expectation is one that the public would also objectively support and acknowledge as valid, the individual then has a reasonable expectation of privacy and cannot be searched without a warrant.[35] Therefore, when state actions constitute searches under the Fourth Amendment, a warrant must precede the search.[36]

After the Court articulated this general rule, a multiplicity of other cases were decided, expanding and limiting the scope within which individuals have a reasonable expectation of privacy, allowing for fewer and more searches, respectively.[37]

1. Broadening the Scope of Reasonable Expectations of Privacy

Methods of gathering information are consistently an issue when determining whether state actions constitute searches. It is clear that when an officer is physically searching through an individual's purse, there is a reasonable expectation of privacy that necessitates the preexistence of a warrant supported by probable cause.[38] The picture is muddied, however, when physical intrusions are not present and technology is the medium through which officers engage in surveillance and data collection. The general rule is: "Technologically assisted surveillance becomes a search and requires a search warrant when police use advanced surveillance devices not in general public use to spy on activities carried on in private."[39]

---

constituted a search); Riley v. California, 134 S. Ct. 2473 (2014) (finding that going through the digital contents of a cell phone incident to arrest constitutes a search).

[34] *See* JACQUELINE R. KANOVITZ, CONSTITUTIONAL LAW FOR CRIMINAL JUSTICE 179 (14th ed. 2015).

[35] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (explaining that the majority opinion articulates a two-prong test to determine whether an individual has a reasonable expectation of privacy).

[36] *See* U.S. CONST. amend. IV; KANOVITZ, *supra* note 34, at 185.

[37] *See, e.g.*, California v. Carney, 471 U.S. 386 (1985); *Jones*, 565 U.S. 400; Maryland v. Dyson, 527 U.S 465 (1999); United States v. Miller, 425 U.S. 435, 443 (1976); Rakas v. Illinois, 439 U.S. 128 (1978); Rawlings v. Kentucky, 448 U.S. 98, 104 (1980); *Riley*, 134 S. Ct. 2473.

[38] *See, e.g.*, *Rawlings*, 448 U.S. at 104 (noting that the owner of a handbag is the individual with a reasonable expectation of privacy in that handbag); *See also Rakas*, 439 U.S. 128 (articulating an individual's right to privacy in their personal property and effects under the Fourth Amendment).

[39] KANOVITZ, *supra* note 34, at 279.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

In *United States v. Jones*,[40] officials attached a GPS tracker to the bottom of a man's vehicle to monitor his movements for approximately a month under an expired warrant.[41] In that case, the Court held that because the information was obtained by physically *occupying* the individual's property, there was a search in violation of the Fourth Amendment.[42] The Court analyzed the issues from the standpoint of property law and trespass, and it maintained that the general rule previously articulated[43] was a deviation from the earlier property-based Fourth Amendment jurisprudence.[44] Although the *Jones* majority opinion has been viewed negatively[45] Justice Sotomayor's concurrence allowed for future Courts to bypass the property-based analysis and revert back to the reasonable expectation of privacy test as articulated in *Katz*.[46]

Another technological mode of collecting data faced the Supreme Court in *Kyllo*, where state agents used a thermal imager to find "hot spots" within a home where the owner was suspected of growing marijuana.[47] The hot spots were then used to obtain a warrant.[48] The Court determined that, while the imager did not physically penetrate the home,[49] the amount of privacy one expects within their home

[40] *Jones*, 565 U.S. at 400.

[41] *Id.* at 402–03.

[42] *Id.* at 404–05.

[43] *See supra* note 34 and corresponding text (explaining that when determining whether a search requires a warrant, the main question is whether the individual had a reasonable expectation of privacy in the thing being searched).

[44] *Jones*, 565 U.S. at 404–05 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

[45] *See generally* Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1 (2012) (discussing the effects of the *Jones* opinion).

[46] *Jones*, 565 U.S. at 414 (Sotomayor, J. concurring) (positing that *Jones* would have come out the same way regardless of whether the analysis was rooted in property law and trespass or in the reasonable expectation of privacy test formulated in *Katz*).

[47] Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

[48] *Id.* at 30.

[49] Under *Jones*, physical penetration of the home would likely have been necessary to amount to a search, as physical presence is required under property and trespass law. *See* 565 U.S. at 404–05.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

is great enough to place a proverbial barrier at the entrance to the home past which officials may not intrude, in any manner, without a warrant.[50]

Cell phones became the subject of Fourth Amendment privacy dicta in *Riley*,[51] where it was deemed that because a cell phone is essentially an extension of a person, similar to a technological fifth-limb,[52] a warrant was necessary to access its stored information during a search incident to a valid arrest.[53]

The Court in *Riley* held that there is a distinction between cell phones and other physical possessions that may be subject to a search after arrest.[54] Because of the vast quantity of personal data stored within the phone (the privacy issue), and the trivial physical threat they pose to law enforcement interests, the necessity of an on-site search was found to be minimal and a warrant was required.[55]

It is important to distinguish that, in *Riley*, the phone was searched for information pertinent to that specific person's activities, and the collected data would have been used in relation to that individual citizen.[56] Distinctively, cell site simulators collect more data from non-target individuals than from target individuals. Since cell site simulators gather all of the cellular information in a given geographical area, most of the gathered information is ancillary. Regardless of whether the gathered information would ever be used, it would still be collected without consent or prior knowledge, and that is where the true constitutional issues lie. By applying additional limitations to the use of cell site simulators,[57] information

---

[50] *Kyllo*, 533 U.S. at 34 ("We think that by obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use." (citation omitted)).

[51] *See generally* Riley v. California, 134 S. Ct. 2473 (2014).

[52] *See id.* at 2488–89.

[53] *Id.* at 2495, 2473. A search incident to a valid arrest is an exception to the warrant requirement for searches. During a search incident to a valid arrest, an officer may search the individual if they believe that he or she is within reach of a weapon, or if they believe evidence of the suspected crime could be destroyed. *See, e.g.*, *id.* at 2488.

[54] *Id.* at 2485.

[55] *Id.* at 2485–86.

[56] *Id.* at 2480–81 (The police were looking for evidence of the defendant's involvement in the "Bloods" street gang).

[57] *See infra* Part IV(A) & (B).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

gathered could come with a guarantee that it would not be used against a non-target of the initial search.

2. Limiting the Scope of Reasonable Expectation of Privacy

Although fewer things may be searched without a warrant, and fewer devices may be used to subvert privacy protections, the scope of one's reasonable expectation of privacy has also been limited by the broad exceptions to the general warrant requirement. Although the Supreme Court has expressed its preference that searches be conducted under the authority of a warrant,[58] four exceptions to the requirement currently exist. Warrants are not necessary (1) when there is consent, (2) when the search is incident to a valid arrest ("SIVA"), (3) when authorities have probable cause to believe that evidence is inside a vehicle, and (4) when exigent circumstances are present.[59] For reasons specific to each exception, the only one pertaining to our analysis is that of exigent circumstances.

The consent exception does not apply to situations involving cell site simulators because the individuals at issue are unaware that their data is being collected and therefore are incapable of consenting to its collection.[60] Under the SIVA exception, a search incident to a valid arrest must be preceded by an arrest. This situation is highly unlikely in cases involving cell site simulators, as the devices are primarily used to obtain evidence that will ideally *lead* to an arrest. If there were a valid arrest, however, officers would still be unable to search a cell phone without a warrant, as per the protections of *Riley*.[61] Although police may search the vehicle when they have *probable cause* to believe that it contains contraband or evidence of criminal

[58] *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting Katz v. United States, 389 U.S. 347, 357 (1967) (noting that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions").

[59] *See, e.g.*, California v. Carney, 471 U.S. 386 (1985).

[60] It could be argued, however, that because cellular providers already collect a lot of this data through cell-towers, and consumers of the services *consent* to it in the contracts they sign when they purchase their phones, that perhaps this consent to third parties could also be read as consent to the government. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (noting that a defendant forfeits Fourth Amendment protection in *any* information that is knowingly revealed to a third party, even though it may only be revealed for a limited purpose).

[61] *See* Riley v. California, 134 S. Ct. 2473, 2489–93 (2014) (holding that because a cell phone is essentially a miniature computer, sometimes containing more personal information than could ever be found on a person's person, they cannot be searched incident to a valid arrest without a warrant).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

activity,[62] vehicles are not cell phones, and thus, are not capable of being searched by a cell site simulator in this capacity.

Exigent circumstances exist where there is a call for urgent and immediate action.[63] The main exigencies include the pursuit of a fleeing suspect, threats to officer safety, and the potential for destruction of evidence.[64]

When acting under the exigent circumstances exception, the search must be limited to action *immediately necessary* to address the exigency that allowed for the search.[65] In the case of potential destruction of evidence, the search itself cannot be completed until a warrant is issued.[66] For example, if police have reasonable suspicion that narcotics relating to a drug investigation are inside a house and could be destroyed at any time, they may enter without a search warrant to ensure that no evidence is tampered with.[67] However, they may not initiate the actual search until they obtain a search warrant.[68] It is important to distinguish this exception to the warrant requirement because a warrant is still necessary; the exigency simply gets them through the proverbial door to protect against the destruction of any evidence that may be uncovered during the search.

All of these requirements, along with their exceptions, relate to obtaining a search warrant for a *specific* individual or place, and to any evidence obtained from that individual or place. With cell site simulators, however, the search extends to far more citizens than the target individual.[69] Therefore, certain safeguards must be put in place to ensure that, when there is no reasonable suspicion against an individual, no collected cellular information may be stored or used against them.

---

[62] *See, e.g.*, Maryland v. Dyson, 527 U.S 465 (1999).

[63] *See, e.g.*, Brigham City v. Stuart, 547 U.S. 393, 405 (2006) ("[W]arrants are generally required to search a person's home or his person unless the exigencies of the situation make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment." (citation omitted) (internal quotation marks omitted)).

[64] *See, e.g.*, Segura v. United States, 468 U.S. 796 (1984).

[65] *See* KANOVITZ, *supra* note 34, at 189.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *See* Owsley, *supra* note 4 and accompanying text.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

Because the Supreme Court has held that cell phones are entitled to protection from warrantless searches and seizures,[70] it is only logical that they should also be properly protected from searches conducted with cell site simulators. However, the legislation as it currently stands lacks practicality.

III. CURRENT LEGISLATION

Until recently, no state had addressed or drafted legislation concerning the use of cell site simulators. Within the past few months, with incentive likely coming from the ongoing tension between privacy rights and state interest in public safety, as well as the regulations released by the Department of Justice ("DOJ"),[71] some states have begun drafting and proposing legislation governing the use of cell site simulators.

In September 2015, the DOJ released a set of guidelines pertaining to department-wide use of cell site simulators for domestic criminal investigations.[72] The guidelines call for warrants, a data handling program instituting daily deletions of stored information, and declare that no stored cellular information such as emails, text messages, photographs, or contact lists may be collected.[73] Additionally, the release notes how instrumental cell site simulators have been in "kidnappings, fugitive investigations, and complicated narcotics cases."[74]

Since individual states are not bound by the DOJ regulations, several have begun drafting, introducing, and codifying state bills pertaining to cell site simulator use.[75] In some of the bills, adherence to the DOJ regulations is, at best, tenuous. That being said, much of the drafted legislation includes similar provisions. For example, all states that allow use of the technology require either a warrant or a court order

[70] *See* Riley v. California, 134 S. Ct. 2473 (2014).

[71] *See supra* note 6.

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *See, e.g.*, 725 ILL. COMP. STAT. 137/10 (2016) (effective Jan. 1, 2017); WASH. REV. CODE § 9.73.260 (2015); H.B. 138, 2015 Reg. Leg. Sess. (La. 2015) (introduced Mar. 24, 2015; withdrawn from further consideration); H.B. 904, 2016 Reg. Sess. (Md. 2016) (introduced Feb. 10, 2016; failed); H.B. 2214, 98th Gen. Assemb. 2d Reg. Sess. (Mo. 2016) (introduced Jan. 13, 2016; failed); L.B. 738, 104th Leg., 2d Reg. Sess. (Neb. 2016) (introduced Jan. 6, 2016; failed); A.B. 8055, 238th Ann. Legis. Sess. (N.Y. 2015) (introduced June 5, 2015); H.B. 2046, 2015 Reg. Sess. (Pa. 2016) (introduced May 9, 2016); H.B. 7681, 2015 Reg. Sess. (R.I. 2016) (introduced Feb. 24, 2016); H.B. 4522, 121st S.C. Gen. Assemb., 2d Reg. Sess. (S.C. 2015) (introduced Dec. 3, 2015; failed); H.B. 3165, 84th Leg. Sess. (Tex. 2015) (introduced Mar. 11, 2015; pending).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

before granting its use.[76] It should be noted that far more states require a court order rather than a warrant.[77]

Of the states that allow cell site simulator use, each requires that, to obtain a warrant or court order, the telephone number or name of the individual who owns the suspected device must be known.[78] All but two states require regular deletion of collected data.[79]

The information necessary for obtaining either a court order or a warrant varies between states. In Maryland, not only may a court order be granted when there is probable cause to believe that either a felony *or* a misdemeanor "has been, is being, *or will be* committed . . . ,"[80] but also when there is probable cause to believe that the evidence to be obtained while using the device "is . . . or will lead to evidence of, the

[76] These two methods of obtaining judicial approval may vary in the burdens they place on obtaining approval for cell site simulators, as one requires reasonable suspicion while the other does not. In the Eleventh Circuit, distinctions have been made between the types of information that may be obtained with a subpoena (subscriber information), court order (customer usage or purchase records), or a search warrant (email contents, documents in online cloud storage). *See, e.g.*, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (discussing statutory requirements under which the government can require a cellular carrier to disclose customer records).

[77] *See supra* note 75; *see infra* note 120 and accompanying text.

[78] *See, e.g.*, WASH. REV. CODE § 9.73.260(4)(C)(ii) (2015) (requiring the "telephone number or other unique subscriber account number"); H.B. 138, 2015 Reg. Leg. Sess. § 1315(B)(2)(A) (La. 2015) (requiring a "telephone number or other unique subscriber account number" for the target device); H.B. 904, 2016 Reg. Sess. § 1-203.1(b)(3)(II)(2) (Md. 2016) (requiring the unique subscriber account number for the target device); H.B. 2214, 98th Gen. Assemb. 2d Reg. Sess. § 542.405(3)(2) (Mo. 2016) (requiring the "telephone number or other unique subscriber account number"); A.B. 8055, 238th Ann. Legis. Sess. § 700.30(4)(3) (N.Y. 2015) (requiring a "telephone number or other unique subscriber account number" of the target device); H.B. 3165, 84th Leg. § 4(14A)(D)(2) (Tex. 2015) (requiring the identification of the "cellular telephone or other wireless communications device to be monitored").

[79] *See* H.B. 138, 2015 Reg. Leg. Sess. §§ 1315(F)(2), (F)(3) (La. 2015) (requiring immediate deletion for non-target data, and 30 days for target data if there is no longer probable cause to support the belief that the data is evidence of a crime); H.B. 904, 2016 Reg. Sess. §§ 1-203.1(C)(2)(1), (4) (Md. 2016) (requiring immediate deletion with a forty-eight hour grace period for non-target data, and requiring deletion within thirty days where there is no longer probable cause for target data); H.B. 2214, 98th Gen. Assemb. 2d Reg. Sess. §§ 542.405(5)(2)-(3) (Mo. 2016) (requiring immediate deletion for non-target data, and thirty days for target data if there is no longer probable cause); A.B. 8055, 238th Ann. Legis. Sess. (N.Y. 2015) (requiring immediate deletion for non-target data, and within thirty days for target where there is no longer probable cause).

[80] H.B. 904, 2016 Reg. Sess. (Md. 2016) (emphasis added).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

misdemeanor or felony."[81] Of the states with proposed legislation, Maryland has one of the broadest thresholds for approving cell site simulator use.

All of the states propose a number of days within which the warrant or order is valid.[82] Beyond that date, all allow for applications for extension, in most cases for the same amount of time as the principal term of warrant validity.[83] These principal terms vary greatly, from seven days in New York,[84] to ninety days in Texas.[85] Of note is the differences between New York's principal warrant term for cell site simulators compared to other eaves dropping and video surveillance warrants. For the latter, the term may extend to thirty days, but, as previously mentioned, for cell site simulators it may only be extended for seven.[86]

Some proposed bills also state that any information collected from non-targets cannot be transmitted, used, or retained for any purpose, such as further criminal investigations and trials.[87] However, of the eleven states with proposed and passed legislation,[88] only four have provided for this protection.[89] The idea that no non-target data can be used against the non-targets is one that should be given far more weight than it currently is. Without such a provision, the government could essentially obtain a warrant for one person and, through the incidental collection of non-target data, could potentially charge hundreds of other people with large- and small-scale crimes—all without the requisite probable cause necessary to obtain and retain the non-target's information in the first place. Essentially, without a provision protecting non-targets from prosecution on the basis of their incidentally collected data, the warrant requirement would be superfluous.

---

[81] *Id.*

[82] *See supra* note 75.

[83] *Id.*

[84] A.B. 8055, 238th Ann. Legis. Sess. § 6 (N.Y. 2015).

[85] H.B. 3165, 84th Leg., Reg. Sess. § 4 (14A)(E) (Tex. 2015).

[86] A.B. 8055, 238th Ann. Legis. Sess. § 2.2 (N.Y. 2015).

[87] *See* H.B. 138, 2015 Reg. Leg. Sess. § 1315(F)(2) (La. 2015); H.B. 3165, 84th Leg. § 4(I)(1)(B) (Tex. 2015); H.B. 904, 2016 Reg. Sess. § (F)(3) (Md. 2016).

[88] *See supra* note 75.

[89] WASH. REV. CODE § 9.73.260(6)(C) (2015); H.B. 904, 2016 Reg. Sess. § 1-203.1(C)(2)(II) (Md. 2016); H.B. 2214, 98th Gen. Assemb. 2d Reg. Sess. § 542.400(5)(2) (Mo. 2016); A.B. 8055, 238th Ann. Legis. Sess. § 2(2) (N.Y. 2015).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

Washington and Illinois are the only states to codify cell site simulator legislation thus far.[90] While Illinois does not enumerate a primary term for warrant validity specific to cell site simulators,[91] Washington allows for a sixty-day primary term, with a possible sixty-day extension.[92] Similar to other states, Washington outlines situations in which a court order is not necessary. Those exceptions are narrower than the exceptions detailed in the general warrant requirement previously discussed.[93] In Washington, a court order is not required in situations where there is "immediate danger of death or serious bodily injury."[94] The general warrant requirements acknowledge exigent circumstances where there is merely a possibility of danger or where a valid arrest has taken place.[95] The fact that the exceptions are narrower is interesting because many of the exceptions to the warrant requirement for searches and seizures rarely apply to cell site simulators.[96] Arguably, they apply de jure, as there is still a search being conducted, but not de facto, as the requisite circumstances for the exceptions are highly unlikely to be present in the same situations where police seek to use cell site simulators. This is precisely why there must be detailed and thorough limiting provisions in any federal bill pertaining to the use of cell site simulators.

The proposed Maryland legislation is distinctively limiting with its prohibition on "exploratory" use of the devices, meaning they cannot be used unless the general location of the cellular device is known.[97] New York, although prescribing court orders rather than warrants,[98] has a particularly attractive section, which may be more acceptable for the majority of society. Not only does New York's proposed legislation limit the principal term of validity to seven days with a corresponding potential extension, it also states that,

---

[90] 725 ILL. COMP. STAT. 137/10; WASH. REV. CODE § 9.73.260.

[91] 725 ILCS 137/10.

[92] WASH. REV. CODE § 9.73.260(1)(D).

[93] WASH. REV. CODE § 9.73.270(6)(A).

[94] *Id.*

[95] *See supra* Part II(B)(2).

[96] *Id.*

[97] *See* H.B. 904, 2016 Reg. Sess. (Md. 2016).

[98] A.B. 8055, 238th Ann. Legis. Sess. § 2(2) (N.Y. 2015); *see also infra* note 115 and accompanying text (discusses the differing evidentiary bases for obtaining a warrant versus a court order).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

> [a]n order authorizing eavesdropping through use of a **cell site simulator** device must include a provision directing that the law enforcement agency (I) take all steps necessary to limit the collection of any information or metadata to the target specified in the warrant, (II) take all steps necessary to permanently delete any information or metadata collected from any party not specified in the applicable warrant immediately following such collection and must not transmit, use, or retain such information or metadata for any purpose whatsoever, and (III) delete any information or metadata collected from the target specified in the warrant within thirty days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.[99]

By including (III) in the provision, the legislation takes protection of privacy more seriously: it ensures that even though there *may have been* probable cause to believe someone committed, was committing, or was about to commit a crime which allowed for approval of a court order, if that probable cause no longer exists, the government may not retain the collected data for further use past the specified thirty-day period.[100] Thus, no matter what information is collected, it cannot be stored for more than thirty days without continuing probable cause. Many states also include a provision specifying that the target of the investigation must be notified of their target status within a certain amount of time after their data has been collected.[101]

These, as well as the other commonalities between drafted and passed legislation, paint the picture that inter-state concerns are relatively aligned regarding the use of cell site simulators, making it a more desirable option to pass one federal bill codifying the use of cell site simulators throughout the country, in line with Fourth Amendment jurisprudence. These proposed and passed state bills should be used as models upon which to draft more extensive and protective federal legislation. In particular, New York's limiting provision,[102] Maryland's no-exploratory-use

---

[99] *Id.* (emphasis in original).

[100] Louisiana has a similar provision, but specifies thirty-five days instead of thirty. H.B. 138, 2015 Reg. Leg. Sess. (La. 2015). However, the rest of Louisiana's legislation allows for broad use, and does not require the target to be notified that they are the subject of an investigation or that their data was collected. *Id.*

[101] *See, e.g.*, H.B. 904, 2016 Reg. Sess. (Md. 2016); H.B. 2214, 98th Gen. Assemb. 2d Reg. Sess. § 452.405(8) (Mo. 2016); H.B. 3165, 84th Leg. Sess. § 14A(H) (Tex. 2015) (indicating that the officer must do so within seven days of the data collection); *but see* H.B. 138, 2015 Reg. Leg. Sess. § 1315D(2) (La. 2015) (requiring the lessor or owner of the device to not disclose to anyone "the existence of the . . . cell site simulator device or the existence of the investigation to . . . any other person").

[102] A.B. 8055, 238th Ann. Legis. Sess. § 4(11) (N.Y. 2015).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

provision,[103] and the common prohibition on use of non-target data, are three provisions that should be considered as foundations for federal cell site simulator legislation.

A. Why There Should be Federal Legislation Pertaining to Cell Site Simulators

> Because criminals of all types use cell phones, mobile devices, and Internet-based means of communication more than ever, electronic evidence is now critical in prosecuting cases involving terrorism, espionage, violent crime, drug trafficking, kidnapping, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses.[104]

Although the term "search" was originally interpreted to require a physical intrusion into one's papers, houses, persons, and effects, as delineated by the Fourth Amendment,[105] technological advances have necessitated additional safeguards. The advent of the telephone meant that people could communicate instantly and with ease from a distance, but it also meant that the government had a new way of gathering information—namely, wiretapping.[106] Similarly, the recent use of cell cite simulators requires that new legislative protections be implemented uniformly throughout the United States.[107] A *federal* bill is necessary because, under the Equal Protection Clause of the Fourteenth Amendment, a state is not allowed to "deny any person within its jurisdiction the equal protection of the laws."[108] Although the Fourteenth Amendment's Equal Protection Clause applies only to state governments, the Fifth Amendment's due process clause has been interpreted to impose the same requirement on the federal government.[109] When the state enacts legislation, it cannot

---

[103] H.B. 904, 2016 Reg. Sess. § 1-203.1(c)(1)(III) (Md. 2016).

[104] *See* OWSLEY, *supra* note 4.

[105] *See* KANOVITZ, *supra* note 34, at 179.

[106] *Id.*

[107] In addressing the issue of wiretapping, the Supreme Court has long acknowledged a court may not "distinguish between electronic surveillance which is carried out by means of a physical entry and surveillance which penetrates a private area without technical trespass." *See* Alderman v. United States, 394 U.S. 165, 179 n.11 (1969).

[108] U.S. CONST. amend. XIV.

[109] *See, e.g.*, Adarand Constructors, Inc. v. Peña, 515 U.S. 200 (1995); Bolling v. Sharpe, 347 U.S. 497 (1954).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

lead to unfair treatment of individuals at the hands of the government without a proper governmental objective.[110] A thorough federal bill delineating rules that all states must uniformly follow must be passed through Congress to ensure that these constitutional protections are not violated.

Although a house bill has been introduced to federally regulate the use of cell site simulators by amending Title 18 of the United States Code,[111] the effect of which would be a federal law binding all state authorities,[112] the proposed provisions do little in the way of protecting privacy when cell site simulators are used for searches. There are, however, some appealing aspects to the proposal as written.

The bill pushes for a potential ten-year sentence of incarceration for any unauthorized use, which includes any non-governmental entity that possesses and uses a cell site simulator.[113] This provision is appealing because it ensures that companies or other entities with the knowledge and resources necessary to assemble their own devices would be barred from putting those devices into use.[114] However, it does not criminalize individual creation of cell site simulators, and, for that reason, it is inadequate.[115]

Additionally, the bill fails to mention the data collected from non-targets, effectively allowing for states to collect and store as much of it as they want.[116] This would be, without question, a violation of society's perception of the constitutional right to privacy.

By creating a uniform standard for cell site simulator use, enforcement agencies could ensure that they are protecting the privacy held in one's person as extended through cellular devices[117] from arbitrary searches and seizures of cellular data.

---

[110] *See Bolling*, 347 U.S. at 499–500.

[111] Stingray Privacy Act, H.R. 3871, 114th Cong. (1st Sess. 2015) (introduced Nov. 2, 2015; referred to subcommittee on Crime, Terrorism, Homeland Security, and Investigations Dec. 4, 2015).

[112] *See* 1 U.S.C. § 204 (2012).

[113] Stingray Privacy Act, H.R. 3871, 114th Cong. (1st Sess. 2015).

[114] *See supra* Part I(A).

[115] *See* Stingray Privacy Act, H.R. 3871, 114th Cong. (1st Sess. 2015).

[116] *Id.*

[117] The Supreme Court has previously described cell phones as an extension of the person and therefore subject to the same constitutional protections against unreasonable searches and seizures. *See* Riley v. California, 134 S. Ct. 2473, 2484–85 (2014).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

IV. WHAT THAT LEGISLATION SHOULD ENTAIL

Any time a constitutional right is at issue, the nation should be on alert for potential inter-state discrepancies that could amount to due process violations. Because the use of cell site simulators developed from the government's wiretapping technologies,[118] protections should flow in the same manner.

To start, it should be a federal offense to privately create or use your own cell site simulator. Without a provision such as this, it would be impossible to determine who has access to our cellular data at any given time, and we would not know what those individuals might do with that information. With legislation regulating governmental use of cell site simulators, citizens may feel a sense of security knowing that their information cannot be used against them and will be permanently deleted if they are not the targets of the investigation.

Additionally, to access the information, a warrant should be required rather than a court order. Judges issue court orders, whereas neutral and detached magistrates issue warrants.[119] By enforcing warrants, it is more likely that the appropriate level of probable cause will be present before granting the use of cell site simulators in any given situation. Although a majority of the states that have drafted legislation enumerate warrant-like guidelines for approval of court orders, the fact remains that a state may grant a court order, but not a warrant, on less than probable cause.[120] By mandating warrants in every state, none will be able to subvert the reasonable expectation of privacy required by Fourth Amendment jurisprudence.

The Court in *Riley* held that searching a cell phone incident to a valid arrest must be predicated by a warrant because of the private data it contained.[121] Therefore, it seems logical to posit that a warrant should also be required for collecting cellular data without the owner's permission by mimicking a cell tower. However, even with the tensions surrounding personal privacy, there are certain situations where allowing warrantless use of cell site simulators may be beneficial to society.

---

[118] *See supra* note 21 and accompanying text.

[119] *See, e.g.*, *What is the* Difference *Between a Subpoena, a Search Warrant and a Court Order Under the ECPA?*, TRANSPARENCY REPORT, https://www.google.com/transparencyreport/userdatarequests/legalprocess/#whats_the_difference (last visited Dec. 1, 2016) (noting that for a court order, the government agency must present "specific facts . . . demonstrating that the requested information is relevant and material to an ongoing investigation," whereas a warrant requires a demonstration of probable cause to believe that "certain information related to a crime is presently in the specific place to be searched").

[120] *Id.*; *see generally supra* note 76.

[121] Riley v. California, 134 S. Ct. 2473, 2485 (2014).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

A. New Exceptions to the Warrant Requirement

Since protecting citizens' technological privacy rights would be the impetus for a bill such as the one proposed herein, the rights of certain "target" individuals must be addressed as well.

There are circumstances in which obtaining a warrant could endanger more lives than it protects. Similar to the exceptions currently carved out in the general warrant requirement, "Emergency Situations" should be included as an exception. Speedy and effective search techniques are necessary to protect the best interests of society. Currently, however, many in-the-field search techniques simply use eyesight. Groups of people search through the woods in grid-like patterns to search for missing people; helicopters search for the destructive trail of an avalanche to locate endangered individuals; and state officials rely on eye-witness reports to find abducted children. These are instances where an exception to the warrant requirement would be reasonable and highly beneficial.

To meet the standard for an Emergency Situation, a human life should be in immediate peril—similar to the exigent circumstances exception to the general warrant requirement.[122] This includes kidnappings, avalanches, missing person searches, etc. These situations *may* involve an element of criminal activity, but society's main focus should be on saving a life. If, for example, a skier were caught in an avalanche, a helicopter with a cell site simulator could fly above and, ideally, find the missing person without taking the time to obtain a warrant. Similarly, if an individual were abducted but certain information was known, such as whether they had their phone with them and the area from which they were taken, authorities could more easily search for that individual and potentially find more missing persons within the critical time period following abduction. Both of these examples contain an element of *immediacy* that should not be glossed over. These situations are ones where data would not be collected for the primary purpose of prosecution, but, rather, to save a specific, identified individual's life.

When determining whether the warrantless use of a cell site simulator comports with the proposed exception, the focus should be on the goal of the search; are we looking for evidence to support an arrest, or for a citizen whose life is in immediate peril? If the answer echoes the latter, it is likely that the proposed exception has been met.

[122] *See supra* Part II(B)(2) (discussing the exceptions to the warrant requirement).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

Further, to qualify for a warrant at all, the crime suspected should be a felony, not a misdemeanor, and a warrant should only be issued for those crimes that are occurring or have already occurred. Allowing the issuance of a warrant in instances where there is a *possibility* that a misdemeanor *may* be committed in the future[123] is far too broad for such an invasive device.

To illustrate, it is important to note that misdemeanors are more serious than infractions, but less serious than felonies,[124] and are usually punishable with up to a year in jail.[125] Examples of misdemeanors in many states include disorderly conduct, driving under the influence, and minor assault.[126] The idea that one could be punished for "intent to drive under the influence" because they texted to their friend, "I'd rather drive drunk than take a cab" is an absurd one. However, this could be interpreted as an example of intent to commit a misdemeanor. It seems ludicrous to think that pursuing this "criminal activity" would be considered a reasonable use of official resources, let alone a constitutionally sound practice for investigating something that may be entirely void of any real intent to violate the law. However, the drafted legislation in many states would allow action such as this. By allowing *potential future* misdemeanors to satisfy the probable cause requirement, use of cell site simulators would be so broad that authorities could effectively use them *whenever they want*.

There are also certain instances where crimes are so widespread that the scope of the search required to apprehend suspects far exceeds the limitations on the geographical scope of permitted use. These situations may include crimes between states, where legislation concerning the use of cell site simulators varies and complicates investigative practices. Thus, in certain situations, the legislation should allow for increased geographical searches. This exception should relate to "Large Scale Mass Crime & Inter-State Criminal Organizations or Activities." To qualify for a warrant in this category, the enforcement agency must have *reasonable articulable suspicion*,[127] rather than the higher standard of probable cause, that the

[123] *See, e.g.*, H.B. 904, 2016 Reg. Sess. (Md. 2016) (noting that a court may issue an order when there is probable cause to believe that a "misdemeanor or felony has been, is being, or will be committed by the owner or user of the . . . device").

[124] *See* Pope v. State, 396 A.2d 1054, 1076 (Md. 1979).

[125] *See What Distinguishes a Misdemeanor From a Felony*, FINDLAW, http://criminal.findlaw.com/criminal-law-basics/what-distinguishes-a-misdemeanor-from-a-felony.html (last visited Dec. 20, 2016).

[126] *See* Eisha Jain, *Arrests as Regulation*, 67 STAN. L. REV. 809, 818–19 (2015).

[127] *Reasonable articulable suspicion* means that the officer "must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant the

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

suspect is actually a member of a group that commits large scale, inter-state crimes. These crimes may include, among others, human trafficking, drug trafficking, and black market sales. In these situations, the impact of the criminality should be so objectively offensive as to necessitate special investigative techniques that may not usually be accepted by the public.

In these instances, it seems logical to enforce additional warrant requirements so that sweeping searches are not conducted for the purpose of identifying previously unknown criminal groups. These requirements may include knowledge of the nature and size of the organization or activity, approximately how many victims there are or the suspected rate at which victims are being injured, supported with the reasons for suspecting such a rate, the duration of the criminal activity, and the number of states (or countries) that the activity or organization has infected. By allowing for cell site simulator use in these situations, the protections against overbroad uses are still enforced,[128] while allowing use in situations that necessitate broader searches.

B. Legislating the Use of Collected Information

It is important to codify not only how one may be granted use of a cell site simulator, but also what can be done with the information after it is collected. The DOJ regulations call for daily deletion of non-target data.[129] However, some states have broadened this regulation and propose more lenient rules.[130]

By mandating the deletion of all gathered information that does not relate *directly* to the investigation, not only would the government protect itself from unduly infringing upon privacy rights, but it would also ensure that any ancillary information collected from the target phone would be deleted. This requirement

---

intrusion" without a warrant. *See* Terry v. Ohio, 392 U.S. 1, 21–22 (1968). Termed a "Terry Stop," reasonable articulable suspicion allows for brief detention of persons on reasonable suspicion of involvement in criminal activity, but short of probable cause to arrest. Similar to a "Terry Stop," some additional, articulable evidence must be present to support the claim that the target individual is a member of the widespread organization covered under this exception.

[128] *See supra* Part III(A) (the suggestions for the new warrant requirements will help to protect against overbroad use of cell site simulators).

[129] *See* U.S. Dep't of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, https://www.justice.gov/opa/file/767321/download (last visited Oct. 20, 2016).

[130] *See, e.g.*, H.B. 904, 2016 Leg., Reg. Sess. (Md. 2016) (delineating that deletion should occur immediately after collection, but no less than once every forty-eight hours); H.B. 3165, 84th Leg., Reg. Sess. (Tex. 2015) (listing no regulations pertaining to the deletion of non-target information).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

could potentially limit irrelevant biases against the target, which could lead to tunnel vision and wrongful convictions.[131]

It is easy to think of an instance where a non-target's data could reveal unexpected criminal activity, or the potential for such. However, it is imperative that the legislation bar any and all use of this collected information. The point of obtaining a warrant is to ensure that the investigative techniques do not infringe an individual's reasonable expectation of privacy—this is why probable cause to believe specific individuals are or have committed a crime is necessary to obtain a warrant.[132] Subverting this requirement and using information gathered against non-targets should be a per se Fourth Amendment violation. If the requisite probable cause were present concerning the non-targets, they would have been listed in the warrant. Any use of collected non-target data violates the warrant requirement,[133] and should not be allowed in any circumstance.

In some cases, even where the requisite probable cause is present, searches will turn up fruitless. A provision calling for the permanent deletion of *all* collected data against the target individual after a certain period of dormancy should be included. Data deletion should occur within 180 days if the investigation was not furthered by the data or if there is no longer probable cause against the individual. This way, any evidence obtained in a fruitless search cannot be held until a time when it may become relevant.

General requirements for a warrant should include (i) reasonable certainty of the general location (within 5 miles) of the suspected cellular device,[134] (ii) the name

---

[131] Tunnel vision is a "natural human tendency that has . . . pernicious effects . . . that lead actors in the criminal justice system to focus on a suspect, select and filter the evidence that will build a case for conviction, while ignoring or suppressing evidence that points away from guilt." Keith A. Findley & Michael S. Scott, *The Multiple Dimension of Tunnel Vision in Criminal Cases*, 2006 WIS. L. REV. 291, 292 (2006) (internal quotation marks omitted).

[132] *See supra* Part II.

[133] *See supra* Part II(B).

[134] *See, e.g.*, WASH. REV. CODE § 9.73.270(4)(c)(ii) (2015) (requiring, among other things, "the physical location [if known] of the device"); H.B. 138, 2015 Leg., Reg. Sess. (La. 2015) (requiring the location "if known" of the device); H.B. 904, 2016 Leg., Reg. Sess. (Md. 2016) (requiring the physical location, if known, of the device); H.B. 2214, 98th Gen. Assemb., 2d. Reg. Sess. (Mo. 2016) (requiring the location of the device, *or other information* for a warrant to be issued); A.B. 8055, 238th Gen. Assemb., Ann. Legis. Sess. (N.Y. 2015) (requiring the location only "to the extent known"); H.B. 3165, 84th Leg., Reg. Sess. (Tex. 2015) (requiring the applying officer to "state the judicial district in which the telephone or device is reasonably expected to be located").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

or cellular carrier identification number,[135] (iii) the crime suspected, (iv) the relevance of the information sought, (v) the likelihood and potential amount of non-target data that may be collected, (vi) the geographic area that will be covered by the search, and (vii) the type of device to be searched.

V. CONCLUSION

Congress and the Supreme Court have previously held that state invasions into personal communications require heightened protection.[136] This protection usually comes in the form of a warrant, which ensures that there is probable cause before allowing a search or seizure of anything in which citizens have a reasonable expectation of privacy.[137]

By examining Supreme Court Fourth Amendment jurisprudence[138] in conjunction with the advantages and disadvantages of using cell site simulators,[139] a common theme has remained: all good things come at a cost. The main question the Supreme Court must answer when faced with a case involving cell site simulator use is the same question Congress will have to face when drafting federal legislation: is society willing to accept this kind of search as reasonable?

Every individual's data could be accessed and recorded at any moment without their knowledge. With the proper legislative and procedural safeguards, this may not be as daunting as it sounds. If all non-target information is disposed of within twenty-

---

[135] *See, e.g.*, WASH. REV. CODE § 9.73.270(4)(c)(ii) (2015) (requiring the "telephone number or other unique subscriber account number"); H.B. 138, 2015 Leg., Reg. Sess. (La. 2015) (requiring a "telephone or other unique subscriber number" for the target device); H.B. 904, 2016 Leg., Reg. Sess. (Md. 2016) (requiring the unique subscriber account number for the target device); H.B. 2214, 98th Gen. Assemb., 2d Reg. Sess. (Mo. 2016) (requiring the "telephone number or other unique subscriber account number"); A.B. 8055, 238th General Assemb., Ann. Legis. Sess. (N.Y. 2015) (requiring a "telephone or other unique subscriber number" of the target device); H.B. 3165, 84th Leg., Reg. Sess. (Tex. 2015) (requiring the identification of the "cellular telephone or other wireless communications device to be monitored").

[136] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801(a), 82 Stat. 197, 211 (codified as amended at 18 U.S.C. § 2510 (2010)) ("The Congress makes the following findings: There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, Mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. . . . To safeguard the privacy of innocent persons, the interception of wire or oral communications . . . should be allowed only when authorized by a court with assurances that the interception is justified and that the information obtained thereby will not be misused.").

[137] *See supra* Part II (discussing the reasonable expectation of privacy and how it has developed through Supreme Court precedent).

[138] *Id.*

[139] The main advantage to be kept in mind is that the use of cell site simulators can save human lives in immediate peril.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu

four hours, including data, photos, and stored documents, and if warrants are necessary before using cell site simulators for criminal investigations, perhaps people may be more comfortable allowing state officials to use such an invasive tool to protect society.

When drafting the necessary federal legislation enumerating when, how, and by whom a cell site simulator may be used, the main things to keep in mind are not only that these devices can be used to collect personal information from an unquantifiable number of citizens without their knowledge or consent, but also that they can be used to save human lives. The use of cell site simulators to secretly and seamlessly collect mass information from an indeterminable number of citizens at one time is an invasion of personal privacy that has yet to be federally recognized or codified as such. Finding the legislative balance between protecting the right to privacy and the need for efficient law enforcement investigations is a difficult-but-necessary task that Congress must address.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2017.470
http://lawreview.law.pitt.edu