Washington University Law Review

Volume 95 | Issue 2

2017

How Lambis and CSLI Litigation Mandate Warrants for Cell-Site Simulator Usage in New York

Cindy D. Ham
Washington University School of Law

Follow this and additional works at: https://openscholarship.wustl.edu/law_lawreview

 Part of the Criminal Law Commons, Criminal Procedure Commons, and the Science and Technology Law Commons

Recommended Citation

Cindy D. Ham, *How Lambis and CSLI Litigation Mandate Warrants for Cell-Site Simulator Usage in New York*, 95 WASH. U. L. REV. 507 (2017).
Available at: https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

This Note is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Washington University Law Review by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.

HOW *LAMBIS* AND CSLI LITIGATION MANDATE WARRANTS FOR CELL-SITE SIMULATOR USAGE IN NEW YORK

INTRODUCTION

Over the years, various federal, state, and local law enforcement agencies have enjoyed the growth and development of technology in aiding their efforts to combat crime. Until recently, not much information had been available regarding the use, or existence, of cell-site simulators. Cell-site simulators have been around for at least fifteen years,[1] and they operate by mimicking cell phone towers.[2] Known also by their popular brand name, Stingray, cell-site simulators have the capability to extract information such as location and call records by tricking a nearby cell phone to connect to them instead of cell towers.[3]

Perhaps as a result of the petitions of various civil liberty groups and privacy advocates, the Department of Justice (DOJ) and the Department of Homeland Security (DHS) issued guidance policies on their use of cell-site simulators. These policies generally require a warrant to be obtained if probable cause exists, unless the circumstances are exigent or exceptional.[4] On the state level, however, the extent of available information and issued guidance varies widely. California's Electronic Communications Privacy Act requires a warrant before state law enforcement can obtain data through cell-site simulators and other means,[5] while the New York Police Department (NYPD) has been sued by the New York Civil Liberties Union (NYCLU) after it refused to reveal information on its use of cell-site simulators.[6]

As cell phones continue to play a larger and vital role in the everyday lives of Americans, it is troubling that enforcement agencies possess an unhindered ability to gather personal—and mostly irrelevant—information

1. Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, THE INTERCEPT (Sept. 12, 2016, 1:33 PM), https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

2. *Id.*

3. *Id.*

4. DEP'T OF HOMELAND SEC., POLICY DIRECTIVE 047-02 (2015), https://oversight.house.gov/wp-content/uploads/2015/10/15-3959-S2-DHS-Signed-Policy-Directive-047-02-Use-of-Cell-Site-Simulator-Tech.pdf; DEP'T OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download.

5. CAL. PENAL CODE § 1546.1 (West 2016); *see infra* Section V.a.

6. New York Civil Liberties Union v. N.Y.P.D., Docket No. 100788/2016 (N.Y. Sup. Ct. May 19, 2016).

Washington University Open Scholarship

from anyone within the range of cell-site simulators without a warrant. This Note will focus on how cell-site simulators have been used in New York, and how New York's state and local law enforcement agencies must take note of *United States v. Lambis*[7] and appropriately modify or create (as it is unknown whether they even have such policy)[8] their policies to require warrants.

Part II of this Note will discuss the available information on cell-site simulators with specific regard to use in New York. Part III will discuss legal precedent regarding cell-site simulators and cell site location information (CSLI), comparing the two types of surveillance and analyzing why CSLI precedent points to the necessity of a warrant for cell-site simulators. Part IV will discuss *Lambis* in detail and its potential impact on cell-site simulators. Part V will discuss what a proposed legislative enactment on cell-site simulators should address and also discuss California's relevant statute briefly as an example. Lastly, Part VI will conclude this Note by discussing past and current efforts to require warrants for cell-site simulator use, why law enforcement officials should modify their policy to require warrants, and how state legislatures could, alternatively, take anticipatory action and modify statutes to require warrants for such devices.

I. THE FRIGHTENING CAPABILITY OF CELL-SITE SIMULATORS TO OBTAIN VARIOUS INFORMATION FROM CELL PHONES WITHIN THEIR RANGE

Much of the information available on cell-site simulators stems from federal agencies and their disclosures. Based on available information,[9] it appears that the state and local use of such simulators are similar.[10] According to the Department of Justice, cell-site simulators force cell phones, within a certain range, to connect to them rather than the cell towers, and cause the phones to give up the phone and electronic serial numbers that are assigned by the manufacturers.[11] The DOJ emphasized in its policy that data obtained through cell-site simulators are similar to those from pen

7. 197 F. Supp. 3d 606 (S.D.N.Y. 2016).

8. *Stingrays*, NEW YORK CIVIL LIBERTIES UNION, http://www.nyclu.org/stingrays (last visited Jan. 15, 2017).

9. *See infra* Section II.a. (discussing efforts by federal agencies to mandate that state and local agencies remain in total secrecy regarding their use of cell-site simulators).

10. *See generally* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 142 (2013).

11. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS (June 2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

registers,[12] in that they only provide records such as phone numbers and call logs, and do not disclose emails, texts, the user's name, or the address.[13] However, state and local law enforcement agencies, especially those in New York, have refused to release in detail what type of information they collect, what they retain, and what is ultimately destroyed.[14]

The DOJ's policy only covers federal agencies and fails to provide insight on how the devices are used on the state and local level,[15] where the simulators are used extensively and where the devices are often borrowed from the federal agencies.[16] Given that cell-site simulators have the full capacity to obtain a phone's location history, track its location through GPS, and also obtain contents of calls, texts, and history of visited websites,[17] the lack of transparency by state and local agencies is deeply concerning.

A. Usage of Cell-Site Simulators in New York

Prior to discussing how the cell-site simulators have been used in New York, it must be noted that these devices are not cheap. As of May 2015, the New York state police had spent over $640,000 on cell-site simulators.[18] Some portions of that amount were spent on upgrading the devices, including the purchase of an amplifier that could augment their surveillance capabilities.[19]

While spending inordinate amounts of money purchasing and upgrading the cell-site simulators, when confronted with a Freedom of Information Law request, the New York State Police responded that it did not have any

12. A pen register is "[a]n 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." *Pen Register*, BLACK'S LAW DICTIONARY (10th ed. 2014).

13. DEP'T OF JUSTICE, *supra* note 4. DHS's policy also contains very similar language. DEP'T OF HOMELAND SEC., *supra* note 4.

14. *See, e.g.*, NYCLU, *supra* note 8 (discussing how Rochester Police Department's policy in New York suggests that it "keeps the records they intentionally acquired through Stingray use for a minimum of ten years," although they do "destroy or seal the material they acquire inadvertently").

15. The DHS's policy does include a section on "State and Local Partners," but its vague language does not appear to be binding on state and local enforcement agencies, especially since it is unclear which circumstances qualify. "This policy applies to all instances in which [DHS] use[s] cell-site simulators in support of other federal agencies and/or state and local law enforcement agencies." DEP'T OF HOMELAND SEC., *supra* note 4.

16. Kim Zetter, *New Bill Would Force Cops to Get Stingray Warrants*, WIRED (Nov. 3, 2015, 3:27 PM), https://www.wired.com/2015/11/new-bill-would-force-cops-to-get-warrants-before-spying-with-stingrays/.

17. Pell & Soghoian, *supra* note 10, at 144–46.

18. NYCLU, *supra* note 8.

19. *Id.*

Washington University Open Scholarship

records on numbers of investigations during which the equipment was used or any applications to court to request the use of cell-site simulators.[20] However, there is evidence of the FBI working with state and local police departments to maintain secrecy on use of the devices, subjecting the departments to nondisclosure agreements.[21] Notably, the Erie County Sheriff's Office entered into a confidentiality agreement with the FBI.[22] This agreement required the Sheriff's Office to maintain total secrecy about the use of cell-site simulators, including in court filings and when responding to court orders, absent explicit written consent by the FBI.[23] Furthermore, the Office was required to pursue dismissal of a criminal prosecution rather than compromising the disclosure of any information concerning the devices and their use.[24]

The usage of cell-site simulators is not uncommon. The NYPD used the devices in over 1,000 cases between 2008 and 2015, and the seriousness of the alleged crimes ranges from homicide to identity theft.[25] New York state and local police continue to use cell-site simulators and spend significant amounts of money to maintain them, without being subject to any constraints or regulations. They continue to use these devices while refusing to disclose any information.[26] Thus, it is unsurprising that privacy advocates have probed the practice with increased scrutiny in recent years.[27]

B. Efforts by the New York Civil Liberties Union and Legislative Attempts to Require Warrants Have Been Unsuccessful

In 2015, two bills were introduced to the New York legislature to require either a court order or a warrant before utilizing cell-site simulators. S04914, a bill introduced in the New York Senate in 2015, sought to include "mobile phone surveillance systems" within the New York pen register statute that

20. *Id.*

21. STAFF OF H.R. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., REP. ON LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHS: PRIVACY CONCERNS AND RECOMMENDATIONS 3, 31–32 (2016).

22. NYCLU, *supra* note 8.

23. *Id.*

24. *Id.*

25. Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. TIMES (Feb. 11, 2016), http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=0.

26. *See, e.g.*, *NYCLU and Activists File Lawsuit After NYPD Refuses to Respond to Records Requests About Anti-Protest Activities*, NYCLU (May 23, 2017), https://www.nyclu.org/en/press-releases/nyclu-and-activists-file-lawsuit-after-nypd-refuses-respond-records-requests-about.

27. *See, e.g.*, NYCLU, *supra* note 8.

granted the court to issue orders.[28] Another bill proposed including cell-site simulators specifically in the eavesdropping statute, which would require a warrant before use.[29] Neither bill proceeded beyond being sent to a committee for approval.[30]

In 2016, a number of bills were introduced that would require warrants for cell-site simulators unless the agency had the explicit permission of the owner or authorized user of the electronic device.[31] Named the New York Electronic Communications Privacy Act, it advanced past the codes committee and was sent to the rules committee for approval in June 2016, but it did not proceed beyond that.[32] It is unclear why the bills have not garnered enough support to continue through the process and eventually become law, especially given that the bills gained support from prominent companies and organizations such as Google and The Legal Aid Society.[33]

In March 2017, two members of the New York City Council introduced the Public Oversight of Surveillance Act (POST Act) that would require the NYPD to disclose basic information on the surveillance tools they use, including cell-site simulators.[34] Specifically, it would require the NYPD to "issue a surveillance impact and use policy about these technologies," which will be open for comments and the final version will be provided to the Council, the Mayor, and be posted on the NYPD's website.[35] After a committee hearing held on June 14, 2017, the bill was "laid over,"[36] indicating that no votes or further actions were taken.[37] Since Mayor Bill De Blasio has publicly opposed it, this means that the bill must gain the

28. S. 4914, 2015–16 Leg. (N.Y. 2015).

29. A.B. 8055, 2015–16 Leg. (N.Y. 2015).

30. *Senate Bill S4914A*, THE NEW YORK SENATE, https://www.nysenate.gov/legislation/bills/2015/S4914/amendment/A (last visited Feb. 13, 2017); *Assembly Bill A8055*, THE NEW YORK SENATE, https://www.nysenate.gov/legislation/bills/2015/A8055 (last visited Feb. 13, 2017).

31. Mike Maharrey, *NY Electronic Communications Privacy Act Passed*, ACTIVIST POST (June 17, 2016), http://www.activistpost.com/2016/06/ny-electronic-communications-privacy-act-passed.html.

32. *Id.*

33. *Protect Your Privacy: Help Pass the New York State Electronic Communications Privacy Act*, NYCLU, http://www.nyclu.org/ecpa. (last visited Jan. 15, 2017).

34. Int. No. 1482, 2017–18 Leg. (N.Y. 2017).

35. *Summary of Int. 1482*, THE NEW YORK CITY COUNCIL (2017), http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=2972217&GUID=0D8289B8-5F08-4E6F-A0D1-2120EF7A0DCA&Options=ID%7C&Search=.

36. *Meeting Minutes*, THE NEW YORK CITY COUNCIL (June. 14, 2017, 10:00 AM), http://legistar.council.nyc.gov/View.ashx?M=M&ID=547508&GUID=B95086F9-B596-40F1-A752-3C5E427577B1.

37. *Featured Legislation: Task Force on Police Body Cameras*, NYC COUNCILMATIC, https://nyc.councilmatic.org.

Washington University Open Scholarship

support of at least two-thirds of the Council, or 34 votes, to override his veto, if the vote ever occurs.[38]

II. HOW THE UNRESTRICTED USAGE OF CELL-SITE SIMULATORS VIOLATES FOURTH AMENDMENT RIGHTS

Traditionally, legal issues concerning privacy have been scrutinized under well-established tests such as the reasonable expectation of privacy under *Katz v. United States*[39] and the mosaic theory as implied in *United States v. Jones*[40] and *Riley v. California*.[41] However, this Note will evaluate and discuss cell-site simulators through the lens of CSLI[42] litigation and the *Lambis* decision;[43] the latter of which held that using cell-site simulators requires a warrant. Additionally, the Note will incorporate established Fourth Amendment frameworks in analyzing the various litigation.[44] The *Lambis* decision, even though it was adjudicated in federal court, is important here because it establishes proper legal context to evaluate cell-site simulator use and why it requires a warrant, as apposite cases at the state level are practically nonexistent most likely due to the nondisclosure agreements.[45]

A. Comparing CSLI and Cell-Site Simulators

Cell-site simulators are best analyzed under the existing legal precedent

38. Ali Winston, *NYPD Attempts to Block Surveillance Transparency Law with Misinformation*, THE INTERCEPT (July 7, 2017, 10:59 AM), https://theintercept.com/2017/07/07/nypd-surveillance-post-act-lies-misinformation-transparency/; *What is New York City Council, and How Does It Work?*, NYC COUNCILMATIC, https://nyc.councilmatic.org/about/.

39. 389 U.S. 347, 350–51 (1967).

40. 565 U.S. 400, 430–31 (2012).

41. 134 S. Ct. 2473, 2489 n.1 (2014).

42. CSLI indicates which cell tower the phone's antenna connects to so that it can access the cellular network. *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 9–10 (2013) (statement of Mark Eckenwiler, Senior Counsel, Perkins Coie LLP). If the user moves from one coverage area of a tower to another, the call could be "seamlessly 'handed off'" to one or more towers in sequence. *Id.* Depending on whether the phone was connected to a cell tower in an urban, suburban, or rural network, the coverage area of the tower varies, affecting how precisely the phone's location could be traced. *Id.*

43. United States v. Lambis, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016).

44. For a traditional Fourth Amendment analysis of cell-site simulators, see generally W. Scott Kim, *The Fourth Amendment Implications on the Real-Time Tracking of Cell Phones Through the Use of "Stingrays,"* 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 995 (2016).

45. *See supra* Section II.a. (discussing efforts by federal agencies to mandate that state and local agencies remain in total secrecy regarding their use of cell-site simulators).

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

through CSLI litigation. This is primarily because not many lawsuits exist that specifically address the simulators. Additionally, the similarities and differences between the two facilitate the discussion on how the current trend of *not* requiring warrants for CSLIs bolsters the argument that cell-site simulators *do* require warrants.

Before analyzing legal precedent, it is worthwhile to compare the two types of data collection. Both CSLI and information collected from cell-site simulators take advantage of the ubiquitous nature of cell phones to assist law enforcement efforts and both have presented legal issues recently.[46] Both have been used by federal, state, and local law enforcement agencies[47] to obtain information on a suspect of a crime, such as location history, using the suspect's cell phone. However, this is where the similarities end.

The differences are stark in contrast. To obtain CSLI, the government requires the assistance of the suspect's cell phone service provider, such as Verizon, to provide the information.[48] Cell-site simulators, however, are devices that are purchased directly by the law enforcement agencies and function by extracting information directly from cell phones that connect to

46. The issue with warrants and CSLI surfaced in August 2005 when a New York Magistrate Judge publicly denied the government's request for such information due to lack of proof of probable cause. *Cell Tracking*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cell-tracking (last visited Jan. 16, 2017). Although the first case that dealt with a primitive version of a cell-site simulator was in 1995, the technology became more well-known because of *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012). In that case, the defendant was convicted based on evidence that was later revealed to have been acquired by a cell-site simulator. *Have There Been Any Major Court Decisions About Cell-Site Simulators?*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/sls/tech/cell-site-simulators/faq#faq-Have-there-been-any-major-court-decisions-about-cell-site-simulators?- (last visited Jan. 16, 2017). The government did not disclose how it obtained information to prosecute Rigmaiden. For more information on how Rigmaiden uncovered the government's cell-site simulator usage, see Cale Guthrie Weissman, *How an Obsessive Recluse Blew the Lid Off the Secret Technology Authorities Use to Spy on People's Cellphones*, BUSINESS INSIDER (Jun. 19, 2015, 5:04 PM), http://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6.

47. For information on how various federal, state, and local agencies have used CSLI to assist their law enforcement efforts, see generally Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, THE ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ (noting that in 2014, AT&T received over 64,000 requests for CSLI, and Verizon received more than 21,000 requests for CSLI in the first six months of 2015).

48. *Cell Phone Location Tracking Laws by State*, ACLU, https://www.aclu.org/map/cell-phone-location-tracking-laws-state?iframe=1 (last visited Jan. 15, 2017). Note that because the nature of CSLI involves a service provider as a "third party," four circuit courts have held that a warrant is not required to obtain CSLI due to the third-party doctrine. *See* In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013), United States v. Carpenter, 819 F.3d 880, 887–89 (6th Cir. 2016), United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015), United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016). The third-party doctrine is further discussed *infra* Section III.b.

Washington University Open Scholarship

them, eliminating the need for service providers.[49] More importantly, CSLI requires the government to target a specific individual as the information provided by the servicers are limited in scope to that user's phone.[50] On the other hand, cell-site simulators collect information indiscriminately within a target range.[51] The simulators do not focus on a specific phone, but instead gather information by tricking all of the phones within an area to connect with them rather than the cell towers.[52]

Moreover, CSLI supplied by third-party service providers consists of a history of the phone's location.[53] In comparison, cell-site simulators are able to not only provide the location history, but can also pinpoint the location of the phone with enough accuracy for officials to locate the user.[54] This difference is especially significant because some state or local agencies, while obtaining a warrant for cell-site simulators, may mislead the court by making them appear to be pen registers[55] instead.[56] It has been found that at least one local law enforcement has used the state pen register statute to obtain court orders to use cell-site simulators.[57] Because the orders require

49. *See* Orin Kerr, *Applying the Fourth Amendment to Cell-Site Simulators*, THE WASHINGTON POST (Apr. 4, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/04/04/applying-the-fourth-amendment-to-cell-site-simulators/?utm_term=.c9655c776a44.

50. *See* State v. Earls, 70 A.3d 630, 637 (N.J. 2013) (quoting expert testimony that CSLI is one of two primary methods to track mobile devices).

51. NYCLU, *supra* note 8.

52. *Id.*

53. *See, e.g.*, United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (describing CSLI as "the records of the phone company that identify which cell towers it used to route Defendants' calls and messages"); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 141 (2012).

54. Kerr, *supra* note 49 (discussing how the officials in State v. Andrews, 134 A.3d 324, 326 (Md. Ct. Spec. App. 2016), were able to locate the defendant at his apartment using cell-site simulator).

55. *See* BLACK'S LAW DICTIONARY, *supra* note 12.

56. In *Andrews*, 134 A.3d at 324, the government obtained a pen register warrant and used a pen register to identify the defendant's cell phone number and later used a cell-site simulator to locate him. After holding that using a cell-site simulator constitutes a Fourth Amendment search, the Maryland Special Court of Appeals further held that the state pen register statute does not include the usage of cell-site simulators as "federal law specifies that the federal equivalent to the Maryland pen register statute does not authorize location information." *Id.* at 356. *See also* Jason Tashea, *Police Face Constitutional Challenges for Using Cellphone Tracking Devices to Locate Suspects*, ABA JOURNAL (July 1, 2016, 2:50 AM), http://www.abajournal.com/magazine/article/police_face_constitutional_challenges_for_using_cellphone_tracking_devices.

57. Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, THE BALTIMORE SUN (Apr. 9, 2015, 6:42 AM), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

a lower burden of proof than traditional warrants, and due to a lack of public knowledge on cell-site simulators, a defense attorney commented that the law enforcement agencies were basically "duping these judges into signing authorizations to use stingrays."[58] Pen register orders require a lower burden of proof than warrants because pen registers invade one's privacy on a much lower scale than CSLI or cell-site simulators: they only collect numbers dialed from a specific phone.[59]

B. Current Litigation on CSLI and Why the Cases Indicate that Cell-Site Simulator Usage Must Require Warrants

Federal and state courts have generally held that obtaining CSLI does not invoke Fourth Amendment protections, and thus warrants are not required. This, however, may change soon as the United States Supreme Court recently granted *certiorari* to review a Sixth Circuit case that held warrants are not required in order to obtain CSLI, scheduled for the October 2017 term.[60]

In *United States v. Carpenter*, the Sixth Circuit Court of Appeals held that the government did not conduct a Fourth Amendment search when it obtained CSLI because the information constituted business records.[61] The court also made three propositions that are particularly relevant in contrasting CSLI against cell-site simulators: 1) CSLI cannot be evaluated under *Jones*, where the court said in dicta that "GPS monitoring in government investigations of most offenses impinges on expectations of privacy," because CSLI could not provide an accurate location;[62] 2) a reasonable expectation of privacy under *Katz* could not be found here because the CSLI records were held by a third party—the mobile service provider—as business records; and 3) the third-party doctrine under *Miller*[63]

58. *Id.*

59. *See infra* Section III.c. (detailed discussion on pen registers and its comparison with cell-site simulators).

60. *See* Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 2017 WL 2407484 (U.S. June 5, 2017) (No. 16-402). *See also* Amy Howe, *Justices to Tackle Cellphone Data Next Term*, SCOTUSBLOG (June 5, 2017, 12:52 PM), http://www.scotusblog.com/2017/06/justices-tackle-cellphone-data-case-next-term/ (discussing how the Justices' views on business records may have changed because these types of data are stored on cellphones, which "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Riley v. California, 134 S. Ct. 2473, 2484 (2014).

61. *Carpenter*, 819 F.3d at 887–90.

62. *Carpenter*, 819 F.3d at 888 (quoting United States v. Jones, 565 U.S. 400, 430 (2012)).

63. United States v. Miller, 425 U.S. 435, 443 (1976). The Supreme Court in *Miller* held that a reasonable expectation of privacy did not exist for bank records because they were held by the bank as

Washington University Open Scholarship

applied for CSLI.[64]

The first rationale behind the *Carpenter* decision was that CSLI could not be evaluated under *Jones* because CSLI could not pinpoint the exact location of the user.[65] This relates to the most evident difference between CSLI and information obtained by cell-site simulators: cell-site simulators have the capability of not only extracting the location history of a cell phone, but can also locate the phone in real time using GPS.[66] Under this rationale, using cell-site simulators would absolutely violate Fourth Amendment rights because they have the capability to direct law enforcement officials to a precise location.[67] This concern was articulated in *Carpenter*, which stated that accurate GPS tracking "might tell a story of trips to 'the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on'" because it could pinpoint an individual's location to a specific building.[68]

The second rationale in *Carpenter* was that the user could not have a reasonable expectation of privacy because CSLI qualified as business records held by a third party.[69] The business records defense cannot hold true for cell-site simulators because using the simulators eliminates the need for obtaining a set of records from the service provider. This difference also points to why the third-party doctrine,[70] which served as the last rationale of the *Carpenter* decision, does not apply to cell-site simulators. By using the devices, the law enforcement agencies cut out the "third party" and acquire information directly.[71] Additionally, courts have ruled that customers do not actively share location information—or any other

business records, and the government was able to obtain the records through a third party rather than directly from the defendant. *Id.*

64. *Id.* at 888–89.

65. *Carpenter*, 819 F.3d at 888 (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (discussing its commentary against GPS monitoring)).

66. Kerr, *supra* note 54 (discussing how the officials in State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016), could locate the defendant at his apartment using a cell-site simulator).

67. *Compare Carpenter*, 819 F.3d at 889 (classifying location history as a business record and contrasting it with GPS information, which can locate a target within fifty feet of accuracy), *with Jones*, 565 U.S. at 414–16 (2012) (Sotomayor, J., concurring) (discussing GPS monitoring and its impingement on reasonable expectations of privacy if information not obtained lawfully).

68. *Carpenter*, 819 F.3d at 889 (quoting Justice Sotomayor's concurring opinion in *Jones*, 565 U.S. at 415).

69. *Carpenter*, 819 F.3d at 887.

70. *See also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979). The Supreme Court held in *Smith* that installation and use of a pen register does not constitute a Fourth Amendment search. *Id.* at 745–46. This was one of first cases to apply the third-party doctrine, which states that there is no valid expectation of privacy once the customer provides the information to a third party. *Id.* at 743–44.

71. *See generally supra* Section III.0.

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

information, for that matter—when they connect to a cell tower.[72]

The third-party doctrine was also the driving reason behind the Fourth Circuit's decision in *United States v. Graham*.[73] The court held that cell phone users do not have Fourth Amendment protections over their CSLI because the third-party doctrine still applies when the information is "'revealed' to a third party . . . 'on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'"[74] Yet the court hinted at the diminishing relevance of this doctrine.[75]

Nonetheless, the court in *Graham* specified that CSLI falls directly under the ambit of the third-party doctrine because, by connecting to a cell tower to utilize cell phone services, the users "convey" their location to their providers whenever they connect to the network.[76] Conversely, this rationale cannot be applied to cell-site simulator data because the connection between users and providers are interrupted by the device. Rather than conveying the information voluntarily, the users are tricked into connecting with the device, which then forces their phones to give up personal information.[77]

The defendants in *Graham* also unsuccessfully argued that CSLI deserves Fourth Amendment protections.[78] Defendants claimed that CSLI is analogous to the contents of letters and calls that are already protected by legal precedent.[79] However, the court disagreed, noting that CSLI is more similar to mailing addresses and phone numbers.[80] Comparison to content written on letters and information written in envelopes is a historical analogy used in the Fourth Amendment context,[81] and the *Graham* opinion divided such types of information into "content" and "non-content" respectively.[82] Information under "content" would include anything that

72. United States v. Lambis, 197 F. Supp. 3d 606, 615 (S.D.N.Y. 2016) (discussing State v. Andrews, 134 A.3d 324, 398 (Md. Ct. Spec. App. 2016) and In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005)).

73. 824 F.3d 421, 427–28 (4th Cir. 2016).

74. *Graham*, 824 F.3d at 425 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

75. "The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case." *Id.* at 425.

76. *Id.* at 429.

77. *See* Biddle, *supra* note 1.

78. *Graham*, 824 F.3d at 433–34.

79. *Id.*

80. *Id.*

81. *See* Ex parte Jackson, 96 U.S. 727, 733 (1877).

82. *Graham*, 824 F.3d at 433–34.

Washington University Open Scholarship

reveals information contained within communications, such as the letter itself. In *Katz*,[83] the Supreme Court held that the contents of phone calls are protected, and the Sixth Circuit held that the contents of e-mails are protected in *Warshak* under the same rationale.[84] The *Graham* court also noted that there are cases expressly withholding Fourth Amendment protection only from "non-content" information,[85] such as the mailing address found on the envelope,[86] phone numbers that were dialed,[87] and information in the "to" and "from" fields found in emails.[88]

Applying the same rationale, if CSLI is classified as "non-content" information because it "facilitate[s] personal communications rather than [representing] part of the content of the communications themselves,"[89] it would be difficult to argue that information obtained from cell-site simulators belongs in the same category. Although both types of information reveal location, cell-site simulators provide real-time location data, which the *Jones* concurrence described as impinging upon Fourth Amendment rights and reasonable expectations of privacy.[90] Additionally, as previously noted, cell-site simulators can also acquire contents of calls and texts,[91] which definitely reveal the actual contents of communication. Even if the law enforcement officials claim that cell-site simulators are only used to locate someone, that in and of itself already constitutes a Fourth Amendment search under *Jones*.[92]

III. WHY *UNITED STATES V. LAMBIS* MATTERS

While litigation regarding cell-site simulators has been scarce, likely due to federal agencies subjecting state and local law enforcement officials to nondisclosure agreements and directing them to settle cases to prevent exposure,[93] the Southern District Court of New York recently held that cell-

83. Katz v. United States, 389 U.S. 347, 353 (1967).
84. United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010).
85. *Graham*, 824 F.3d at 432.
86. *Ex Parte Jackson*, 96 U.S. at 733.
87. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
88. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008). *See also* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (noting that Fourth Amendment protections do not extend to phone numbers disclosed to phone companies and email addresses disclosed to internet service providers).
89. *Graham*, 824 F.3d at 433.
90. *Jones*, 565 U.S. at 430.
91. *See* Pell & Soghoian, at 144–46 n.10.
92. *See Jones*, 565 U.S. at 430. Since real-time location would be used, classifications of "content" and "non-content" would be irrelevant here.
93. *See* STAFF OF H.R. COMM. ON OVERSIGHT AND GOV'T REFORM, *supra* note 21. The FBI

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

site simulators require a warrant in an opinion providing a much-needed, detailed insight into a court's perspective on this issue.[94]

A. Introduction of the Case

In 2015, the Drug Enforcement Administration (DEA) sought a warrant for the usage of a pen register and CSLI to aid in investigating an international drug-trafficking organization.[95] After obtaining the warrant and using CSLI, the DEA agents were able to narrow the location of Lambis, the suspect, to a specific intersection in Manhattan, but CSLI was not precise enough to provide the exact building.[96] To pinpoint the suspect's location, the DEA agents used a cell-site simulator to locate the building with the strongest "ping," which is a signal that cell phones typically transmit when they connect to a cell tower.[97] The strength of the "pings" coming from the suspect's phone was calculated by the cell-site simulator that forced all phones within the area to connect to it.[98] Through this process, the DEA agents were able to locate the building where the target phone was; then, the technician walked the halls of the building, utilizing the cell-site simulator, until he located the apartment unit with the strongest signal.[99]

After locating the unit, the agents obtained consent from the suspect's father to enter, obtained consent from the suspect to search his bedroom, and acquired evidence that included drug paraphernalia.[100] Lambis filed a motion to suppress this evidence.[101]

---

stated that there has been a misunderstanding behind the purposes of nondisclosure agreements, as their intentions were "'to protect the disclosure of sensitive information regarding the tradecraft and capabilities of the device.'" Jemal Brinson, *Cell Site Simulators: How Law Enforcement Can Track You*, CHICAGO TRIBUNE (Feb. 18, 2016, 12:21 PM), http://www.chicagotribune.com/news/plus/ct-cellphone-tracking-devices-20160129-htmlstory.html. However, the FBI cannot limit information such as whether the device had been used to pursue an individual, as a criminal defendant would have a right to know. *Id.* Additionally, there now is no merit in claiming that disclosure of cell-site simulator use would compromise an agency's ability to carry out its efforts to combat criminals and terrorists, because the only likely countermeasure of interfering with such efforts would be by turning off their phones. *See* Biddle, *supra* note 1.

94. United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016).
95. *Id.* at 608.
96. *Id.* at 609.
97. *Id.*
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*

Washington University Open Scholarship

B. Analysis by the Court in Lambis

The district court began with a discussion on what constitutes a Fourth Amendment search, which will not be explored in depth here.[102] However, the court's rejection of the exceptions to Fourth Amendment protections is relevant and warrants discussion.

After concluding that the government's conduct did constitute a Fourth Amendment search, the court rejected both the attenuation doctrine and the third-party doctrine as valid exceptions to the warrantless search of Lambis's bedroom.[103] The attenuation doctrine deems evidence as admissible if the connection between the unconstitutional police conduct and the evidence is "remote or has been interrupted by some intervening circumstance."[104] The government argued that, because they were able to obtain consent from Lambis's father and Lambis himself to search the apartment, the doctrine is applicable and thus evidence should not be suppressed.[105]

The attenuation doctrine is not particularly instructive on cell-site simulator use and will not be discussed further. The *Lambis* decision ultimately concluded that searches resulting from information obtained by such devices will not produce admissible evidence simply because the person eventually consents to a physical search.[106]

The court also struck down the third-party doctrine as a valid exception. The relevance of this doctrine has been decreasing in the ever-changing world of technology. In modern times, it is "nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life."[107] In *Jones*, Justice Sotomayor expressed the decreasing relevance of the third-party doctrine as

102. *Id.* at 609–10. Broadly, the court used Kyllo v. United States, 533 U.S. 27 (2001), to discuss reasonable expectations of privacy and how the home especially deserves Fourth Amendment protections because of the right of a person to retreat into his or her own home and be free from unreasonable governmental intrusion. *Lambis*, 197 F. Supp. 3d, at 609–10. *Kyllo* held a Fourth Amendment search had occurred when the government used a thermal imaging device to detect infrared radiation that was emanating from a home. *Id.* The main reason behind this holding was that the government used a device that was "not in general public use to explore details of the home that would previously have been unknowable without physical intrusion." *Id.* (quoting *Kyllo,* 533 U.S. at 40). Analogous to *Kyllo*, the government here was able to obtain information that could not have been obtained by the general public. *Lambis*, 197 F. Supp. 3d, at 609–10.

103. *Id.* at 612–16.

104. *Id.* at 612 (quoting Utah v. Strieff, 136 S. Ct. 2056, 2061 (2016)).

105. *Id.*

106. *Id.* at 613–14.

107. United States v. Davis, 785 F.3d 498, 525 (11th Cir. 2015) (Rosenbaum, J., concurring), *cert. denied*, 136 S. Ct. 479 (2015).

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

it is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[108] Notably, this doctrine has been used by courts in generally allowing for warrantless searches to obtain pen register information and CSLI.[109]

Unlike CSLI, the government cannot assert the third-party doctrine as an exception to the Fourth Amendment in order to use cell-site simulators. Pen registers record phone numbers that are dialed by the customer, and the information is essentially initiated by the user because he or she "voluntarily" gives it up each time to make a phone call. However, courts have held that users do not voluntarily give up information concerning their phones simply by turning the devices on and having them connect to a cell tower.[110] These "pings" are automatically sent by the phone once it is powered on, and the user plays no active role in this process.[111] Instead, the cell tower, or the cell-site simulator, forces the phones to connect with it to provide network support.[112] In the case of cell-site simulators, agencies are able to locate and pinpoint a targeted phone by forcing the phone to connect to the simulators, having the phone repeatedly transmit its identifying number, and then calculating the strength of the "ping" until the phone's location is found.[113]

Whether CSLI is voluntarily given is a contested topic, but the fact that pen registers and CSLI require a third party is not.[114] The crux of the third-party doctrine is that once a customer provides information *voluntarily* to a third party, he or she cannot be said to hold a reasonable expectation of

108. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

109. *Lambis*, 197 F. Supp. 3d at 613–16. Whether the third-party doctrine should be struck down in its entirety, with particular regard to CSLI, is beyond the scope of this Note and will not be discussed in detail. But it is important to emphasize the disparity between technology that existed at the time when the third-party doctrine emerged and now. *See generally* Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (discussing pen registers, which recorded all the numbers dialed from a telephone); United States v. Miller, 425 U.S. 435, 443–44 (1976) (no reasonable expectation of privacy exists for bank account holders in their bank records since they are business records).

110. *See Lambis*, 197 F. Supp. 3d at 615 (discussing a line of cases: In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."); Tracey v. State, 152 So. 3d 504 (Fla. 2014); State v. Earls, 70 A.3d 630, 641 (N.J. 2013)). Although other courts have ruled that CSLI does fall outside of Fourth Amendment protections because of the third-party doctrine, the stronger rationale behind such ruling is that CSLI involves a third party, beyond the issue of whether a user actively provides information to a third party when it connects to a tower. *See Lambis*, 197 F. Supp. 3d at 616.

111. *Id.*

112. *Id.* (discussing State v. Andrews, 227 Md. App. 350, 359 n.4 (Md. Ct. Spec. App. 2016)).

113. *Id.*

114. *Id.* at 617.

Washington University Open Scholarship

privacy.[115] Unlike *Carpenter* or *Graham*,[116] the government cannot assert that cell-site simulators obtain information maintained as business records, or that phone users concede a reasonable expectation of privacy by simply turning on their phones. Because the government cuts out the third party by directly using the cell-site simulators, the third-party doctrine cannot absolve the need for warrants.

C. Shortfalls and Concerns: What the Lambis Decision Fails to Address

Although the *Lambis* decision eliminates arguments that law enforcement agencies could make to justify their warrantless usage of cell-site simulators, there are certain shortfalls that need to be addressed. Based on *Lambis*, the government cannot assert that: 1) using a cell-site simulator usage does not implicate Fourth Amendment protections, 2) subsequent searches could produce admissible evidence even with consent, and 3) the attenuation or third-party doctrine excuse their misconduct.[117] However, courts have not addressed the concerns of privacy advocates who fear that agencies can obtain warrants without disclosing their use of cell-site simulators.[118] Furthermore, even if a request for a warrant may indicate the intended use of the simulators, it may not accurately portray their capabilities or the type of information that they intend to collect. Given the lack of knowledge and awareness on this topic, judges could be inclined to grant warrants without realizing that cell-site simulators are not only capable of tracking location history, but could also track a phone in real-time and even record calls.[119] This, combined with the efforts by federal agencies to keep information regarding cell-site simulators hidden, raises concerns that even if warrants are sought, the actual usage of cell-site simulators may exceed what the court initially had in mind when it granted the warrant.

Moreover, within the specific context of New York law, there is support

115. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); *see also* United States v. Miller, 425 U.S. 435, 442 (1976) (a bank depositor has no legitimate expectation of privacy in information voluntarily conveyed to banks in the ordinary course of business).

116. *See supra* Section III.b.

117. *See supra* Section IV.b.

118. *See supra* note 56.

119. *See* Dell Cameron & Patrick Howell O'Neill, *Police Documents Reveal How Law Enforcement Keep Stingray Use Secret*, THE DAILY DOT (Oct. 7, 2016 6:58 AM), http://www.dailydot.com/layer8/stingray-surveillance-doj-warrant-north-carolina/. *See also* Pell & Soghoian, *supra* note 10, at 144–46.

that an eavesdropping warrant, which is a type of warrant with heightened privacy protections, should be required for cell-site simulators.[120] This would require law enforcement officials to "demonstrate probable cause of unlawful activity before a surveillance warrant will issue" while being subjected to "procedures for minimizing intrusions on privacy" when using the cell-site simulators.[121] Currently, New York law explicitly covers surveillance methods such as pen registers and "trap and trace" devices.[122] While the law includes language that could apply to cell-site simulators, there has been a lack of support indicating that such devices fall directly under the ambit of New York's eavesdropping law.[123]

Additionally, the *Lambis* decision only concerns federal agents, who may already have been implicated by the DOJ's policy on cell-site simulators.[124] Because of the varying jurisdictions of federal, state, and local law enforcement, the *Lambis* decision is limited in effect in that DEA agents could now claim that they are acting in accordance with the DOJ's newly issued policy, while state and local agencies may continue their cell-site simulator usage without any consequences. To effectively monitor cell-site usage by all law enforcement officials at any level, legislation amending current New York state law is necessary and required.

120. *Memorandum: Warrant Requirement for the Use of Stingrays in New York*, NYCLU (Aug. 2015), https://www.nyclu.org/sites/default/files/memo_stingrayuse_NY_201508_final.pdf.

121. *Legislative Memo: In Support of a Warrant Requirement for the Use of Stingrays*, NYCLU (Aug. 2015), https://www.nyclu.org/en/legislation/support-warrant-requirement-use-stingrays.

122. "Trap and trace" devices, which also have been inaccurately used interchangeably with cell-site simulators by agencies, display the originating number of a phone. *See* NYCLU, *supra* note 120 (quoting N.Y. CRIM. PROC. LAW § 705.00(2), which describes trap and trace devices "as devices that identify the originating number").

123. The nature of cell-site simulators requires more effort to make the eavesdropping law directly applicable. *See* NYCLU, *supra* note 120. The eavesdropping laws criminalize "unlawfully . . . intercepting or accessing . . . an electronic communication." N.Y. PENAL LAW § 250.05. But legal exceptions, such as an exception for wiretapping, provided by the laws could also make the cell-site simulators escape the grasp of New York's penal laws. NYCLU, *supra* note 120 (obtaining "telephonic or telegraphic communication," defined as "any aural transfer" made through wire, cable, or other similar facilities, is exempt because it is separately covered by wiretapping statutes—however, wiretapping nonetheless requires a warrant). Another exception also includes signals from a "tracking device consisting of an electronic or mechanical device which permits the tracking of the movement of a person or object." *Id.* This exception covers any tracking devices, for which cell-site simulators could qualify. *Id.* Even if the devices qualify for this exception, the usage would still require warrants under *People v. Weaver*, 12 N.Y.3d 433, 447 (N.Y. 2009). *Id.*

124. *See* Benjamin Weiser, *D.E.A. Needed Warrant to Track Suspect's Phone, Judge Says*, N.Y. TIMES (July 12, 2016), http://www.nytimes.com/2016/07/13/nyregion/dea-needed-warrant-to-track-suspects-phone-judge-says.html.

Washington University Open Scholarship

IV. SUGGESTED LEGISLATIVE REMEDIES

An order by a Northern District of Illinois judge is particularly instructive on what a bill should look like in order to restrict use of cell-site simulators and to require warrants.[125] In this opinion, the court outlined specific guidelines for law enforcement officers when utilizing cell-site simulators: 1) they "must make reasonable efforts to minimize the capture of signals emitted from cell phones used by people other than the target of the investigation;" 2) they "must immediately destroy all data other than the data identifying the cell phone used by the target[, and t]he destruction must occur within forty-eight hours after the data is captured;" and 3) the officers are "prohibited from using any data acquired beyond that necessary to determine the cell phone information of the target."[126]

The second prong of the court's suggestion, instructing destruction of all data other than the data identifying the cell phone used by the target, is particularly important given the privacy interests at stake. On the federal level, the DHS policy includes a "Data Collection and Disposal" section that lists practices such as deleting all data immediately following the completion of a mission, deleting data as soon as the target is located, and making sure that the equipment does not have any data stored from previous use prior to using it for a different mission.[127] However, this does not ensure the same for state and local officials who also utilize cell-site simulators.

It is especially concerning that, after multiple requests by the NYCLU for information on cell-site simulator use, the New York State Police indicated that it had no records of relevant policy documents while continuing to purchase upgrades to improve cell-site simulator capabilities.[128] Essentially due to the nondisclosure agreements between local officials and the FBI, information is kept well-hidden regarding cell-site simulator use on the state and local level.[129] This implies that currently there is no way of determining whether New York state and local officials have implemented any policy to destroy data acquired by cell-site simulators, especially those of innocent bystanders who happen to be in the same area as a suspect of a crime.[130] The proposed bill must explicitly

125. In re Application of U.S. for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015).

126. *Id.* at *3–4.

127. DEP'T OF HOMELAND SEC., *supra* note 4.

128. NYCLU, *supra* note 8.

129. *Id.*

130. The Electronic Frontier Foundation has explained why those individuals not targeted by criminal investigations should still be concerned: "[I]f you[a]re in the area where the police are using

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9

mandate enforcement officials to destroy all collected data that is irrelevant to the investigation at hand and eventually all data after the suspect has been located.

However, note that the guidelines established by the Northern District of Illinois's decision only come into play after assuming that cell-site simulator usage initially requires a warrant.[131] The need to prove probable cause to obtain a warrant cannot be viewed as an "undue burden" placed on law enforcement[132] because of the capabilities of cell-site simulators[133] and privacy interests that are subsequently implicated. Because New York state and local officials currently engage in cell-site simulator usage without any legal oversight or even internal policies, a requirement of a warrant is necessary to protect the public from unreasonable intrusions on privacy.[134]

A. Legislative Example: California's "CalECPA"

In contrast to New York's policies, or lack thereof, California has been praised for having the most "forward-thinking" state privacy laws.[135] According to the ACLU, California state and local enforcement agencies have been using cell-site simulators in a similar manner to agencies in New York.[136] However, California's lawmaking authority took quite a drastic approach compared to New York. In 2015, California passed legislation, known as the California Electronic Communications Privacy Act (CalECPA), that strengthened the state's privacy laws and required, among other things, state and local agencies to obtain a warrant prior to using cell-

a cell-site simulator, your phone information would be captured as well—even though you may have absolutely no connection to the person or people who are the target of the search. Yet as one court opinion pointed out, applications for orders allowing the use of this technology seldom '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.'" *If I'm Not a Target of a Criminal Investigation, Why Do I Have to Worry About Cell-Site Simulators?*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/sls/tech/cell-site-simulators/faq#faq-If-I'm-not-a-target-of-a-criminal-investigation,-why-do-I-have-to-worry-about-cell-site-simulators? (last visited Jan. 15, 2017).

131. *In re Application of U.S. for an Order Relating to Telephones Used by Suppressed*, 2015 WL 6871289 at *1 (discussing how the matter came about after the government applied for a warrant for usage of cell-site simulators).

132. *See* Ada Danelo, Note, *Legislative Solutions to Stingray Use: Regulating Cell Site Simulator Technology Post-Riley*, 91 WASH. L. REV. 1355, 1391 (2016).

133. *See* Pell & Soghoian, *supra* note 10.

134. NYCLU, *supra* note 121.

135. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

136. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Jan. 15, 2017).

Washington University Open Scholarship

site simulators.[137] CalECPA broadly prohibits any governmental entities from obtaining any type of digital data, including metadata, location data, emails, and text messages, unless they obtain a warrant.[138] In addition, California recently passed another law that requires all agencies that use cell-site simulators to create specific policies regarding their use and to post them "conspicuously" on their websites.[139]

Ultimately, the New York state legislature is in the best position to ensure that state and local law enforcement officials request and obtain warrants before using cell-site simulators. Given the persistent efforts by NYCLU and the court's decision in Lambis, the New York legislature must now acknowledge that not only are cell-site simulators being frequently used, but that such unrestrained usage violates privacy rights.

CONCLUSION

It is undisputed that cell-site simulators have been used by law enforcement officials throughout the country, and especially in the state of New York. Although public knowledge of cell-site simulator use may have contributed to the publication of cell-site simulator policies by the DOJ and DHS,[140] the full impact of these devices has yet to be felt by a majority of the states. Moreover, a nondisclosure agreement between the FBI and the Erie County Sheriff's Office reveals even more troubling facts—that the Sheriff's Office is to maintain total secrecy on its cell-site simulator use, even in court filings and responding to court orders, and that it should seek dismissal of a criminal prosecution if it would entail disclosing "compromising" information on cell-site simulators.[141] This not only raises the issue of why cell-site simulators are shrouded in such secrecy, but also whether the New York state and local officials should continue to engage in cell-site simulator use without any legal restrictions or requirements.

---

137. CAL. PENAL CODE § 1546.1 (West 2017). Specifically, the statute prohibits government entities from doing the following unless they obtain a warrant, court order, or a subpoena: (1) compelling the production of or access to electronic communication information from a service provider; (2) compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device; or (3) accessing electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity. *Id.*

138. *California Rejects Warrantless Surveillance, Enacts "CalECPA,"* ELECTRONIC PRIVACY INFORMATION CENTER (Oct. 9, 2015), https://epic.org/2015/10/california-rejects-warrantless.html.

139. CAL. GOV'T CODE § 53166 (West 2016).

140. *See supra* note 4 and accompanying text.

141. NYCLU, *supra* note 8.

Efforts to keep cell-site simulator usage from public view have resulted in few adjudicated cases, but *Lambis* allowed both the public and law enforcement agencies to get a glimpse of how the court would rule, although policies issued by federal agencies already govern federal cell-site simulator usage to a large extent.[142] Specifically, the *Lambis* decision rejected the third-party doctrine, noting that cell-site simulators allow the government to directly obtain any information sought from the targeted individual and his or her cell phone, eliminating any involvement by a third party.

Additionally, CSLI litigation has also shed light on how courts evaluate these types of information and how cell phone data is acquired and used by law enforcement agencies. The clear differences that distinguish CSLI from information obtained by cell-site simulators show that such exceptions would not hold true for cell-site simulators. The trend among circuit courts is that a warrant is generally not required for CSLI because it is stored by a service provider. Since a third party stores such records, CSLI can be further classified as business records and is not protected by the Fourth Amendment due to the third-party doctrine. Furthermore, CSLI is "non-content" information, similar to the mailing addresses found on envelopes, thus government agencies do not conduct a search when they obtain CSLI.

Although numerous bills have been introduced by New York lawmakers to combat the issue of unrestricted usage of cell-site simulators, none of them have been made into law. Failed bills that have been proposed in the last two years indicate that even though there is support by privacy advocates and private companies,[143] there is a lack of support at the legislative level. The lack of transparency by New York state and local law enforcement officials regarding their use of cell-site simulators should be a source of concern not only for privacy law experts, but also for anyone who lives within the state and uses a cell phone. With the amount of information currently available, largely due to NYCLU's research and efforts, the informed public can play a vital role in petitioning their legislators to ensure that a future bill mandating warrants for cell-site simulator use would pass. In addition, the proposed legislation should also require any governmental agencies utilizing a cell-site simulator to minimize the capturing of data from anyone else but the target, take immediate measures to destroy any other acquired data besides those from the target, and limit the use of information to what is absolutely necessary to locate the target.[144]

142. *See supra* note 4 and accompanying text.
143. NYCLU, *supra* note 33.
144. *See* In re Application of U.S. for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015). *See also supra* Part IV.

Washington University Open Scholarship

Evidence acquired by civil rights groups amounts to a conclusion that law enforcement agencies have, for years, attempted to cover their cell-site simulator usage in secrecy. While their efforts to combat crimes should be recognized and respected, it does not mean that the privacy rights of ordinary citizens should be compromised without any limitations. It is time to require the legislature to act.

Cindy D. Ham[*]

* J.D. Candidate (2018), Washington University School of Law; B.A. (2013), New York University. I would like to thank Professor Neil Richards for his insight in helping me select a timely and interesting topic, and Brett Hochberg for his guidance throughout the initial drafting process of this Note. A special thanks to the excellent editors of the *Washington University Law Review*: Pierce Lamberson, Max Noreng, Minzala Mvula, Michaela Connolly, and Kara Lillehaug for all of their help in shaping this Note for publication.

https://openscholarship.wustl.edu/law_lawreview/vol95/iss2/9