Case Western Reserve Law Review

Volume 70 | Issue 1 Article 13

2019

What *Carpenter* Tells Us About When a Fourth Amendment Search of Metadata Begins

Geneva Ramirez

— Note —

What *Carpenter* Tells Us About When a Fourth Amendment Search of Metadata Begins

"Given the advancing state of both the remote sensing art and the capacity of computers to handle an uninterrupted and synoptic data flow, there seem to be no physical barriers left to shield us from intrusion."[1]

CONTENTS

1. United States v. White, 401 U.S. 745, 757 (1971) (Douglas, J., dissenting) (quoting ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 46 (1971)).

INTRODUCTION

The Fourth Amendment protects individuals from unreasonable government searches by requiring the government to procure a warrant supported by probable cause that "particularly describe[es] the place to be searched, and the persons or things to be seized," prior to searching persons or their homes, papers, or effects.[2] Traditionally, the Supreme Court's conception of the Fourth Amendment's protection was tied to physical space. The government could not seek information in an individual's constitutionally protected areas (e.g., one's home or office) without first acquiring that individual's permission or obtaining a warrant.[3] This made sense because people stored private information in private spaces, and private and public spaces were usually delineated by clear, physical boundaries. But as technology has advanced, the constitutionally-protected-area conception of the Fourth Amendment fails to provide adequate protection for that private information that is now stored, communicated, and generated digitally.

Recognizing this technological shift in 1967, the Supreme Court in *Katz v. United States*[4] adopted the view that "the Fourth Amendment protects people, not places."[5] In doing so, the Court laid down a new reasonable-expectation-of-privacy test that is not confined to constitutionally protected areas or tangible things, but extends outside of the home and office to cover electronic and digital information and other communications to which an individual has a reasonable expectation of privacy.[6]

Today, over fifty years after *Katz*, the reasonable-expectation-of-privacy test has become an even more vital safeguard against unreasonable government intrusions that are due, in large part, to the Internet. As one observer noted, "the Internet is not some standalone, separate domain where a few of life's functions are carried out. . . . Rather, it is the . . . place where virtually everything is done. It is . . . where the most private data is created and stored."[7] In fact, "more data has been created [in the years 2014 and 2015] than in the entire previous

2. "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." U.S. CONST. amend. IV.

3. Jones v. United States, 565 U.S. 400, 406 (2012).

4. 389 U.S. 347 (1967).

5. *Id.* at 351.

6. *Id.* at 352–53.

7. GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 5–6 (2014).

history of the human race."[8] And the amount of data that is created and stored on the Internet continues to grow exponentially: by 2020, "about 1.7 megabytes of new information will be created every second for every human being on the planet."[9]

The data we produce using digital devices fall into two categories: content—the substance of digital communications and activities—and metadata—data about content.[10] While the content of our digital activities is generally agreed to be subject to Fourth Amendment protection,[11] some have argued that metadata is not. In 2013, following Edward Snowden's revelation that the National Security Agency was collecting metadata about U.S. citizens on a massive scale, Senator Dianne Feinstein argued that metadata is not protected under the Fourth Amendment.[12] She reasoned that, because the records being collected did not include content, names, or locations, their collection did not qualify as surveillance.[13]

But while it is true that metadata on its face is almost meaningless to most people, it can, when analyzed, reveal the most intimate details of our lives. Our digital-activity records create information-rich "metadata trails" that, because of metadata's structured nature, can "often yield information more easily than . . . the actual content of our communications."[14] And the greater the quantity of metadata analyzed, the more revealing it can be. Large datasets can be used for everything from mapping an individual's location over a period of years, to identifying a person's relationships, habits, and behaviors.[15] This previously inaccessible source of information has the potential to make the govern–

8. Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, Forbes (Sept. 30, 2015, 2:19 AM), https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#27f04f2117b1 [https://perma.cc/R4RM-PCLS].

9. *Id.*

10. GREENWALD, *supra* note 7, at 132.

11. *See Katz*, 389 U.S. at 352; Smith v. Maryland, 442 U.S. 735, 741 (1979) (accepting *Katz*'s holding that a communication's content is subject to Fourth Amendment protection).

12. Dianne Feinstein, *Continue NSA Call-Records Program*, USA Today (Oct. 20, 2013, 6:22 PM), https://www.usatoday.com/story/opinion/2013/10/20/nsa-call-records-program-sen-dianne-feinstein-editorials-debates/3112715/ [https://perma.cc/4AAL-LFXK].

13. *Id.*

14. Declaration of Professor Edward W. Felten at ¶¶ 1, 20, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-3994).

15. *Id.* at ¶ 24.

ment practically omniscient—and it is widely agreed that "police omniscience is one of the most effective tools of tyranny."[16]

But to hold the government accountable for analyzing our metadata, we must revisit one of the Fourth Amendment's fundamental questions: When does the search begin?[17] This question is important because it determines not only at what point in the process of metadata analysis—i.e., acquisition, analysis, or use[18]—must the government secure a warrant, but also the ways in which the government may analyze and use our metadata after acquiring it.[19] While the Supreme Court has not directly addressed this issue, it provided some guidance in *Carpenter v. United States*.[20]

In *Carpenter*, the FBI subpoenaed 127 days of Timothy Carpenter's cell-site location information ("CSLI")—metadata in the form of time-stamped records containing the identification number of the cell site that his phone was connected to at a given time—from his network provider.[21] The Court held that "[t]he location information obtained from Carpenter's wireless carriers was the product of a search";[22] thus, the government had violated the Fourth Amendment by failing to acquire a warrant. The Court based its holding on its reasoning in two lines of cases.[23] The first concerns a person's expectation of privacy in their long-term physical movements.[24] The second concerns "a person's

16. United States v. White, 401 U.S. 745, 760 (1971) (Douglas, J., dissenting) (quoting Lopez v. United States, 373 U.S. 427, 466 (Brennan, J., dissenting)); *see also* Smith v. Maryland, 442 U.S. at 751 (Marshall, J., dissenting) ("[F]or those extensive intrusions that significantly jeopardize individuals' sense of security more than self-restraint by law enforcement officials is required."); GREENWALD, *supra* note 7, at 4 ("Unless such power is held in check by rigorous oversight and accountability, it is almost certain to be abused.").

17. *See generally* Orin S. Kerr, *When Does a* Carpenter *Search Start—and When Does It Stop?*, Reason: The Volokh Conspiracy (July 6, 2018, 3:34 PM), https://reason.com/volokh/2018/07/06/when-does-a-carpenter-search-start-and-w (exploring how *Carpenter v. United States*, 138 S. Ct. 2206 (2018), complicates the determination of when a search begins and ends) [https://perma.cc/KC3G-66NY].

18. Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, Brookings (Apr. 19, 2011), https://www.brookings.edu/research/use-restrictions-and-the-future-of-surveillance-law/ [https://perma.cc/9SKN-HAAN].

19. Kerr, *supra* note 17; *see also infra* Part III.

20. 138 S. Ct. 2206 (2018).

21. *Id.* at 2212.

22. *Id.* at 2217.

23. *Id.* at 2214.

24. *Id.* at 2209.

expectation of privacy in information voluntarily turned over to third parties."[25] Though the Court did not directly answer the question of when a search of metadata begins, its reasoning and the concerns it considered provide a foundation for determining when such a search begins. The answer to this question determines *what* the Fourth Amendment protects—metadata itself, or the information that results from its analysis—as well as *how* the government may use metadata it has legally obtained.

This Note explores when a Fourth Amendment search of one's historical metadata begins, based on the Supreme Court's reasoning and concerns in *Carpenter*. Part I provides an overview of what metadata is and what types of information its analysis can yield. It then takes a closer look at CSLI—the metadata at issue in *Carpenter*—and addresses the threat to privacy posed by the aggregation of large amounts of metadata. Part II provides a close analysis of the Supreme Court's reasoning in *Carpenter*. Part III discusses the various stages in the process of metadata-based surveillance at which a Fourth Amendment search could begin. It argues that, to best safeguard privacy, the search must begin not when metadata is acquired, but when it is analyzed to reveal private information. Part IV proposes a framework for analyzing when a metadata search begins. Finally, Part V suggests a reinterpretation of the Fourth Amendment's particularity requirement as it pertains to historical metadata.

I. Metadata

This section explains what metadata is, the uses for which it is collected, and what it can reveal when analyzed. It then provides an in-depth explanation of CSLI—the metadata at issue in *Carpenter*—and continues by describing the enormous range of private information that can be gleaned from the analysis of aggregated metadata.

A. Types of Metadata and Its Uses

Metadata is data about data. It does not describe a communication's or digital activity's content, but instead it comprises information about that communication or activity. For instance, if you call your mother, the metadata about the call will not take the form of a transcript of the conversation. Instead, it will contain the call's length, the date and time when the call took place, both the initiating and the receiving telephone number, the cell-site identification number of the cell tower your phone was connected to, and other logistical data.[26] Basically, it is just a list of numbers. Almost every digital activity we

25. *Id.*

26. Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 Minn. L. Rev. 577, 585–86 (2017).

engage in leaves behind "rich metadata trails."[27] And virtually every–thing we do while browsing the Internet or using digital devices is recorded and stored, "creating a permanent record of unparalleled pervasiveness and depth."[28]

This collection of data about our communications and activities may seem innocuous compared to the collection of records detailing those communications and activities. But when our metadata trails are analyzed, metadata can reveal an intimate picture of our lives.[29] In fact, by virtue of metadata's structured nature, metadata analysis can often reveal those details more easily and cost-effectively than the content of our communications.[30] This structure makes it easy to store and quickly analyze vast sets of data for patterns that can reveal our "personal details, habits, and behaviors."[31] By contrast, to analyze the content of a phone call, an analyst must transcribe the conversation, determine its meaning (taking into account a multitude of factors including language differences and code phrases), and identify relevant information.[32] The government simply does not have the resources to perform content analysis on the phone calls of three-hundred million Americans.[33]

Although Edward Snowden's revelations in 2013 gave rise to an Orwellian fear of government mass-surveillance,[34] in many cases, metadata is initially collected by private companies and only later acquired by the government. Wireless-network providers record the duration of their customers' phone calls, the number of texts they send, the numbers they call, the cell sites their phones connect to, the apps they use, and the time they spend using the Internet.[35] Websites "secretly track [their] custome[rs'] websurfing," amassing "record data about [their] ISP, computer hardware and software, the website [they] linked from, and exactly what parts of the website [they] explored and

27. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 1.

28. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 26 (2004).

29. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 1.

30. *Id.* ¶¶ 1, 20–21, 29 (attributing this ease and cost-effectiveness to metadata being "stored in a predictable, standardized format").

31. *Id.* ¶ 24.

32. *Id.* ¶ 28.

33. *Id.* ¶ 29.

34. Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, The Guardian (June 11, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/2V2Y-V3VK].

35. *See infra* Part I.B.

for how long."[36] Google acknowledges that it collects its users' "unique identifiers tied to the browser, application, or device [they]'re using" as well as data concerning "the interaction of [the users'] apps, browsers, and devices . . . , including IP address, crash reports, system activity, and the date, time, and referrer URL."[37] Even fitness apps track and record metadata about their users' health and activity.[38]

These service providers generally collect this information for a variety of business purposes. Wireless-network providers use the metadata they collect to: (1) monitor and improve network performance; (2) deliver and maintain products and services; (3) monitor and maintain account and billing records; (4) detect misuse and assure security; (5) deliver marketing offers; and (6) in the case of T-Mobile, respond to legal processes and emergencies.[39] Network providers also aggregate this data "for a variety of purposes such as scientific and marketing research and services."[40] Websites use metadata to reveal what parts of the website are most popular, how long a user's attention span is, what language the site should be displayed in for a particular user, and what kinds of products a user might be interested in.[41] In 2004, in preparation for Hurricane Frances, Walmart knew to ship not only extra flashlights to Florida's Atlantic Coast, but also strawberry Pop-Tarts and beer—products that Walmart's data analysis showed sell at up to seven times their normal rate in the period immediately before a hurricane hits.[42]

36. SOLOVE, *supra* note 28, at 23–24.

37. *Google Privacy Policy,* GOOGLE (May 25, 2018), https://www.gstatic.com/policies/privacy/pdf/20180525/853e41a3/google_privacy_policy_en.pdf [https://perma.cc/BD8E-QDBC].

38. Susan Freiwald & Stephen W. Smith, *The* Carpenter *Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205, 230 (2018).

39. *Wireless Customer Agreement*, AT&T, https://www.att.com/legal/terms.wirelessCustomerAgreement.html#howCanIGetMobileContent [https://perma.cc/MY96-UYTK]; *Sprint Corporation Privacy Policy*, SPRINT, https://www4.sprint.com/legal/privacy.html [https://perma.cc/XV4Y-7X7F] (last updated Mar. 29, 2017); *T-Mobile Privacy Statement*, T-MOBILE, https://www.t-mobile.com/responsibility/privacy/tvision-privacy-policy [https://perma.cc/NA8Q-HAFY] (last updated Oct. 1, 2019); *Privacy Policy*, VERIZON, https://www.verizon.com/about/privacy/full-privacy-policy [https://perma.cc/Y5CD-JKZZ] (last updated Apr. 2019).

40. *Wireless Customer Agreement*, AT&T, https://www.att.com/legal/terms.wirelessCustomerAgreement.html#howCanIGetMobileContent [https://perma.cc/97R7-ACSA].

41. SOLOVE, *supra* note 28, at 23–24.

42. Constance L. Hays, *What Wal-Mart Knows About Customers' Habits*, N.Y. TIMES (Nov. 14, 2004), https://www.nytimes.com/2004/11/14/

The same metadata that private companies use to improve their marketing and products is also valuable to the government for other purposes, namely cost-effective and minimally invasive surveillance.[43] The government often acquires metadata by wiretapping Internet service providers, using court-ordered warrants or subpoenas, or simply purchasing it from data brokers or directly from the websites that collect it.[44] This metadata can be analyzed and searched to discover more information about an identified target or "to discover the perpetrator of a past or future event."[45] In some cases, it reveals information that the government could not obtain through other means, allowing the government to "track individuals through places where it would otherwise be uneconomical to do so, [and] even through places where it would otherwise be effectively *impossible* for the government to do so, such as within the surveillance target's own home or office."[46] Historical metadata even allows the government to go back in time to track a suspect.[47]

B. CSLI

In *Carpenter v. United States*, Carpenter challenged the government's warrantless acquisition of his cell-site location information—the metadata generated every time a phone connects to a cell site. Cell phones perform most of their functions by connecting to radio antennas owned by wireless-network providers.[48] These radio antennas and the towers that house them are commonly referred to as "cell sites."[49] A

business/yourmoney/what-walmart-knows-about-customers-habits.html [https://perma.cc/P2PW-GTD9].

43. Kerr, *supra* note 18, at 11–12.

44. Bryan Bumgardner, *How Are the NSA and Others Collecting and Using Our Data?*, SCI. AM. (June 20, 2013), https://www.scientificamerican.com/article/how-are-the-nsa/ [https://perma.cc/8BTH-GQ9C]; Bruce Schneier, *Do You Want the Government Buying Your Data from Corporations?*, THE ATLANTIC (Apr. 30, 2013), https://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/ [https://perma.cc/FU5W-XQXW].

45. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 322–23 (2008).

46. Brief of Technology Experts as Amici Curiae in Support of Petitioner at 28–29, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (emphasis in original).

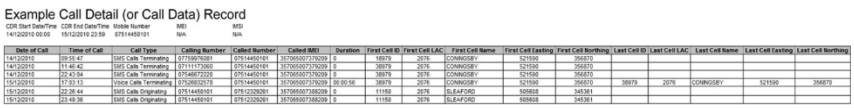
47. Slobogin, *supra* note 45, at 322–23.

48. *Carpenter*, 138 S. Ct. at 2211; Matthew Tart et al., *Historic Cell Site Analysis—Overview of Principles and Survey Methodologies*, 8 DIGITAL INVESTIGATIONS 185, 186 (2012).

49. Eric Pait, *Find My Suspect: Tracking People in the Age of Cell Phones*, 2 GEO. L. TECH. REV. 155, 157 (2017).

cell phone typically connects to surrounding cell sites and pushes through data via the strongest connection, which is often, but not always, the cell site in closest proximity to that phone.[50] As the phone is carried from place to place, "its connection transfers from cell site to cell site, maintaining a continuous connection with the strongest available signal."[51]

When a cell phone connects to a cell site, it generates a time-stamped record containing metadata about that connection (aka, CSLI), which is collected and stored by the wireless-network provider that owns the cell site.[52] CSLI includes the identification number of the cell site ("Cell ID") that the phone initially connected to, the date and time the connection was made, the phone numbers involved, and often the Cell ID of the site the phone was connected to when the call ended.[53] When analyzed, this information can reveal a cell phone's general location, and by proxy, its user's location, at the time the record was generated.[54] If enough CSLI records are analyzed, it is possible to observe "the whole of [a person's] physical movements."[55]


Example Call Detail (or Call Data) Record

CDR Start DateTime 14/12/2010 00:00 CDR End DateTime 15/12/2010 23:59 Mobile Number 07514456101 IMEI N/A IMSI N/A

Date of Call	Time of Call	Call Type	Calling Number	Called Number	Called IMEI	Duration	First Cell ID	First Cell LAC	First Cell Name	First Cell Easting	First Cell Northing	Last Cell ID	Last Cell LAC	Last Cell Name	Last Cell Easting	Last Cell Northing
14/12/2010	09:55:47	SMS Calls Terminating	07759976081	07514456101	357065007379299	0	38979	2076	CONINGSBY	521590	356870					
14/12/2010	11:46:42	SMS Calls Terminating	07711173968	07514456101	357065007379299	0	38979	2076	CONINGSBY	521590	356870					
14/12/2010	22:43:04	SMS Calls Terminating	07546872220	07514456101	357065007379299	0	38979	2076	CONINGSBY	521590	356870					
15/12/2010	17:33:13	Voice Calls Terminating	07526832278	07514456101	357065007379299	00:00:56	38979	2076	CONINGSBY	521590	356870	38979	2076	CONINGSBY	521590	356870
15/12/2010	22:26:44	SMS Calls Originating	07514456101	07512329261	357065007388299	0	11150	2076	SLEAFORD	505808	345361					
15/12/2010	23:49:36	SMS Calls Originating	07514456101	07512329261	357065007388299	0	11150	2076	SLEAFORD	505808	345361					

56

While wireless-network providers collect and retain CSLI for a variety of business purposes,[57] their data-collection efforts have also

50. Tart et al., *supra* note 48.

51. Pait, *supra* note 49.

52. Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, THE ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197/ [https://perma.cc/8K45-FNJD].

53. Tart et al., *supra* note 48, at 185.

54. *Id.* at 188.

55. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). In 2009, Malte Spitz, a German politician, sued his wireless-network provider because it refused to disclose to Spitz the CSLI generated by his cell phone. *Tell-All Telephone*, ZEIT ONLINE, https://www.zeit.de/datenschutz/malte-spitz-data-retention [https://perma.cc/BE7S-CV2X] (last visited Aug. 29, 2019). In settlement, Spitz received six months of metadata his wireless-network provider had collected. *Id.* Together with Zeit Online, he created an interactive map of his movements, calls, tests, and internet connectivity revealed by analyzing the six months of metadata. *Id.* To get a sense of the historical surveillance capacity of CSLI, *see id.*

56. Tart et al., *supra* note 48, at 188.

57. *See supra* notes 39–40 and accompanying text.

been a boon for law enforcement officials who can now determine a suspected criminal's present and past locations simply by analyzing the CSLI generated by the suspect's cell phone.[58] Because most individuals keep their cell phones with them at all times, the analysis of this historical CSLI can paint a detailed picture of their past movements, information that may otherwise be unavailable to law enforcement.[59] And law enforcement taps this power frequently, requesting historical CSLI from phone companies tens of thousands of times each year.[60]

After law enforcement acquires an individual's CSLI from a phone company, it must analyze it "in conjunction with other information such as survey and geographic data, to determine areas where a phone may, or may not, have been when it was used."[61] The first step is to combine the CSLI with a database containing, for instance, the location of the cell sites that correspond to the Cell IDs in the records.[62] Next, law enforcement must determine "the area over which the cell [site] could be expected to provide service and whether or not this includes specific locations of interest to the investigation."[63] The precision of the location information gleaned from CSLI is determined by the cell coverage area,[64] which depends on a variety of factors, including "the height of the [cell] antenna (aerial), the power used, the location of other cells and the geography of the land (hills, trees, etc.) including

58. Pait, *supra* note 49, at 158.

59. *Id.* at 156, 160–61.

60. Law enforcement is not required to keep records of how many CSLI requests they make each year, but a rough estimation can be made based on the transparency reports of major wireless-network providers. *See* Freiwald & Smith, *supra* note 38, at 232. From January 2018 through June 2018, AT&T received 42,180 demands from law enforcement for the CSLI records of its users. AT&T, TRANSPARENCY REPORT 4 (Aug. 2018), https://about.att.com/ecms/dam/csr/aug2018/TransparencyReports/Aug-2018-TransparencyReport.pdf [https://perma.cc/3EER-Y5VM]. In 2017, T-Mobile received 64,266 CSLI demands. T-MOBILE US INC., TRANSPARENCY REPORT FOR 2017, at 6 (2017), https://www.t-mobile.com/content/dam/t-mobile/corporate/newsroom/pages/factsheetspdf/TransparencyReport2017.pdf [https://perma.cc/KHP2-BDMA]. *See also* VERIZON, TRANSPARENCY REPORT 1H 2018, https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2018/08/Transparency-Report-US-21-2018.pdf [https://perma.cc/S4CZ-3UAQ]; SPRINT, SPRINT CORPORATION TRANSPARENCY REPORT (Jan. 2018), https://newsroom.sprint.com/csr/content/1214/files/Transparency%20Report%20January%202018.pdf [https://perma.cc/AN2P-PPMU] (listing law enforcement's demands for customer information by type of request).

61. Tart et al., *supra* note 48, at 185.

62. *Id.* at 187.

63. *Id.*

64. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

surrounding buildings."[65] While it is true that CSLI is not as precise as GPS coordinates,[66] the growing demand for cell-phone data has prompted wireless-network providers to install more and more cell sites, resulting in smaller coverage areas for each cell site, thereby increasing the precision of the collected location information.[67] Today, the cover–age area of a cell site can range from twenty kilometers in rural areas to as little as one hundred meters in densely populated areas like shopping malls.[68]

It is unclear exactly how many CSLI data points wireless-network providers collect from a cell phone each day. But in *Carpenter*, MetroPCS and Sprint together provided the government with 127 days of CSLI from Timothy Carpenter's phone, totaling 12,898 location points.[69] This means that, on average, Sprint and MetroPCS collected 101 data points per day from Carpenter's phone.[70] It is also unclear what types of phone activity cause CSLI to be generated and stored.[71] If, however, most providers are like T-Mobile—one of the few wireless-network providers that discloses the types of activities that generate CSLI—they probably collect CSLI every time a cell phone is "turned on, calls and text messages [are] sen[t] or receive[d] . . . , and other data services [are] use[d]."[72]

C. The Aggregation Problem

Most metadata can be analyzed in various ways to produce different types of information. A single CSLI record, for example, could be analy–zed in one way to reveal the user's general location at the time she placed a call, and in another way to reveal who she called. But the risk that the government might analyze metadata to reveal information it did not originally seek is exacerbated by the aggregation problem. While discrete pieces of metadata can reveal highly private information,

65. Tart et al., *supra* note 48, at 186.

66. United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016), *rev'd and remanded*, 138 S. Ct. 2206 (2018).

67. *Carpenter*, 138 S. Ct. at 2211–12.

68. Tart et al., *supra* note 48, at 186.

69. *Carpenter*, 138 S. Ct. at 2212.

70. *Id.*

71. When I contacted AT&T on January 4, 2019, seeking my own CSLI, I was told that AT&T's technical division could not provide me with that data due to its "sensitive nature," nor would AT&T forward my request to its legal department without a "subpoena or legal document."

72. *T-Mobile Privacy Statement*, T-MOBILE, https://www.t-mobile.com/responsibility/privacy/privacy-policy [https://perma.cc/EC7B-6HYK] (last updated Oct. 1, 2019).

aggregated metadata can expose much more.[73] When metadata is amassed in large quantities and analyzed, patterns and correlations start to emerge.[74] And those patterns can reveal information that is fundamentally different from what could be gleaned through isolated, relatively innocuous pieces of metadata.[75]

By analyzing aggregated call records, the government can create a detailed map of a person's social network, including his or her friends, family, colleagues, psychiatrists, insurance providers, doctors, baby–sitters, lawyers, and so on.[76] These records can reveal not only who someone calls, but the nature of the caller's relationship with the call's recipient.[77] People who call each other every week likely have a closer relationship than those who speak only once a year.[78] Two people who frequently call each other late at night might be in a relationship; if they stop calling, the relationship has probably ended.[79] If two people talk only between 9:00 a.m. and 5:00 p.m., they likely have a prof–essional relationship. Metadata can even reveal people's relative power and social status. The Economist noted that "[p]eople at the top of the office or social pecking order often receive quick callbacks, do not worry about calling other people late at night and tend to get more calls at times when social events are most often organi[z]ed, such as Friday afternoons."[80] This analysis reveals information about not only the person being surveilled, but also about people who were never the intended targets of that surveillance.[81]

Highly personal information can also be discovered by analyzing a sequence of calls in context.[82] Edward Felten, Deputy U.S. Chief Technology Officer during the Obama Administration,[83] provides the following illustration:

---

73. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 39.

74. Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 Wash. L. Rev. 35, 42 (2014).

75. Berman, *supra* note 26, at 579.

76. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 48.

77. *Id.* ¶¶ 49–50.

78. *Id.* ¶ 49.

79. *Id.*

80. *Untangling the Social Web*, The Economist (Sept. 4, 2010), https://www.economist.com/technology-quarterly/2010/09/04/untangling-the-social-web [https://perma.cc/7SKF-9FFB].

81. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 24.

82. *Id.* ¶ 52.

83. Megan Smith & Alexander MacGillivray, *The White House Names Dr. Ed Felten as Deputy U.S. Chief Technology Officer*, The White House: Blog (May 11, 2015, 2:00 PM), https://obamawhitehouse.archives.gov/blog/

> A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.[84]

Location metadata, too, can reveal deeply private information "because of the common sense observation that individuals often go to *particular locations* for *particular purposes*."[85] A person's location metadata that contains repeat visits to a particular church every Sunday morning might reveal his religion. Another's metadata containing regular visits to that same church every Tuesday evening might reveal that he is attending an addiction-support group.

In *Carpenter*, the Court acknowledged that a person may have a greater expectation of privacy in her aggregated location information because of the power that aggregation has to reveal information that would be otherwise unavailable.[86] Aggregation can reveal information that a surveillance target never made a conscious decision to share; information that once could have been acquired only by examining the content of a person's communications;[87] information that, if stored in a physical form, the government could acquire only with a warrant.

II. WHAT *CARPENTER* TOLD US

Carpenter is the first Supreme Court case to address an individual's Fourth Amendment rights with regard to historical metadata. In holding that the government must obtain a warrant to "access[] historical cell phone records that provide a comprehensive chronicle of the user's past movements,"[88] the Court broke new ground in ensuring individuals' digital privacy. This Part discusses the facts of *Carpenter* and the analysis the Supreme Court used to determine that individuals have a legitimate expectation of privacy with regard to their aggregated CSLI.

2015/05/11/white-house-names-dr-ed-felten-deputy-us-chief-technology-officer [https://perma.cc/S3ZU-7KS5].

84. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 52.

85. Brief of Technology Experts as Amici Curiae in Support of Petitioner, *supra* note 46, at 29 (emphasis in original).

86. Carpenter v. United States, 138 S. Ct. 2206, 2219, 2232 (2018).

87. Declaration of Professor Edward W. Felten, *supra* note 14, ¶ 39.

88. *Carpenter*, 138 S. Ct. at 2211.

A. The Facts

In 2011, the Detroit Police Department arrested four people it suspected of breaking into a series of Radio Shack and T-Mobile stores in Michigan and Ohio.[89] One of the suspects admitted that the group had robbed nine different stores over a four-month period.[90] After confessing, the suspect provided the FBI with the names and cell-phone numbers of fifteen other individuals who he claimed were accomplices in one or more of those robberies.[91] Timothy Ivory Carpenter was one of those named individuals.[92] Based on the suspect's information, the prosecutors sought court orders under the Stored Communications Act to acquire 152 days of Carpenter's CSLI from his wireless-network providers.[93] The Stored Communications Act requires only that the prosecutor presents "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . sought are relevant and material to an ongoing investigation."[94] Finding that this standard had been met, a magistrate judge issued two orders to produce Carpenter's CSLI.[95]

The first order directed MetroPCS, Carpenter's network-service provider, to hand over 152 days of his CSLI. The second directed Sprint, the network Carpenter's phone had connected to for a week while it was "roaming" in northeastern Ohio, to hand over seven days of CSLI. The CSLI sought included "call detail records . . . [and] cell site info–rmation from the target telephones at call origination and at call termination for incoming and outgoing calls."[96] In response, MetroPCS produced 127 days of records. Sprint produced two.[97] All told, the government obtained 12,898 CSLI data points tracing Carpenter's movements over the course of more than four months.[98] In addition to the CSLI itself, MetroPCS and Sprint provided the locations and other details of each of their cell sites in Michigan and Ohio, including the

89. *Id.* at 2212.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*; 18 U.S.C. § 2703 (2012).

94. 18 U.S.C. § 2703(d) (2012).

95. *Carpenter*, 138 S. Ct. at 2212.

96. Brief for Petitioner at 3–4, *Carpenter*, 138 S. Ct. 2206 (No. 16-402); *see also Carpenter*, 138 S. Ct. at 2212 (explaining that the magistrate judges issued orders directing Carpenter's cellular carriers to disclose the cell-site information for his phone during the four-month period of the robberies).

97. *Carpenter*, 138 S. Ct. at 2212.

98. *Id.*

longitude, latitude, physical address, and directional orientation of each antenna.[99] By cross-referencing Carpenter's CSLI with the cell-site information, the government was able to connect Carpenter's cell phone's physical location to four of the robberies.[100]

The government charged Carpenter with six counts of aiding and abetting a robbery in violation of the Hobbs Act.[101] Before trial, Carpenter moved to suppress the cell-site evidence on the ground that the government violated the Fourth Amendment by obtaining his CSLI records without a warrant supported by probable cause.[102] The district court rejected that argument, accepting the government's position that Carpenter had no legitimate expectation of privacy in his CSLI because it served merely as a "proxy for [his] visually observable location . . . along public highways."[103] The Sixth Circuit affirmed, holding that individuals have no reasonable expectation of privacy in cell-phone location records because they qualified as business records obtained from a third party.[104] The Supreme Court reversed, holding that Carpenter had a reasonable expectation of privacy in his cell-site records.[105]

B. The Supreme Court's Reasoning

Writing for the majority, Chief Justice Roberts declared that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[106] This principle has guided the evolution of the Supreme Court's interpretation of the Fourth Amendment as the technological revolution has progressed.[107]

The Chief Justice observed that, traditionally, the Court's interpretation of the Fourth Amendment has been "tied to common-law tres–

99. Petition for Writ of Certiorari at 6, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

100. *Carpenter*, 138 S. Ct. at 2212–13.

101. *See id.* at 2212; 18 U.S.C. § 1951 (2012).

102. *Carpenter*, 138 S. Ct. at 2212.

103. United States v. Carpenter, No. 12-20218, 2013 WL 6385838, at *2 (E.D. Mich. Dec. 6, 2013), *aff'd*, 819 F.3d 880 (6th Cir. 2016), *rev'd and remanded*, 138 S. Ct. 2206 (2018).

104. United States v. Carpenter, 819 F.3d 880, 888–89 (6th Cir. 2016); *see also infra* Part II.C.2.

105. *Carpenter*, 138 S. Ct. at 2220.

106. *Id.* at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001) (alteration in original)).

107. *Id.* at 2213–14.

pass and focused on whether the Government obtains information by physically intruding on a constitutionally protected area."[108] But the Court severed this tie between property rights and privacy rights in *Katz v. United States*.[109] In *Katz*, the government attached a recording device to the outside of a public telephone booth that Katz used to transmit wagering information and submitted the recordings of Katz's side of the conversation as evidence at trial.[110] The government argued that the booth was not a constitutionally protected area; and even if it was, the recording device did not physically penetrate the phone booth.[111]

The Court rejected those arguments, holding that intruding on a defendant's physical property is not necessary to invoke the Fourth Amendment because "the Fourth Amendment protects people, not places."[112] In so holding, the Court created a reasonable-expectation-of-privacy standard that redefined the scope of the Fourth Amendment's protection. In his concurring opinion, Justice Harlan articulated a two-part test to define what constitutes a reasonable expectation of privacy: (1) the person must have an actual, subjective expectation of privacy; and (2) that expectation must be "one that society is prepared to recognize as 'reasonable.'"[113] Justice Harlan's test has been widely adopted by subsequent courts,[114] which have measured objective reasonableness by "historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'"[115]

After establishing that *Katz* provides the relevant standard, Chief Justice Roberts noted that two lines of cases emerged from *Katz* that were applicable in *Carpenter*.[116] The first concerns "a person's expectation of privacy in his physical location and movements."[117] The second

108. *Id.* at 2213.

109. 389 U.S. 347 (1967).

110. *Id.* at 348.

111. *Id.* at 351–52.

112. *Id.* at 350–51.

113. *Id.* at 361 (Harlan, J., concurring).

114. *See* Kyllo v. United States, 533 U.S. 27, 33 (2001); Smith v. Maryland, 442 U.S. 735, 740–41 (1979).

115. Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925) (alteration in original)).

116. *Id.* at 2214–15.

117. *Id.* at 2215.

concerns whether a person has a legitimate expectation of privacy in information he has shared with a third party.[118]

1. Expectation of Privacy in Physical Location and Movements

In the first line of cases, the Court considered its prior holding in *United States v. Knotts*[119] and the concurring opinions in *United States v. Jones*.[120] In *Knotts*, the government suspected Knotts and his co-defendants, Petschen and Armstrong, of manufacturing illicit drugs after the M3 Company, a chemical manufacturer, reported to the police that Armstrong—one of its employees—had been stealing chemicals that could be used to manufacture illicit drugs.[121] Visual surveillance of Armstrong revealed that he continued to purchase the same type of chemicals from another local chemical company after the M3 Company terminated him.[122] With the chemical company's consent, officers installed a radio beeper—a device that emits periodic radio signals that can be picked up with a receiver—in a drum of chloroform later purchased by Armstrong.[123] The officers then used both the beeper and visual surveillance to tail Armstrong and Petschen to Knotts's property, where the drugs were being manufactured.[124] The Court rejected Knotts's Fourth Amendment claim, stating that he had no reasonable expectation of privacy in his movements over public thoroughfares.[125]

Similarly, in *Jones*, the government, without a valid warrant, attached a GPS monitor to the undercarriage of Jones's Jeep.[126] The government argued that attaching the GPS monitor was the equivalent of the beeper in *Knotts*, and that Jones had "no reasonable expectation of privacy . . . in the locations of the Jeep on public roads, which were visible to all."[127] Writing for the Court, Justice Scalia determined that Jones's Fourth Amendment rights had been violated because the government "occupied private property [the undercarriage of Jones's Jeep] for the purpose of obtaining information."[128] In doing so, the government's action fell under the traditional property-based approach

118. *Id.* at 2216.

119. 460 U.S. 276 (1983).

120. 565 U.S. 400 (2012).

121. *Knotts*, 460 U.S. at 278.

122. *Id.*

123. *Id.*

124. *Id.* at 278–79.

125. *Id.* at 281–82.

126. United States v. Jones, 565 U.S. 400, 402–03 (2012).

127. *Id.* at 406.

128. *Id.* at 404.

to Fourth Amendment analysis.[129] Though Justice Scalia acknowledged the *Katz* reasonable-expectation-of-privacy test, he concluded that *Katz* did not overrule the traditional property-based analysis, but added an additional method of analysis.[130]

Even though all nine justices joined in Justice Scalia's holding that the government had violated the Fourth Amendment, Justice Sotomayor (writing for herself) and Justice Alito (joined by Justices Ginsburg, Breyer, and Kagan) wrote separately, advocating that the *Katz* reasonable-expectation-of-privacy test was the proper standard. Both Justice Sotomayor and Justice Alito argued that individuals have a reasonable expectation of privacy in the whole of their physical movements, and that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[131] Justice Sotomayor and Justice Alito observed that, while Jones's location had been gleaned by intruding on Jones's private property, a Fourth Amendment violation would have occurred even if the government had not used technology necessitating such an intrusion.[132]

Justice Sotomayor acknowledged that when amassed, location information can reveal intimate details about a person's life—including "their political and religious beliefs, sexual habits, and so on"—that could not be learned by examining an individual's location through short-term surveillance.[133] Accordingly, she argued that individuals have a reasonable expectation of privacy in their long-term physical location.[134] Justice Alito, in turn, noted that historically, privacy protections were often practical as much as constitutional.[135] He explained that as technology advances and makes increasingly pervasive surveillance more practical, measuring the scope of Fourth Amendment protections using a reasonable-expectation-of-privacy standard is necessary to protect people from unreasonable government intrusion.[136]

In *Carpenter*, the majority employed the logic of Justice Sotomayor and Justice Alito's *Jones* opinions to hold that the broad scope of the location information acquired by the government violated Carpenter's reasonable expectation of privacy in the whole of his physical movements.[137] The Court emphasized that the ease of CSLI's acquis–

129. *Id.* at 405.

130. *Id.* at 409.

131. *Id.* at 415 (Sotomayor, J., concurring).

132. *Id.* at 414–15; *id.* at 430 (Alito, J., concurring).

133. *Id.* at 415–16 (Sotomayor, J., concurring).

134. *Id.*

135. *Id.* at 429 (Alito, J., concurring).

136. *Id.* at 429–30.

137. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

ition and analysis, its aggregation over a four-month period, and its retrospective quality were all factors indicating that Fourth Amendment protection should apply.[138]

2. Expectation of Privacy in Information Shared with Third Parties

In the second line of cases, the Court considered whether individuals retain an expectation of privacy in information they share with third parties. In the first of those cases, *United States v. Miller*,[139] the government subpoenaed Miller's bank records after he was suspected of defrauding the government of whiskey taxes.[140] The Court applied the *Katz* test and held that Miller had no reasonable expectation of privacy in his bank records because the records were "negotiable instruments," not private papers.[141] By revealing those instruments to the bank, a third party, Miller assumed the risk that they might be shared with the government.[142] This idea became known as the "third-party doctrine," whereby an individual does not maintain an objectively reasonable expectation of privacy in information they voluntarily share with a third party.[143]

Three years later, in *Smith v. Maryland*,[144] the Court again applied the third-party doctrine. Smith claimed that the warrantless installation of a pen register—a device that records the telephone numbers dialed from a particular phone—in his telephone company's central office to record the numbers he dialed was a violation of his Fourth Amendment rights.[145] But, applying the *Katz* analysis, the Court expressed doubt that individuals subjectively expect that the numbers they dial are private.[146] Even if Smith had subjectively believed that the numbers were private, the Court determined that this expectation was not objectively reasonable because by voluntarily sharing the numbers with the telephone company, Smith forfeited his reasonable expectation of privacy.[147]

138. *Id.* at 2217–20.

139. 425 U.S. 435 (1976).

140. *Id.* at 436.

141. *Id.* at 442.

142. *Id.* at 440, 442–43.

143. WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(c) (5th ed. 2012).

144. 442 U.S. 735 (1979).

145. *Id.* at 737, 741.

146. *Id.* at 742.

147. *Id.* at 743–44.

In its decision not to apply the third-party doctrine in *Carpenter*, the Court noted that "*Smith* and *Miller* . . . did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate "expect–ation of privacy" concerning their contents.'"[148] The Court determined that, despite being in the possession of a third party, CSLI is not "shared" in the normal sense because the decision to share CSLI is not conscious or voluntary.[149] The Court reasoned that cell-phone use is "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[150] Furthermore, cell phones record CSLI as a "dint of their operation, without any affirm–ative act on the part of the user beyond powering up."[151] As Justice Sotomayor observed in *Jones*, the third-party doctrine may require reconsideration in this digital age so as not to make secrecy "a prereq–uisite for privacy."[152] The *Carpenter* Court seems to have agreed; its interpretation of the third-party doctrine represents a significant narrowing of the doctrine's scope.[153]

3. What *Carpenter* Tells Us About When the Search Begins

While the *Carpenter* Court told us that "the information obtained from Carpenter's wireless carriers was the product of a search," it did not tell us at what point that search began.[154] The Court alternated between the terms "access" and "acquire" to refer to the government's actions.[155] Its use of those terms provides little guidance, however, as the Court used the terms interchangeably, yet seemingly assigned them distinct, undefined meanings. Even so, the Court's rationales and considerations provide an excellent foundation for determining when a search of metadata begins.

148. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

149. *Id.* at 2220.

150. *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

151. *Id.*

152. 565 U.S. at 417–18 (Sotomayor, J., concurring).

153. Freiwald & Smith, *supra* note 38, at 224.

154. 138 S. Ct. at 2217.

155. Kerr, *supra* note 17.

III. Stages of Digital Surveillance Using Metadata and a Result-Oriented Application of Fourth Amendment Metadata Analysis

The Supreme Court has repeatedly held that the purpose of the Fourth Amendment is "to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[156] As such, Fourth Amendment analyses must evolve to "assure[] preserv–ation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[157] This Part describes the various stages at which a Fourth Amendment search could be said to begin regarding metadata-based surveillance. Furthermore, this Part argues that an acquisition-based model—determining that the search begins when the government obtains metadata—would often be insuff–icient to safeguard privacy in the digital age. At least where most historical metadata are concerned, privacy is better protected by a result-oriented model—finding that a search begins when metadata is analyzed to reveal meaningful information, not when raw metadata is acquired by the government.

There are several basic stages of digital surveillance at which a search could begin: (1) data collection, (2) data analysis, (3) disclosure to a person of the results of analysis, and (4) public disclosure.[158] The first stage, data collection, occurs when the government acquires data by accessing and copying it.[159] In *Carpenter*, this occurred when the wireless-network provider sent a copy of Carpenter's unanalyzed CSLI records to law enforcement.

The second stage, data analysis, occurs when the government manipulates the data it has acquired to "achieve particular goals."[160] This manipulation commonly involves transferring the data to a database and combining it with another database in a way that gives meaning to and contextualizes the original data.[161] At this stage, the data are manipulated by a computer and neither the data nor the results of its analysis are viewed by a human analyst.[162] CSLI is manip–ulated first by aggregating it into a database then combining that database with a second set of data containing the location of, and other

156. *Carpenter*, 138 S. Ct. at 2213.

157. *Id.* at 2214 (alteration in original) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

158. Kerr, *supra* note 18.

159. *Id.*

160. *Id.*

161. *Id.*; Kerr, *supra* note 17.

162. Kerr, *supra* note 18.

information about, the cell sites that correspond to the Cell IDs in the CSLI.[163]

The third stage, disclosure to a person, occurs when "an individual with proper access to the database receives the fruits of the [prior] data collection and [analysis]."[164] An analyst can do this by searching or querying the machine-manipulated data to access information in an intelligible form.[165] Using CSLI, this step occurs when the analyst queries the combined CSLI and the informational databases to create a map of the user's historical location.[166]

The final stage of the metadata-surveillance process, public disclos–ure, occurs when the government discloses or uses the information it has gleaned from the data.[167] In *Carpenter*, this occurred when the government presented at trial the location evidence derived from Carpenter's historical CSLI records.[168]

Traditionally, a search for tangible evidence stored in physical space begins when the government breaches a private space where it believes the evidence is stored.[169] "The reasons for this focus are largely historical":[170] the framers were concerned with limiting the government's power to intrude upon and seize private citizens and their property. Thus, "[t]he Fourth Amendment was enacted to limit the government's ability to break into homes and other private spaces in order to take away private property. Breaking into the home was a search. Taking away property was a seizure."[171] But generally, there is no private space breached when conducting a metadata search because most metadata is stored on third-party-owned servers. So at what stage in the metadata-based surveillance does the equivalent of a breach occur?

The intuitive answer is that the search begins at stage one: data acquisition.[172] Requiring the government to procure a warrant before it acquires metadata would mean that the government could not secretly amass huge stores of metadata. This idea is highly appealing in light of

163. *See* Tart et al., *supra* note 48, at 185.

164. Kerr, *supra* note 18, at 7.

165. *Id.*

166. *See, e.g.*, *Tell-all Telephone*, *supra* note 55.

167. Kerr, *supra* note 18.

168. Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018).

169. Kerr, *supra* note 18.

170. *Id.*

171. *Id.*

172. *See* Kerr, *supra* note 17.

the government's vast data-collection capacity.[173] If the government does not possess data, it cannot misuse it.[174] But a result-oriented approach will ultimately better protect our privacy because it is not until step three—when the data are given meaning through analysis and exposure to human eyes—that metadata reveals private information. If a search begins when a person's reasonable expectation of privacy is infringed upon,[175] then it is not until step three that the search beings.

Two considerations support this view. First, acquiring metadata does not violate personal security in the same way a physical search does. The government entering a person's home is highly invasive. Acquiring metadata from a person's wireless-network provider is more innocuous because, to most people, that metadata is facially meaningless; only after the metadata is analyzed does it reveal private information. For example, CSLI is comprised of numbers that are meaningless without analysis.[176] A map of a person's historical location does not emerge until the Cell IDs in CSLI are cross-referenced with information about the geographic area served by the corresponding cell sites.[177] Thus, a person's sense of security and privacy is violated only by the information the government obtains after its analysis, not by the information's initial acquisition.

The second consideration involves determining when the search ends. In *Illinois v. Andreas*,[178] the Supreme Court found that "once police are lawfully in a position to observe an item first-hand, its owner's privacy interest in that item is lost."[179] The Court's logic supports the idea that once the government is in legal possession of information, it need not obtain further warrants to use that information in other ways or for other purposes. But this poses a distinct privacy risk because analyzing metadata in different ways and in different combinations can result in different information than that which the metadata was originally acquired to reveal.[180] Indeed, the *Carpenter* Court emphasized that its reasoning rested at least in part on the fact that CSLI is "detailed, encyclopedic, and effortlessly compiled."[181] But an individual's privacy is better protected from the government's

173. *See* Greenwald et al., *supra* note 34 (discussing the reveal of NSA's extensive surveillance).

174. *See id.*

175. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

176. *See, e.g.*, Tart et al., *supra* note 48 and accompanying image.

177. *See supra* Part I.B.

178. 463 U.S. 765 (1983).

179. *Id.* at 771.

180. *See supra* Part I.C.

181. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

repeated and varied use of her information if the government can only acquire her metadata without a warrant; if the government wants to analyze it in a particular way, it must get a warrant for that specific purpose.

IV. WHEN THE SEARCH OF METADATA BEGINS: A FRAMEWORK FOR ANALYSIS

To pinpoint when a search of historical metadata begins, and at what point the government must acquire a warrant to analyze that data, an analytical framework is necessary for determining when an invasion of privacy occurs. While *Carpenter* does not enumerate all the types of private information that the Fourth Amendment protects (nor does this Note attempt to do so), it does provide the basic framework for analyzing when the search of metadata begins.

A. Identifying the Information Sought

The first step in determining at what stage of surveillance a search of metadata begins is to determine what is ultimately being sought by law enforcement. Two possibilities are that law enforcement is after (1) the metadata itself, or (2) the information produced by analyzing that metadata.

Using an acquisition-based model, one would have expected the *Carpenter* Court to have asked whether Carpenter had a reasonable expectation of privacy in his CSLI itself because that was what the government acquired from Carpenter's wireless-network provider. But the Court did not phrase its question in those terms. Instead, it asked whether Carpenter had a reasonable expectation of privacy in the whole of his physical movements.[182] This question is striking because it is focused on the information—Carpenter's historical location over a period of time—that results from the government's analysis, not the raw metadata. The Court's phrasing suggests that Carpenter's privacy was infringed upon (and thus the search began) not when the government acquired his raw CSLI metadata, but when the govern–ment's analysis of his CSLI yielded information about the whole of his physical movements.[183]

This result-oriented approach makes sense for two reasons. First, determining whether unanalyzed CSLI is protected by a reasonable expectation of privacy is an abstract and difficult inquiry. Most physical privacy concerns are intuitive, but generally this is not the case in the digital context. For most people, the idea of law enforcement acquiring a set of numbers generated by their cell phones is not as worrisome as law enforcement entering their homes without permission. Home invasion is concrete; numbers are abstract. Metadata's abstraction is

182. *Id.* at 2217.

183. *Id.* at 2218–19.

likely responsible for most people's (including the judiciary's) lack of understanding about what information can actually be gleaned from those numbers. That lack of understanding, in turn, blurs the line between privacy in the traditional sense and privacy in the modern, digital era.

Second, most metadata can be analyzed in various ways to produce different types of information, not all of which may be subject to the same expectations of privacy.[184] For example, the CSLI generated when one makes a call typically includes the date and time the call was initiated, the phone numbers of the persons making and receiving the call, and the Cell ID of the cell sites to which the phone is connected.[185] This information can be analyzed to show the historical location of the cell-phone user and all the people that user called.[186] While the *Jones* and *Carpenter* Courts held that people have a reasonable expectation of privacy in the whole of their physical movements, in *Smith v. Maryland*, the Court held that individuals do not have a reasonable expectation of privacy in the telephone numbers they dial.[187] So although CSLI used to determine a user's location is protected by the Fourth Amendment's warrant requirement, that same metadata is not protected if it is used to determine the user's network of associations.

Asking what information is being sought as a result of metadata analysis remedies both problems. It is a concrete inquiry informed by years of social expectations upon which we can make the determination about whether metadata is subject to and protected by a reasonable expectation of privacy. It also allows us to distinguish between permissible and impermissible uses of metadata. Based on the *Carpenter* Court's phrasing, the government is free to collect and store raw metadata, but it must acquire a warrant if it hopes to analyze that metadata to glean information that is subject to a reasonable expectation of privacy.

B. Determining Whether That Information is Subject to a Reasonable Expectation of Privacy

The second step in determining at what stage of surveillance a search of metadata begins is to determine whether the information sought by the government is subject to a reasonable expectation of privacy and, therefore, protected by the Fourth Amendment. The *Katz* test asks whether a person has both a subjective and objective expectation of privacy in the thing being searched.[188] "The first part of the

184. Berman, *supra* note 26, at 590.

185. *See supra* Part I.B.

186. Tart et al., *supra* note 48, at 185.

187. Smith v. Maryland, 442 U.S. 735, 742 (1979).

188. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Katz test requires only that [a person] have exhibited an expectation of privacy—in other words, that his conduct [has] demonstrated an intention to keep [his] activities and things . . . private, and that he did not knowingly expose them to open view of the public."[189] But the Supreme Court's decisions leading up to *Carpenter* have raised doubt regarding whether a defendant's subjective expectations are relevant in determining whether a defendant's expectation of privacy is a reasonable one. In the Court's cases leading up to *Carpenter*, it seems to have abandoned or give serious consideration to the subjective prong.[190] The *Carpenter* majority, too, declined to consider Carpenter's subjective expectations, indicating that this oft-recited requirement is no longer relevant.[191]

The second part of the *Katz* test—whether the expectation of privacy at issue is "one that society is prepared to recognize as 'reasonable'"[192]—is more complex. In *United States v. White*,[193] Justice Harlan explained that "[t]his question must . . . be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[194] He went on to explain that "intrusions that significantly jeopardize the sense of security which is the paramount concern of Fourth Amendment liberties" are subject to Fourth Amendment protection.[195] This determ–ination largely depends on judges' normative values.[196] But the *Carpenter* and *Jones* Courts have taken steps to ground that inquiry by emphasizing that Fourth Amendment protection should be based on

189. LAFAVE, *supra* note 143, § 2.1(c).

190. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113, 115 (2015) (explaining that the subjective requirement has largely become "phantom doctrine"); *see also Kyllo*, 533 U.S. at 32–35 (reciting the two prongs of the reasonable-expectation-of-privacy test, but only applying the objective prong); *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) (same); *id.* at 423 (Alito, J., concurring) (quoting the *Katz* majority's holding without mentioning Justice Harlan's subjective requirement); *Riley*, 573 U.S. at 381 (not mentioning the subjective requirement and declaring simply that "the ultimate touchstone of the Fourth Amendment is 'reasonableness'").

191. *Carpenter*, 138 S. Ct. 2206.

192. 389 U.S. at 361 (Harlan, J., concurring).

193. 401 U.S. 745 (1971).

194. *Id.* at 786 (Harlan, J., dissenting).

195. *Id.* at 786–87.

196. Freiwald & Smith, *supra* note 38, at 221.

"historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'"[197]

And so, if a judge finds that a defendant's expectation of privacy does not satisfy the *Katz* test, the government would not need a warrant to analyze the defendant's metadata—the analysis would reveal only unprotected information. But if a judge determines that the information is subject to Fourth Amendment protection, the government must acquire a warrant prior to such analysis.

C. An Exception to the Result-Oriented Model and How the Third-Party Doctrine Applies

The *Carpenter* Court held that the third-party doctrine is not applicable to CSLI because CSLI is not truly voluntarily shared by a cell-phone user, rather it is generated purely as a function of using a cell phone.[198] But the Court conflated the claim that a cell-phone user voluntarily shares raw metadata by agreeing to a cell-phone contract with the more dubious claim that a cell-phone user voluntarily shares the whole of her physical location just by using her cell phone. By signing a cell-phone contract, users consent to their network providers both collecting phone-use metadata and using that metadata for various, vaguely phrased purposes enumerated in the contract.[199] But because no cell-phone contract informs a cell-phone user that their cell phone's metadata can be recorded and analyzed, a user cannot be said to have voluntarily shared that information.[200] It follows that the government may collect and store raw, unanalyzed metadata without a warrant because that metadata is subject to the third-party doctrine; but it may not analyze that metadata to reveal information that was not voluntarily revealed because the third-party doctrine does not apply to that information.

Most metadata about a particular person is generated and stored by third parties, but in the rare case the metadata is collected by the individual whom the data concerns—and is stored on her private servers—the search would begin when the government acquires that

197. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (alteration in original) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

198. *Id.* at 2220.

199. The terms of cell-phone contracts acknowledge that the wireless-network provider collects metadata from cell phones and uses it for various business purposes, but those uses do not include a surveillance-type analysis of that data that may reveal the whole of a person's historical movements or her network of associations. As such, it is problematic to suggest that the user has voluntarily shared this information and that she is subject to disclosure under the third-party doctrine. *See supra* notes 39–40 and accompanying text.

200. *See supra* notes 39–40 and accompanying text.

data. In this situation, the third-party doctrine simply does not apply, even to the raw metadata, because the information has not been shared with a third party. Furthermore, although the information in question is stored digitally, it is stored in a private space, and intruding into that space would constitute an invasion of an individual's traditional trespass-based right to privacy.[201]

V. WHAT THE WARRANT MUST CONTAIN

If a Fourth Amendment search of metadata begins when it is analyzed to reveal meaningful information, it is necessary to reinterpret the warrant requirements—what it means to "particularly describ[e] the place to be searched, and the persons or things to be seized"[202]—in the context of metadata. First, when analyzing metadata, there is often no physical "place" or "thing" *where* the search occurs. Nevertheless, some*thing* is being searched. Traditionally, the place to be searched presumably contains the subject of the search. The same is true for metadata. Just as one enters a house through the front door, one "enters" metadata through analysis.

Second, "things to be seized" must be similarly interpreted to include the private information sought by analyzing the metadata. In recent years, courts have frequently interpreted digital information to fall within the scope of the Fourth Amendment. In 2010, the Sixth Circuit described email as "the technological scion of tangible mail."[203] In 2014, the Supreme Court in *Riley v. California*[204] held that the police, without a warrant, may not search the contents of a cell phone belonging to a person in police custody.[205] The Court compared search–ing the digital contents of a cell phone to "rummag[ing] at will among a person's private effects."[206] Understanding "things to be searched" to include categories of private information that can be generated by analyzing metadata is only the next step in the evolution of the Fourth Amendment in the modern electronic age.

In sum, a warrant acquired to analyze metadata in a way that will likely reveal information subject to Fourth Amendment protection must particularly describe both the metadata to be analyzed and the private information to be seized.

---

201. United States v. Jones, 565 U.S. 400, 409 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in original).

202. U.S. CONST. amend. IV.

203. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

204. 573 U.S. 373 (2014).

205. *Id.* at 403.

206. *Id.* at 399 (quoting Arizona v. Gant, 556 U.S. 332, 345 (2008)).

CONCLUSION

Technology is evolving at a rapid pace, and with it the government's surveillance capabilities. "[A]s late as 1900, [law enforcement] involved little more than an able-bodied man who was given a hickory club, a whistle, and a key to a call box."[207] Today, law enforcement can click a button and, through metadata analysis, retroactively surveil anyone who uses technology. Determining that a Fourth Amendment search begins when the government analyzes meta–data, rather than when it acquires that data, is the best means of protecting the privacy and security guaranteed by the Fourth Amend–ment.

It is true that this result-oriented framework is broad and would require the government to seek a greater number of warrants when conducting historical metadata-based surveillance. But the result-oriented framework is crucial if the Fourth Amendment is to adequately protect people from an improper governmental search. Under this approach, individuals would retain their privacy interest in information that might otherwise be revealed by analyzing their metadata because the government would be required to apply for a new warrant for each different type of protected information it seeks—even after the police legally acquired that metadata.[208] Only after obtaining a new warrant could the government aggregate and reaggregate metadata to reveal additional private information protected by the Fourth Amendment. For, as Justice White observed in *United States v. Karo*,[209] "[t]he argument that a warrant requirement would oblige the government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement."[210] Indeed, this increased burden is required to preserve the security and privacy of individuals against unreasonable government invasion; and it is a small price for law enforcement to pay in exchange for access to citizens' personal information that is inexpensive, "effortlessly compiled,"[211] and "other–wise unknowable."[212]

207. Joh, *supra* note 74, at 36.

208. *Cf.* Illinois v. Andreas, 463 U.S. 765, 771–72 (1983) (explaining how the plain-view doctrine normally permits objects lawfully within police possession to be searched because the privacy interest has already been lost).

209. 468 U.S. 705 (1984).

210. *Id.* at 718.

211. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

212. *Id.* at 2218.

-Geneva Ramirez[†]

† J.D. Candidate, 2020, Case Western Reserve University School of Law. The author would like to thank Professor Emeritus Jonathan L. Entin for his thoughtful comments and encouragement throughout the writing of this Note. Additional thanks to Orin Kerr who graciously shared with me his early incites about *Carpenter*, which inspired this Note.