January 2022

Putting Together the Pieces: The Mosaic Theory and Fourth Amendment Jurisprudence since Carpenter

Ben Vanston
West Virginia University College of Law

Follow this and additional works at: https://researchrepository.wvu.edu/wvlr

Part of the Constitutional Law Commons, Criminal Law Commons, Criminal Procedure Commons, and the Fourth Amendment Commons

Recommended Citation

This Student Note is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact researchrepository@mail.wvu.edu.
I. INTRODUCTION

If someone could follow your every move for seven days, what could that person figure out about you? Could this person find out your hobbies? What you do for a livelihood? Your address? Maybe even the identities of your friends and family? As smartphones, wearable technology, and a vast array of other increasingly complicated technological devices become commonplace in the United States, so too does it become easier to track where you go and figure out...
who you are. In a day not so long ago, law enforcement, through traditional investigatory techniques, could have been able to pin together a case over time and make an educated guess at a citizen’s most personal information. Now, with non-physical surveillance technology, the days of guessing may be coming to a close.

The “digital age” has ushered in an era that has changed our world for the better, making problems from the past almost unrecognizable to the average member of Generation Z. The ability to communicate with other people around the world has never been more robust. A contemporary example of removing barriers of communication would be the ability for many to have meetings, go to school, and work from home during the COVID-19 pandemic, which could have even more sharply affected everyone’s lives had it not been for telecommunications technology. However, exponentially increasing technological development comes at a cost. Privacy, both in the public and private sphere, is a main concern of this rapidly developing technological landscape. Concerns about the protection of user-privacy have renewed interest among policymakers and activists alike, both in the United States and worldwide.

1 S. O’Dea, Number of Smartphone Users from 2016 to 2021, STATISTA (Aug. 6, 2021), https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/#:~:text=The%20number%20of%20smartphone%20users,mark (showing the number of total cell phones used worldwide increasing from 1.06 billion in 2012 to 6.4 billion in 2021 and projecting 7.5 billion cell phones used worldwide by 2026).


3 See Marc Chase McAllister, GPS and Cell Phone Tracking of Employees, 70 Fla. L. Rev. 1265, 1313–17 (2018) (demonstrating the potential for employers to use cell phone apps to track the location of its employees); Ifeoma Ajunwa, Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, 63 St. Louis U. L.J. 21 (2018) (documenting the implementation of productivity monitoring software applications and wearable technology in the workplace, and arguing there are serious privacy implications with such use); Harvey Gee, Almost Gone: The Vanishing Fourth Amendment’s Allowance of Stingray Surveillance in a Post-Carpenter Age, 28 S. Cal. Rev. L. & Soc. Just. 409, 431–36 (2019) (discussing the erosion of Fourth Amendment rights, specifically in the context of “Stingray” technologies, which operate as a fake cell tower to “trick cell phones in the area into transmitting their locations and identifying information”). For an in-depth look at the socioeconomic factors which can affect “expectations of privacy,” see Stephanie L. Williams, The Haves and Have Nots: Wealth-Based Expectations of Privacy in Fourth Amendment Jurisprudence, 45 N. Ky. L. Rev. 67 (2018).

The use of technology in law enforcement, generally, is a concerning matter as well. Law enforcement is able to take advantage of new-fangled technologies to adjust investigatory techniques, revealing more information than ever before. Specifically, non-physical forms of surveillance, like cell site location information ("CSLI"), can be used in ways that can track a person’s movements, especially when traveling long distances. However, the precision and accuracy of technologies of this type is somewhat disputed. However, it is undisputed that non-physical surveillance technology has changed the dynamic of policing in the United States, and if it is available as an investigatory tactic, law enforcement will use it. Such use by law enforcement calls into question how and to what extent the Fourth Amendment should protect citizens from non-physical surveillance technology and whether these are "searches" within the meaning of the Fourth Amendment.

This Note examines how the lower courts have interpreted Fourth Amendment cases since Carpenter v. United States, specifically how these courts have implemented an interpretation of the mosaic theory and in what contexts. As technological change has become commonplace, there should be a broadly outlined standard for how Fourth Amendment rights are implicated in light of Carpenter. In turn, this will allow lower courts to define the mosaic theory moving forward, and more effectively adjudicate determinations of defendants’ rights in the digital age. First, this Note will discuss the basic doctrinal understanding of Fourth Amendment searches. Next, it will discuss the third-party doctrine and the Supreme Court’s decision in Carpenter v. United States. Then, this Note will discuss and analyze how the lower courts have reacted to Carpenter in its jurisprudence. Finally, this Note will put forth a proposal to best reconcile how Fourth Amendment jurisprudence involving non-physical surveillance technology should be handled in the wake of Carpenter.

---

6 The consensus is that CSLI can reveal sensitive information about an individual’s location, and courts routinely handle it as such. See Carpenter v. United States, 138 S. Ct. 2206 (2018). However, some commentators have raised questions about the propriety of relying on it for precise location. GPS location, which is now available for most, if not all, smartphones and other wearable technology, such as Apple Watches, are considered substantially more accurate. The Two Towers: The Abuse of Mobile-Phone Data, THE ECONOMIST, (Sep. 6, 2014), https://www.economist.com/united-states/2014/09/06/the-two-towers.
II. FOURTH AMENDMENT JURISPRUDENCE SINCE KATZ AND THE MOSAIC THEORY

The Supreme Court’s interpretation of the scope and meaning of the Fourth Amendment has perhaps been its most volatile doctrine, ranging from a traditional property rights-based analysis to a consideration of normal citizens’ privacy expectations. The overarching standard for most Fourth Amendment determinations of whether a “search” has taken place is dependent upon the Katz test; however, in recent years, the Court has complicated this assumption. Since the formulation of the Katz test, the Fourth Amendment has been understood to encompass an evolving standard that conforms with society’s reasonable expectations of privacy. In Part A, this author will briefly summarize what is and is not a “search” under the Fourth Amendment. Next, in Part B, this author will briefly summarize the third-party doctrine, an exception to the warrant requirement under the Fourth Amendment. Finally, in Part C, this author will summarize the “mosaic theory” and Carpenter v. United States.

A. What Is A “Search” Under the Fourth Amendment?

The Fourth Amendment proscribes that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” It further elaborates that no “warrants” for searches or seizures shall be issued “but upon probable cause.” The term “search” within the meaning of the Fourth Amendment is a complete

---

8 There are, generally, two different historical periods for Fourth Amendment jurisprudence. The former was marked by a property rights-based analysis of the Fourth Amendment. A violation of the Fourth Amendment would only occur “when law enforcement “inv[ades]... private property, be it ever so minute....” See Boyd v. United States, 116 U.S. 616, 627 (1886) (quoting Entick v. Carrington, 18 Howell St. Tr. 1029, 1066 (1765) (Eng.)). The second period is characterized by the Katz test. See generally Katz v. United States, 389 U.S. 347 (1967).

9 Compare Katz, 389 U.S. at 361 (Harlan, J., concurring) with United States v. Jones, 565 U.S. 400 (2012) (holding for the first time since Katz that property law principles were still applicable to the Fourth Amendment).

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


12 U.S. CONST. amend. IV.

13 Id. “‘Probable cause’ is a concept that is imprecise, fluid, and very dependent on the context.” Probable Cause, LEGAL INFO. INST., https://www.law.cornell.edu/wex/probable_cause (last visited Nov. 19, 2021). The Supreme Court has held that a flexible approach should be used by lower courts when determining probable cause, using a “practical, non-technical” standard which takes into account the “factual and practical considerations of everyday life on which reasonable and prudent men . . . act.” Illinois v. Gates, 462 U.S. 213, 231 (1983) (citation omitted).
term of art. Thus, the word search, in this context, does not mean "looking for something." Rather, it refers to a specific moment in time where the police have breached the reasonable expectation of privacy and now have an intimate view of a private citizen's person, place, or effect.

During an investigation, the police may search a person's belongings when they have ascertained probable cause and have gotten a warrant approved by a magistrate. However, there are several situations—called exigent circumstances, essentially emergency situations—where warrants are not required. The Supreme Court has deemed such searches reasonable within the meaning of the Fourth Amendment; thus, these searches are constitutional.

The problem traditionally arises when law enforcement conducts a search without previously acquiring a warrant, and there are no applicable exigent circumstances. The 

14 See Joshua Dressler, George C. Thomas III, & Daniel Medwed, Criminal Procedure: Investigating Crime (6th ed., 2006). However, where the Fourth Amendment hinges on the "reasonableness" of the search, or whether it requires a warrant has been an ideological dispute on the Court for the past several decades. See Cynthia Lee, Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis, 81 Miss. L.J. 1133, 1156 (2012) (discussing critiques of "reasonableness" from the political "left," stating "[t]he problematic nature of open-ended reasonableness standards has led some feminist scholars to argue in favor of more subjective standards over purportedly neutral objective ones").


17 See Dressler et al., supra note 14.


19 Exigent circumstances have been defined by the 9th Circuit as "circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984), overruled on other grounds by Estate of Merchant v. Comm'r, 947 F.2d 1390 (9th Cir. 1991). Additionally, police may be able to use the exigent circumstances exception even when there is a mistake. Kentucky v. King, 563 US 452, 463 (2011) (holding that the exigent circumstances rule applies when police do not gain entry to a premises by means of actual or threatened violation of the Fourth Amendment). Finally, the Court has found that the exigent circumstances exception "almost always" applies when police do a warrantless blood test to an unconscious driver suspected to be under the influence because a less-invasive breath test would be impossible. Mitchell v. Wisconsin, 139 S. Ct. 2525, 2531 (2019). However, the Court previously held that the "natural metabolization of alcohol in the bloodstream" does not present a per se exigency that creates an exigent circumstance; instead, exigency in cases where police are looking to obtain a blood-test for alcohol content should be "determined case by case based on the totality of the circumstances." Missouri v. McNeely, 569 U.S. 141, 145 (2013).
(subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”20 The Katz test is employed in a sequential way, meaning that the “courts take a snapshot of the [interaction with law enforcement] and assess it in isolation.”21 Courts have referred to this process as “inherent” when evaluating the Fourth Amendment.22 As Professor Kerr states, the Supreme Court has articulated “each ‘particular governmental invasion’” of expectations of privacy, “starting with the ‘initial’ step and then separately analyzing the ‘subsequent’ steps.”23 Thus, the sequential analysis comes into play when law enforcement shows conduct violative of an individual’s “reasonable expectation of privacy . . . [such as] break[ing] into a private, enclosed space, [ ] a home, a car, a package, or a person’s pockets.”24 Importantly, the sequential analysis is also followed when remedying Fourth Amendment rights violations.25 “Remedies apply only if the unconstitutional act caused the discovery of a specific piece of evidence.”26 Therefore, when law enforcement discovers a piece of evidence during an invalid search, that evidence will be excluded from the trial upon the finding of a Fourth Amendment violation. However, that does not preclude evidence previously found during a valid search from being included in the criminal trial. For example, if the arresting officer has validly arrested you based on probable cause, he may search your person and find evidence of criminal activity.27 However, this does not give the officer the right to search through your car once you have been detained, and if he finds any further evidence in there, it may be excluded.28

20 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). To some extent, that Katz test itself is misleading. Scholars have noted through empirical studies that the first prong of the test, whether an individual has an actual or subjective expectation of privacy, has almost been completely ignored by courts when deciding Fourth Amendment questions. See generally, Orin S. Kerr, Katz Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113 (2015) (arguing that the vast majority of courts, including on occasion the Supreme court, do not consider the first step of the Katz test when conducting an analysis of Fourth Amendment “searches”). This is ironic, mostly because the holding in Katz itself relied so heavily on the fact that the suspect had a reasonable expectation of privacy in conducting a conversation within a phone booth. Katz, 389 U.S. at 361 (Harlan, J., concurring).

21 Kerr, supra note 16, at 315.

22 United States v. Beaudoin, 362 F.3d 60, 70–71 (1st Cir. 2004).

23 Kerr, supra note 16, at 316 (citing Terry v. Ohio, 319 U.S. 1, 19 (1968); United States v. Dionisio, 410 U.S. 1, 8–9 (1973)).


26 Id. (citing Hudson v. Michigan, 547 U.S. 586, 590–94 (2006)).


Moreover, it follows that any evidence thereafter found is "fruit of a poisonous tree," which dictates that any evidence found as consequence of a unconstitutional search shall be excluded.29

B. The Third-Party Doctrine

The third-party doctrine is arguably the most substantial exception to the Fourth Amendment’s warrant requirement.30 At base, the third-party doctrine states that a person has no reasonable expectation of privacy when her or she discloses information voluntarily to a third-party.31 A classic hypothetical is that if Person A and Person B are friends and communicate frequently, there is some degree of trust between them. If Person A tells Person B a secret, that he is illegally dealing drugs, then he has opened his so-called “circle of trust”32 to Person B. If Person B then turns around and offers that information to law enforcement agents, breaking the circle of trust, Person A cannot suppress evidence of the conversation because Person A had been the one who voluntarily disclosed that he dealt drugs to Person B in the first place.33

The third-party doctrine took on substantial new meaning post-Katz in United States v. White, which expanded the third-party doctrine to conversations with informants that were recorded on a hidden device.34 During the investigation, law enforcement did not pursue a warrant for the informant to

---

32 Credit to Professor John E. Taylor for the term “circle of trust,” which he used quite frequently during our Criminal Procedure class. John E. Taylor, Lectures on Criminal Procedure, delivered during his Criminal Procedure: Investigation course taught at West Virginia University College of Law in the fall of 2019.
33 Id.
34 401 U.S. 745, 749 (1971). Notice the mirroring of the Katz test language—emphasizing a “reasonable expectation” of privacy. The White decision largely rested on Hoffa v. United States, 385 U.S. 293 (1966), which held “however strongly a defendant may trust a colleague, his expectations of confidentiality are not privileges when the colleague flips on him to the police.” As one scholar has noted, the Court’s distinction with the third-party doctrine seemingly turns on whether the “eavesdropper” is visibly present to the criminal defendant:

The law treats secret surveillance of speech or other behavior largely according to whether the surveilling agent is visible or invisible to the subject. An agent, visibly present through masquerading [as a confidant], is thought to gather evidence in a fundamentally different manner than a concealed agent or a hidden electronic device. The theory is that the contents of the mind, deliberately revealed to another person, are willingly shared, while the secret eye or ear, possibly electronically enhanced, bypasses constitutional concern to spirit the evidence away.

record the suspect’s conversations via a concealed listening device. The Court held that a warrant was not necessary to authorize this type of informant surveillance. Rather, the Court reasoned that the law permits the frustration of actual expectations of privacy by associates, or “fake friends,” when those associates divulge their conversations to law enforcement. Thus, the analysis does not change when the “fake friend” is concealing a recording device that secretly documents the actual conversations.

The Court has held that the third-party doctrine is applicable to several different scenarios, always involving a criminal suspect voluntarily disclosing information which eventually ends up in the hands of law enforcement. Many of these expansions are fairly analogous to our original hypothetical, as well as United States v. White. In these “circle of trust” scenarios, a suspect tells another individual (who may be undercover law enforcement) incriminating information. That other individual hands over that information to law enforcement by recording their conversations, giving law enforcement access to the place of conversation, or otherwise assisting law enforcement. This is an important and legitimate tool for law enforcement to deploy. Law enforcement activities would be significantly hindered if it was not allowed to utilize the probative value of individuals who have turned “state witness” or are covert law enforcement agents. For example, it would be extremely difficult to prevent inchoate crimes from coming to fruition if all information conveyed to law enforcement by third parties were deemed an invasion of an objective expectation of privacy.

However, the Supreme Court has also allowed the third-party doctrine to encompass areas that are fairly unanalogous to the “circle of trust” hypothetical from above. In Smith v. Maryland, the Court held the third-party doctrine applies to commercial transactions voluntarily entered into by criminal defendants. There, law enforcement, without a warrant, requested that a telephone provider place a pen register on a suspect’s incoming and outgoing

---

35 White, 401 U.S. at 746–47.
36 Id. at 753–54.
37 Id. at 752.
38 Id. at 754. This Author uses the term “fake friend” or “fake friends” to refer to an individual who is working with law enforcement as a confidential informant.
39 See id. at 745 (where a household owner allowed a government agent to hide in the kitchen closet with a recording device while having incriminating conversations with suspect; Hoffa v. United States, 385 U.S. 293, 295–96 (1966) (where law enforcement placed an agent, who defendant conveys incriminating information to under the guise of being a “false friend”); Lopez v. United States, 373 U.S. 427, 430–31, 439 (1963) (where a “false friend,” wearing a concealed tape recorder, recorded conversations with suspect and conveyed the information to law enforcement); Lee v. United States, 343 U.S. 747, 750–57 (1952) (decided on different grounds, pre-Katz, but involved a “false friend” wearing a wire transmitter which conveyed a conversation with a criminal suspect to law enforcement).
calls, to which it complied. The Court held that a warrant was not required because the telephone company's placement of the pen register satisfied the third-party doctrine. In its reasoning, the Court emphasized a lack of the petitioner's subjective expectation of privacy at the telephone company's facilities. Additionally, the pen register would not be able to "listen in" on the conversations the defendant's phone would transmit; it would only transmit the telephone numbers conveyed. This type of information is frequently conveyed to telephone companies, as an individual would be unable to place a call without "expos[ing]" that information to [the telephone company's] equipment in the ordinary course of business. Thus, "petitioner assumed the risk that the company would reveal to police the numbers he dialed."

Justice Marshall's dissent in Smith v. Maryland highlights several considerations and questions about whether individuals would have a reasonable and objective expectation of privacy in their commercial transactions. Justice Marshall questions the reasoning that individuals would expect information for business purposes to be disclosed "to other persons for other purposes." Furthermore, Justice Marshall questions whether one could truly "assume the risk," or "open up their circle of trust," when dealing with an entity that provides what many people would consider to be an essential service in the modern world. Justice Marshall concludes that he would not expand the third-party doctrine to transactions of a commercial nature.

Since the third-party doctrine first appeared in United States v. Miller and Smith v. Maryland, it has been used to warrantlessly request that third parties convey business records to aid in law enforcement investigations. This can

---

42 Id. at 737.
43 Id. at 743 (stating, "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one society is prepared to recognize as reasonable") (internal citation omitted).
44 Id. at 742. The pen register had never been placed on the defendant's property; rather, it had been placed at the headquarters of the telephone company. Id.
45 Id. at 741–42.
46 Id. at 744 (citing United States v. Miller, 425 U.S. 435, 442 (1976)).
47 Id.
48 Id. at 749 (Marshall, J., dissenting) (stating "[e]ven assuming, as I do not, that individuals 'typically know' that a phone company monitors calls for internal reasons, . . . it does not follow that they expect this information to be made available to the public in general or the government in particular.").
49 Id.
50 Id. at 750 (comparing the voluntariness of letting a single individual, or group of individuals, into your circle of trust with "forego[ing] use of what for many has become a personal or professional necessity. . ."). This quote resonates to a greater degree 42 years later.
51 Id. at 752.
52 United States v. Miller, 425 U.S. 435 (1976) (holding that defendant had no protected Fourth Amendment interest in banking records voluntarily conveyed to bank officers).
include banks, phone companies, internet service providers, and e-mail servers. Regardless of what light one sees the third-party doctrine in, it is hard to avoid the reality that Justice Marshall's concerns in 1979 resonate even more today. More controversially, it became apparent that some courts viewed CSLI data as falling under the third-party doctrine. The nature of growing cell phone usage in the United States, and worldwide, forced the Court to reconcile its loyalty with the third-party doctrine to a fundamentally different technological landscape. In two cases, the Supreme Court tweaked the third-party doctrine, specifically as it applied to CSLI data, which ensured broader protection for individuals under the Fourth Amendment.

C. The Mosaic Theory of the Fourth Amendment and Carpenter

The mosaic theory of the Fourth Amendment is a different analysis than under the "sequential" approach. Rather than seeing law enforcement interactions as a step-by-step approach, the mosaic theory views these interactions as a collective whole. If the government conducts a substantial amount of "non-searches," when those pieces are added together, a court may find that a search has been conducted when viewing the entire ordeal from the aggregate. Thus, the mosaic theory fundamentally changes the court's analysis in regard to a Fourth Amendment violation. Rather than viewing a government interaction in isolation, and whether that interaction invaded a reasonable expectation of privacy, a court instead would scrutinize the duration of the interaction.


The mosaic theory first appears in Fourth Amendment jurisprudence in United States v. Jones, which invalidated the use of a "beeper" on a vehicle to track a suspect for 24-hours on public roads. The Court unanimously decided

53 See, e.g., id. (holding that the third-party doctrine applies to information voluntarily conveyed to bank officers); Smith v. Maryland, 442 U.S. 735 (1979) (holding that the third-party doctrine applies to information voluntarily conveyed to telephone companies); United States v. Trader, 981 F.3d 961, 968–69 (11th Cir. 2020) (holding that the third-party doctrine applies to email and IP address information conveyed to law enforcement through messaging app).

54 With access to CSLI data, the government would not only have access to information which the voluntary disclosure of is questionable but through the nature of cell phone usage would be fundamentally different.

55 Kerr, supra note 16, at 320.

56 Id.

57 565 U.S. 400 (2012). A "beeper" is a device that can track the location of an individual by attaching to a vehicle, or other object. Such devices have been used for a significant amount of time in law enforcement and have consistently presented Fourth Amendment issues. See Clifford S. Fishman, Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered, 34 CATH. U.L. REV. 277, 282 (1985).
that the case presented a violation of the defendant’s reasonable expectation of privacy; however, the Court could not agree on why. Justice Scalia, writing for the majority, reintroduced trespass principles to the Court’s analysis of the Fourth Amendment, holding that the installation constituted a trespass on private property. In Justice Sotomayor’s concurrence, however, she mainly focused on the potential that non-physical surveillance has to violate subjective and objective expectations of privacy, rather than focusing on the trespass and physical intrusion, as the majority did. Thus, for situations involving surveillance without a physical intrusion, as in Jones, the majority’s test would “provide little guidance.” Therefore, Justice Sotomayor concluded that “[she] would take [the special circumstances] of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements.” It should also be noted that while writing separately, Justice Alito reaches the same conclusion, stating, “I would analyze the question presented in this case by asking whether respondent’s reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.” Thus, both concurrences are uneasy about the utilization of non-physical surveillance technology in conjunction with citizens’ Fourth Amendment rights.

2. Cell-Site Location Information (“CSLI”)

Before discussing Carpenter v. United States and its reasoning, it is important to have a basic grasp on how CSLI works and how that, in turn, relates to the third-party doctrine. At base, “cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called ‘cell sites.’” Cell sites are usually attached to a large tower, but are scattered throughout more urban areas on buildings, telephone poles, light posts, and other similar fixtures. In order to function properly, cellular phones continuously search an

58 Jones, 565 U.S. at 400.
59 Id. at 404.
60 Id. at 415.
61 Id.
62 Id. at 416.
63 Id. at 417.
64 Id. at 419 (Alito, J., concurring) (emphasis added).
66 Id.
environment in order to obtain the best possible signal from a cell site. Cellular phones, depending on the manufacturer and type, can perform this function up to several times a minute, even when the owner is not consciously using the device.

"Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)." The precision of this system to track the location of the cellular phone user varies widely with the concentration of cell sites within a given area. In rural areas, for example, the nearest cell site may be several miles away. In a more concentrated, urban area, the nearest cell site may be a matter of yards. However, if multiple cell towers record information, law enforcement can "triangulate" the signal and locate a phone with much greater precision—sometimes within five to ten feet.

Wireless carriers collect and store CSLI for their own business purposes, mostly utilizing it to update their own networks to figure out where "weak spots" in wireless coverage exist. Additionally, businesses utilize CSLI to apply "roaming" charges to a customer's bill when the customer is using the cellular phone out-of-network. CSLI has been tracked since cellular phones first entered the market, mostly when incoming calls were placed and now text messages; however, given the vast array of functions, apps, and services that a modern smartphone provides, most cell phones are continuously pinging into a cell site when it is turned on. Thus, this can generate a "map" of where the cellular phone user has been, regardless of what the user is doing, as long as the cellular phone is turned on and is on their person. Because documenting the

---

67 Id. Currently, there are several "cellular" phone and smart phone providers which allow the user to turn off "cell data" usage. Turning off this function will stop the phone from connecting to a cell site. The phone can still be functional using Wi-Fi. However, when the phone is out of range for a Wi-Fi network, it is essentially useless for calls, interaction apps, the internet, or other functions which require connection. However, local functions, such as using the calculator or looking at your calendar, remain operational.

68 Id.

69 Id.

70 See Alexandra C. Smith, Pinging into Evidence: The Implications of Historical Cell Site Location Information, 120 W. Va. L. Rev. 331, 335 (2017).

71 See Carpenter, 138 S. Ct. at 2225 (Kennedy, J., dissenting).


73 Carpenter, 138 S. Ct. at 2212.

74 Id.

75 Id.

76 While Carpenter is constrained to discussing cellular phones, an important development to consider is the introduction of the Apple Watch 5 and other similar devices. The original Apple Watch acted as a "mirror" of the cell phone screen, and thus, could only operate in conjunction with the user's cell phone. The cellular phone was required to be within 15 feet in order for the Apple Watch to operate properly. However, the newer Apple Watch 5 has the ability to make calls,
cellular phone’s location through CSLI is voluntary information disclosed to a manufacturer, it would typically fall under the third-party doctrine.77

3. Carpenter v. United States

Carpenter v. United States was the first case to consider the implications of CSLI in conjunction with the third-party doctrine.78 The case involved fifteen accomplices, including Timothy Carpenter, who conspired to rob nine different store locations in Michigan and Ohio.79 Based upon information gathered from conspirators-turned-informants, law enforcement authorities discovered the cellular phone number of Carpenter.80 Law enforcement then proceeded to apply for court orders under the Stored Communications Act to obtain cell phone records for Carpenter, as well as several other suspects implicated by the informant.81 The Stored Communications Act permitted “the Government to compel the disclosure of certain telecommunications records when it ‘offers specific and articulable facts showing that there are reasonable grounds to believe’ that the records sought ‘are relevant and material to an ongoing criminal investigation.”82 Notably, Carpenter argued that, regardless of the statute, the police needed to obtain a warrant support by probable cause in order to access the cell-site data.83 Using the CSLI, law enforcement was able to obtain 12,898 location points mapping out Carpenter’s movements over a 127 day time period.84 “Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence.”85 Carpenter then moved to suppress

send text messages, stream music, and keep track of your location while being away from your phone. Thus, the Apple Watch 5 is wearable technology which acts independent of a cellular phone and is also pinging into cell sites. This is also true for iPads and other tablets which use cellular data. See Use Apple Watch With a Cellular Network, APPLE, https://support.apple.com/guide/watch/use-your-apple-watch-with-a-cellular-network-apd9a168c68b/watchos (last visited Nov. 19, 2021).

78 Id. at 2206. Some courts considered warrantless collection of CSLI data to be valid under the Fourth Amendment; however, those lower courts had “questioned whether precedent about phone booths, pen registers, and microfilm provides an adequate framework for analyzing privacy expectations in the “smartphone” era. See, e.g., In re U.S. for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013), abrogated by United States v. Beverly, 943 F.3d 225 (5th Cir. 2019) (reasoning, in part, that “[CSLI] is clearly a business record. The cell service provider collects and stores historical cell site data for its own business purposes . . . .”).
79 Carpenter, 138 S. Ct. at 2212.
80 Id.
81 Id.
82 Id. (quoting 18 U.S.C.A. § 2703(d) (West 2021)).
83 Carpenter, 138 S. Ct. at 2212.
84 Id.
85 Id.
the CSLI because law enforcement’s seizure of the records were not obtained pursuant to a warrant supported by probable cause.\textsuperscript{86}

The Court started its analysis with \textit{Knotts}, which concluded that “‘augment[ed]’ visual surveillance did not constitute a search because ‘[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.’”\textsuperscript{87} This is because the movements of the vehicle had been “‘voluntarily conveyed to anyone who wanted to look,’” therefore, there was no privacy interest in the public movements.\textsuperscript{88} However, the Court noted some qualifying language distinguishing more traditional tracking methods from a broader, more substantial mode of surveillance.\textsuperscript{89} The Court also cited \textit{United States v. Jones}, standing for the principle that physical trespass to obtain 24-hour surveillance violated the Fourth Amendment, plus noting the two concurrences by Justice Sotomayor and Justice Alito.\textsuperscript{90}

The Court declined to extend \textit{Smith} and \textit{Miller}, holding that the third-party doctrine was inapplicable to cover the “novel circumstances” of 24-hour CSLI surveillance.\textsuperscript{91} The court concluded that law enforcement using its own technology, or leveraging the technology of a wireless carrier, was an invasion of an individual’s reasonable expectation of privacy in his physical movements.\textsuperscript{92} The Court reasoned that the immensely personal and probative value of such records, and CSLI data becoming “remarkably easy, cheap, and efficient compared to traditional investigative tools” made it a different beast than other applications of the third-party doctrine.\textsuperscript{93} The nature of cellular phones, and the accuracy of the location information made them “almost a ‘feature of human anatomy’ . . . track[ing] nearly exactly the movements of its owner.”\textsuperscript{94} At base, the Court viewed the nature of information disclosed through third-parties as a fundamentally different proposition.

The Court moved on to attack the second rationale for the third-party doctrine, the voluntariness of an individual’s exposure.\textsuperscript{95} The Court reasoned that CSLI data is never “shared” as an individual normally understands the term.\textsuperscript{96}

\textsuperscript{86} \textit{Id}.

\textsuperscript{87} \textit{Id.} at 2215 (citing \textit{United States v. Knotts}, 460 U.S. 276, 281–82 (1983)) (internal citation omitted).

\textsuperscript{88} \textit{Id.} (citing \textit{Knotts}, 460 U.S. at 281).

\textsuperscript{89} \textit{Id.} (citing \textit{Knotts}, 460 U.S. at 283–84) (noting that “different constitutional principles may be applicable if twenty-four-hour surveillance of any citizen of this country [were] possible”).

\textsuperscript{90} \textit{Id}.

\textsuperscript{91} \textit{Id.} at 2217.

\textsuperscript{92} \textit{Id.} at 2217.

\textsuperscript{93} \textit{Id.} at 2218.

\textsuperscript{94} \textit{Id.} (citing \textit{Riley v. California}, 573 U.S. 373, 385 (2014)).

\textsuperscript{95} \textit{Id.} at 2220.

\textsuperscript{96} \textit{Id}.
Rather, cellular phones have become ""a pervasive and insistent part of daily life.""\textsuperscript{97} Second, there is no voluntary, intentional step that a user does to activate CSLI tracking, beyond merely operating the phone.\textsuperscript{98} Rather than actively conveying information, such as conveying information to a bank about financial records; here, there is nothing a user could do to prevent the recording of this information outside of foregoing cellular phone usage. The Court concluded, ""in no meaningful sense does the user voluntarily ‘assume the risk’ of turning over a comprehensive dossier of his physical movements.""\textsuperscript{99} Therefore, the Court concluded as a whole that the warrantless access of CSLI from wireless carriers was a ""search"" within the meaning of the Fourth Amendment.\textsuperscript{100}

Based on this analysis of the issue, importantly, the Court did not articulate a standard for the use of CSLI data.\textsuperscript{101} Justice Roberts, writing for the majority, specified the narrowness of the holding, explicitly stating that the third-party doctrine is still good law and does not address other business records, or information collection techniques.\textsuperscript{102} Additionally, in a footnote, Justice Roberts specified that, for the purposes of Carpenter, ""it is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.""\textsuperscript{103} Some have purported that the test emerging from Carpenter indicates that lower courts should examine (1) ""the deeply revealing nature"" of the information being sought; (2) ""its depth, breadth, and comprehensive reach;"" and (3) ""the inescapable and automatic nature of its collection . . . .""\textsuperscript{104} The Court, in its conclusion, seemingly endorsed the mosaic theory of the Fourth Amendment; however, it does not explicitly state the proposition.\textsuperscript{105} Lack of an express

\textsuperscript{97} Id. (quoting Riley, 573 U.S. at 385) (noting that a cellular phone ""faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales"). The Court cites Riley v. California, 573 U.S. 373, 395 (2014), to show that ""nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."" The Court hammers home the broader point—it views cellular phones and law enforcement use of CSLI data as a different beast because of its particularly revealing nature. See Paul Ohm, The Many Revolutions of Carpenter, 32 Harv. J.L. & Tech. 357, 360 (2018) (stating, ""[r]ecent advances in information technology are different in kind, not merely in degree from what has come before . . . [this] has never before received such a profound endorsement from the Supreme Court").

\textsuperscript{98} Id.

\textsuperscript{99} Id.

\textsuperscript{100} Id. at 2219.

\textsuperscript{101} See generally id.

\textsuperscript{102} Id. at 2220–21 (""Our decision is a narrow one . . . [it do[es] not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras; Nor do we address other business records that might incidentally reveal location information. Further our opinion does not consider other collection techniques involving foreign affairs or national security.").

\textsuperscript{103} Id. at 2217 n.3.

\textsuperscript{104} Id. at 2223; Ohm, supra note 97.

\textsuperscript{105} See Carpenter, 138 S. Ct. 2206.
standard—in conjunction with a lack of guidance of how Carpenter should apply to analogous methods of non-physical surveillance—has left lower courts with a limited framework to apply the mosaic theory to other technologies.

III. THE MOSAIC THEORY POST-CARPENTER

Several lower courts have been left with an indeterminate line of where Carpenter extends and in what contexts. As the Court made clear in Carpenter, citizens have a reasonable expectation of privacy in their own CSLI, and the third-party doctrine is inapplicable. Despite some scholars’ optimism, lower courts have seemingly not taken an aggressive step, post-Carpenter, to extend its reasoning to other non-physical surveillance technology, the third-party doctrine generally, or articulating a standard for CSLI data past seven days. Most lower courts have rejected, either expressly or implicitly, the application of the mosaic theory to other contexts outside of CSLI technology.

A. Lower Courts Declining to Apply the Mosaic Theory’s Rationale to Other Forms of Surveillance Technology.

Since Carpenter, most lower courts have declined to extend the mosaic theory’s rationale to other types of surveillance technologies. Several courts have followed the Court’s preferred formulation of a “narrow” holding in order to reach these results. First, in United States v. Trader, the 11th Circuit declined to extend Carpenter’s reasoning to e-mail messaging “cloud” services and IP addresses associated with private messaging apps. The case involved a criminal defendant accused of soliciting and sending sexually explicit pictures to minors through online messaging apps. The 11th Circuit reasoned, absent Carpenter, the third-party doctrine would normally apply to online messaging services, and that he “voluntarily... and affirmatively act[ed] to open the app, [] log in,” and shared his IP address when using the app without taking steps to protect it. The Court held that Carpenter was inapplicable to online messaging services because of “Carpenter’s ‘narrow’ exception... appl[y]ing only to some [CSLI], not ordinary business records like email addresses and internet protocol addresses.”

106 See, e.g., Ohm, supra note 97, at 361 (arguing that “[w]hen lower courts apply these factors, they are likely to extend the Fourth Amendment to cover many important commercial databases that have never before required a warrant for police to access”). While Carpenter was merely three years ago, and developments could occur in the future, the current view of lower courts errs on the side of narrowness over a broader formulation of Carpenter and its reasoning.

981 F.3d 961 (11th Cir. 2020).

96 Id. The defendant was communicating through a private messaging service called “Kik.” Id. at 964.

97 Id. at 967.

98 Id. at 967–68 (citing Carpenter, 139 S. Ct. at 2220).
In *LopezGamez v. State*, a Texas state criminal appellate court expressly declined to extend the mosaic theory to GPS location systems in automobiles.\footnote{622 S.W.3d 445 (Tex. App. 2020), petition for discretionary review refused (Jan. 13, 2021).} The case involved a GPS location system inside of Ford F-150 truck. The Ford F-150 was purchased from a “tote-the-note”\footnote{A “tote-the-note” dealership is one which directly finances the automobiles that they sell, instead of relying on a traditional banking institution. See *What Does “Tote the Note” Mean?*, DRIVE TIME, https://www.drivetime.com/vft/tote-the-note (last visited Nov. 18, 2021).} dealership, which expressly required GPS location be shared with the dealership owner as a contingency in the event the truck had to be repossessed.\footnote{LopezGamez, 622 S.W.3d at 450–51.} Law enforcement obtained GPS information from the truck through the third-party dealership.\footnote{Id.} The Court reasoned that *Carpenter*, and thus the mosaic theory, did not apply to the voluntary GPS tracking because the defendant and his wife expressly agreed, as a condition of purchase, to allow the dealership to access their truck’s whereabouts.\footnote{Id. at 455.} Thus, the Court expressly rejected *Carpenter*’s application and impliedly rejected an extension of the mosaic theory to GPS monitoring in automobiles.\footnote{116 See, e.g., *United States v. Diggs*, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that *Carpenter* is applicable to long-term acquisition of GPS data from an automobile, thus accepting the mosaic theory).}

Several other lower courts have followed this general reasoning in order to decline extending *Carpenter*’s mandate to other technological devices and services. These situations include declining to apply the mosaic theory to state monitoring programs about prescription medications;\footnote{117 See, e.g., *United States v. Gayden*, 977 F.3d 1146 (11th Cir. 2020) (holding that *Carpenter* does not apply to Florida’s Prescription Drug Monitoring Program because the defendant did not maintain a “special privacy interest” in his prescribing records and was voluntary); *United States v. Motley*, 443 F. Supp. 3d 1203, 1213 (D. Nev. 2020) (holding that no “search” occurred because law enforcement sought information from a public service, the Nevada Board of Pharmacy, and “individuals who receive prescription drugs do not have any reasonable expectation of privacy....”).} “iCloud” and other similar services;\footnote{118 See, e.g., *United States v. Jenkins*, No. 1:18-CR-00181, 2019 WL 1568154, at *4 (N.D. Ga. Apr. 11, 2019) (holding that *Carpenter* does not apply to iCloud services because the records in question did not “contain[] the type of precise location information” as was at issue in *Carpenter*); *United States v. Shipton*, No. 0:18-CR-202-PJS-KMM, 2019 WL 5330928 (D. Minn. Sept. 11, 2019).} and social media information, such as a user sharing extensive information with Facebook.\footnote{119 See, e.g., *United States v. Coleman*, No. 1:18-CR-00484-ELR-JFK, 2020 WL 5229042 (N.D. Ga. Jan. 14, 2020) (holding that *Carpenter* was not applicable to IP and subscriber information obtained from Facebook). The Court distinguished *Carpenter* from the defendant’s situation because CSLI can track a defendant’s location “with near GPS-level precision,” whereas}
Fifth Circuit, have held that *Carpenter* is inapplicable to situations involving cryptocurrency transactions and banking. Finally, several lower courts have easily reaffirmed that *Carpenter* does not affect the privacy interests implicated by more traditional surveillance methods, such as video camera surveillance. Lower courts declining to extend *Carpenter*’s reasoning, and thus extending the mosaic theory to other intrusive, non-physical surveillance systems, represents the overwhelming weight of authority since *Carpenter* was decided.

B. Lower Courts Applying the Mosaic Theory to Other Forms of Non-Physical Surveillance

Despite most lower courts finding that the mosaic theory is inapplicable outside of the CSLI context, some courts have maintained that *Carpenter* is analogous to other forms of non-physical surveillance technology, either in its express holding or in dicta. In *United States v. Diggs*, the Northern District of Illinois determined that *Carpenter* was applicable to warrantless acquisition of GPS location technology in automobiles. The case involved more than a month of GPS location history, which law enforcement obtained through a third-party. The Court’s extensive reasoning relied on *Carpenter*, pointing out that both CSLI and GPS location data are both “detailed, encyclopedic, and effortlessly compiled... [and] provide an intimate window into a person’s life...” In other words, the probative value of the information would otherwise be unobtainable through traditional investigation techniques. Additionally, IP addresses can only disclose a singular, fixed location. *Id.* at *15 (citing *Jenkins*, 2019 WL 1568154, at *4).

---

120 *See United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (holding that defendant lacked a privacy interest in his information located on a cryptocurrency service called “Blockchain”); Zietzke v. United States, 426 F. Supp. 3d 758 (W. D. Wash. 2019).*

121 *See, e.g., United States v. Kelly, 385 F. Supp. 3d 721 (E.D. Wis. 2019); United States v. Harris, No. 17-CR-175-PP, 2021 WL 268322, at *1 (E.D. Wis. Jan. 27, 2021); United States v. Gbenedio, No. 1:17-CR-430-TWT-JSA, 2019 WL 2177943, at *2 (N.D. Ga. 2019); United States v. Moore-Bush, 963 F.3d 29 (1st Cir.), *reh’g en banc granted, opinion vacated, 982 F.3d 50 (1st Cir. 2020).* Additionally, there is at least one case finding *Carpenter* inapplicable to a novel situation where a defendant voluntarily conveyed his cellular phone password to law enforcement, which in turn used it to unlock his phone and observe its contents pursuant to a search warrant. *See People v. Davis, 438 P.3d 266, 269 (Colo. 2019).*

122 Additionally, a substantial amount of the citing references to *Carpenter* find that it does not apply retroactively, and even if it does, the “good faith” exception applies. *See, e.g., United States v. Castro-Aguirre, 983 F.3d 927 (7th Cir. 2020); United States v. Goldstein, 914 F.3d 200 (3d Cir. 2019).*


124 *Id.* at 649–50.

125 *Id.* at 653.

both technologies provide a “tracking capacity [that] runs against everyone.” Finding GPS and CSLI analogous, the Court concluded that “the fact that the police obtained the information from a third party does not overcome . . . Fourth Amendment protection.” Thus, the Court held that the mosaic theory was applicable in contexts outside of CSLI.

Additionally, a lower court has extensively reasoned in dicta that Carpenter would be analogous to “geofencing” technology. In In re Information Stored at Premises Controlled by Google, a court denied a warrant for geofencing information sought by law enforcement in relation to an investigation into the suspected theft of prescription medications. Geofencing is the act of “cast[ing] a virtual net . . . around a particular location for a particular time frame.” In this instance, law enforcement wanted to use the geo-fence “to obtain Google’s historical information about what devices were at those locations at those times.” The Court reasoned in dicta that “there is much to suggest that Carpenter’s holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration.” The Court analogized CSLI to geofencing by stating both technologies “cause [the user] to reveal their location [to third-parties] with great regularity.”

The Court reasoned:

[I]t [is] difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government’s ability to obtain—easily, quickly, and cheaply—their precise geographical location at virtually any point in the history of their use of the device.

The Court moved on to reference other forms of non-physical surveillance technology, such as “tower-dumps” and “real-time CSLI,” stating that Carpenter does not yield a firm basis for what should and should not be considered a
A tower dump is a type of technique in which law enforcement collects CSLI information for “all devices that connected to [a particular] cell site tower at a previous point in time.” Real-time CSLI is information generated by devices known as “cell-site simulators” or “Stingrays,” which law enforcement use to mimic cell sites and transmit a cellular phone’s signal to the Stingray. The Court, pointing to these two technologies—which are altogether different from the issue it considered, the use of geofencing—indicates that there is no clear standard for the Court to reference. Thus, the Court denied the government’s warrant application for geofencing location in relation to its investigation.

While these two decisions carry little persuasive authority, they indicate that lower courts would entertain the application of Carpenter to different contexts outside of CSLI. However, the majority of lower courts directly cite Carpenter as a “one-off” decision, impliedly rejecting that the mosaic theory is applicable to other technologies due to its expressly “narrow” holding. Given the exponential rate of technological innovation—and corresponding utility of non-physical surveillance to law enforcement investigations—the Supreme Court should consider outlining a broader standard, implementing Carpenter’s rationale, to expand the mosaic theory to other contexts and provide lower courts with guidance to its parameters.

IV. ADAPTING THE MOSAIC THEORY TO OTHER CONTEXTS

In light of lower courts’ reticence to adopt the mosaic theory outside of the CSLI context, the Supreme Court should articulate a broader and more explicit standard for non-physical surveillance technology to aid in adapting the Fourth Amendment to expanding technological capabilities. Issuing direct guidance on the mosaic theory will allow lower courts to use the standard as a guidepost to handle Fourth Amendment claims more effectively, increasing judicial efficiency, while also allowing them to fill in “gaps” and step in to protect constitutional rights. The rationale behind such a standard would be an example of “mini-maximalism”—in other words, “there is a need [for lower courts] to look to and rely on guidance from the judiciary” about when the mosaic theory is implicated by non-physical surveillance technology in Fourth Amendment cases. For example, law enforcement has access to historical CSLI, real-time CSLI, tower dumps, facial recognition, GPS location, and other forms of technology already, and this is without considering future innovations to non-physical surveillance technology.
Amendment cases. While some scholars are skeptical about setting a broad standard before definitive cases arise challenging new technologies, the Supreme Court should give lower courts guidance to make such decisions, as law enforcement currently utilizes analogous technologies to historical CLSI.

A. Conceptualizing Carpenter’s Extended Standard

The holding of Carpenter impliedly adopted the mosaic theory, which changes Fourth Amendment analysis. From the text of the decision, the Court seems particularly skeptical of two principles of the third-party doctrine: (a) the probative value of information is deeply revealing, to a degree that was previously incomprehensible; and (b) the questionable voluntariness of the defendant’s decision to open his or her “circle of trust,” or to divulge sensitive information about his or her life to a commercial entity operating in our technological landscape.

First, the Supreme Court was concerned with both the reasonable expectations of privacy and the probative value of the information law enforcement obtained through the third-party. The CSLI at hand contravened “society’s expectation . . . that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement . . . for a very long period.” This is because CSLI “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” Furthermore, the technology is substantially easier and more efficient to use when compared to “traditional investigative tools.” Additionally, the Court was seemingly concerned that the non-physical surveillance technological capabilities surpassed what could have been accomplished through more traditional investigatory methods, stating “the retrospective quality of the data here gives police access to a category of information otherwise unknowable.” Traditional methods are limited to the resources and abilities of the investigating law enforcement.

---

146 Id. (concluding that allowing government access to [CSLI] contravenes society’s reasonable expectation to privacy).
147 Id. (Sotomayor, J., concurring) (quoting United States v. Jones, 565 U.S. 400, 415 (2012)). 148 Id. at 2217–18.
149 Id. at 2218.
agency; however, these limitations are not applicable to more modern sources of non-physical surveillance.\textsuperscript{150} Thus, part of the new standard should emphasize that the probative value of the information is especially adverse to normative privacy interests because it is of a type that traditional Fourth Amendment analysis would not anticipate.

Second, the Court stressed the involuntariness of divulging sensitive information to third parties.\textsuperscript{151} Here, the Court recognizes the “seismic shifts in digital technology that made possible the tracking” in this case.\textsuperscript{152} Furthermore, the Court distinguished the nature of the parties—rather than being a typical witness, the third party at hand was a commercial business involved in telecommunications technology.\textsuperscript{153} Additionally, the “reduced expectations of privacy” stem from the fact that the information was “knowingly shared with another.”\textsuperscript{154} However, longer-term tracking, again, extending beyond the boundary of what is reasonably possible through traditional surveillance techniques, presents a different situation.\textsuperscript{155} Moreover, the CSLI was not “truly ‘shared’ as tone normally understands the term.”\textsuperscript{156} There is very little voluntariness in having your CSLI shared with a wireless carrier, outside of turning on your phone, and it applies to “[v]irtually any activity on the phone. . . .”\textsuperscript{157} The Court articulates no standard, and explicitly states that its holding exclusively applies in the CSLI context. However, these two rationales can be formulated into a standard to give lower courts guidance on how to apply the mosaic theory into the future—whether the Supreme Court ultimately decides in favor of the exclusion of the technology at hand from the third-party doctrine.

Moreover, there are no compelling reasons why the mosaic theory cannot be invoked before seven days.\textsuperscript{158} Following the Court’s own reasoning,

\begin{itemize}
  \item \textsuperscript{150} Id. (stating “[i]n the past, attempts to reconstruct a person’s movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, [law enforcement] can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carrier. . . .”).
  \item \textsuperscript{151} Id. at 2219.
  \item \textsuperscript{152} Id.
  \item \textsuperscript{153} Id. (stating that witnesses of this type are “ever alert, and their memory is nearly infallible”). While the first rationale—the wide scope of information—is not satisfied, the second line of reasoning could arguably be applicable to several different records, including banking records, cryptocurrency wallets or services, and iCloud services. The Court distinguishes this, stating that there is a “world of difference” between the information collected. Id. However, it is outside the scope of this Note to comment on more traditional formulation of the third-party doctrine.
  \item \textsuperscript{154} Id.
  \item \textsuperscript{155} Id. at 2219.
  \item \textsuperscript{156} Id. at 2210.
  \item \textsuperscript{157} Id. at 2220.
  \item \textsuperscript{158} See id. 2217 n.3 (declining to articulate a standard for the mosaic theory past 7 days of collected CSLI data).
\end{itemize}
the severe implications of allowing law enforcement to obtain this type of
information without a warrant is also enough to completely foreclose the
possibility that it will ever be obtained in such a manner. First, data of
this type is much greater in scope and in depth than any traditional investigatory
method, so it follows that such information should only be available when law
enforcement is able to establish probable cause in front of a magistrate. Second,
the involuntary nature of the individual’s disclosure makes for a compelling
argument because an individual is disclosing information without necessarily
being aware that he or she is doing so. Thus, the Court should insist that this
doctrine applies to any information, not just information collected in a less than
seven-day period.

The two-prong Carpenter formulation the Supreme Court should
consider is (a) “the deeply revealing nature” of the information collected by
the technology at hand; and (b) the involuntariness of transmitting the information
to a third party. This is a faithful application of Carpenter’s analysis, while not
foreclosing the possibility that other current or future uses of non-physical
surveillance technology could also fall under the mosaic theory. Further, the
Court should adopt the standard to apply as a wholesale exclusion from the third-
party doctrine. Because the nature of collection involves both deeply revealing
information and involuntary activity, police should be required to apply for a
warrant when using the technology during an investigation, with the normal
exception of exigent circumstances. This ensures that there is never a situation
where police are warrantlessly using a deeply revealing technology for an
extended period, even if police would eventually be required to obtain a warrant.

159 See id. There have been other standards recommended for implementing Carpenter. While
this one differs from the “Carpenter test” discussed above, it is also similar—attempting to stay
true to Carpenter’s rationale while emphasizing it can be applicable to different contexts. See Ohm,
supra note 97 (stating that Carpenter’s test consists of: “(1) ‘the deeply revealing nature’ of the
information; (2) ‘its depth, breadth, and comprehensive reach;’ and (3) ‘the inescapable and
automatic nature of its collection.’” Additionally, other scholars have formulated different
proposals. See Kerr, supra note 143 (arguing that the test implementing Carpenter should be: (a)
the records exist because of the digital age; (b) they were created without meaningful voluntary
choice; and (c) they tend to reveal the privacies of life).

enforcement’s use of real-time CSLI did not violate Carpenter because the defendant “posed a
potentially imminent threat to the safety of identified minor children”).
B. The Mosaic Theory Is Potentially Applicable to Other Technologies

Since Carpenter has been handed down, lower courts have been reluctant to apply its reasoning to other contexts despite analogous factual scenarios.\(^{161}\) Carpenter's reasoning, however, can be applied to these scenarios faithfully, and lower courts should be encouraged to step up and protect Fourth Amendment principles when these situations are sufficiently analogous. Indeed, analogous situations have already arisen involving non-physical surveillance technology which law enforcement already utilizes in investigations.\(^{162}\) Below, I will examine three different types of non-physical surveillance technology that is currently used by law enforcement: Real-time CSLI or "Stingrays," "geofencing," and "tower dumps."

First, real-time CSLI, or a Stingray, as explained above, is when law enforcement uses a device to mimic a cell site tower. When a cellular phone user is in the area of the Stingray, the cellular phone will become confused and connect with the Stingray instead of a regular cell site tower. This information is more particularized than historical CSLI, as a Stingray can only connect with a cellular phone when it is within range of a cell site. A Stingray is not able to pick up any cellular phone signal anywhere, anytime. However, Stingrays certainly exemplify a novel use of technology that was not possible before the digital age.

Real-time CSLI is analogous to the historical CSLI in Carpenter and satisfies the first prong of the proposed standard because it potentially reveals sensitive information. While less comprehensive than the historical CSLI in Carpenter, police would still be able to garner a comprehensive amount of information without having to personally and visually surveil a suspect. Additionally, law enforcement would be able to put together sensitive information about an individual's life based on the movements of their person. For example, a person could go to the store, visit a religious or community association, or partake in their personal, private hobbies. Law enforcement, through normal visual surveillance, would be able to track an individual and garner this information without a warrant. The significant difference is that Stingray makes this information "remarkably easy, cheap, and efficient compared to traditional investigative tools."\(^{163}\)

Additionally, real-time CSLI is not voluntary in any normative sense. By mere operation of a cellular phone, any suspect would be potentially transmitting their cellular phone signal out to law enforcement who is mimicking a cellular phone tower. This may violate our societal expectation of privacy because while

\(^{161}\) See United States v. Diggs, 385 F. Supp. 3d 648, 654 (N.D. Ill. 2019) (quoting Carpenter, 138 S. Ct. at 2219) (reasoning that the mosaic theory applies to a GPS system in an automobile because the defendant had a reasonable expectation of privacy in the "in the whole of his physical movements"); In re Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020) (reasoning that Carpenter's holding may be applicable to geofencing).

\(^{162}\) See Diggs, F. 385 F. Supp. 3d at 654.

\(^{163}\) Carpenter, 138 S. Ct. at 2218.
we may be out on public roads for all to see, we certainly do not expect our cellular phone to be transmitting our exact location to police, who could be up to miles away. Simply operating a cell phone, a virtual necessity for any social or working individual, reveals the individual’s location to law enforcement investigation. Thus, the two-prongs of Carpenter are potentially implicated by this technology.

Second, geofencing is another type of non-physical surveillance technology that could be implicated by a broader formulation of Carpenter. Geofencing is a type of technology which “cast[s] a virtual net” on cellular phone activity within a given area. Any cellular phone, or cellular device, that is in the area of the geofence would be revealed by the technology. However, geofencing an area does not have to be limited to any particular area, or for any particular amount of time. Additionally, many businesses use it for purposes such as targeted advertising to consumers. Moreover, it uses GPS and Bluetooth to figure out an individual cellular phone user’s location.

Geofencing may be implicated by a broader standard of Carpenter for similar reasons as above. First, it is revealing information because it can convey a cellular phone user’s location in an easy and efficient manner, even when law enforcement is not present in the area. Such location does not have to be exclusively in a public area; it can be utilized to search for individuals who have entered into private residences or buildings. Most concerning, it can implicate multiple individuals’ location information, not just a particular person. Furthermore, as with CSLI, this information is conveyed in a far from voluntary manner. By virtue of using a cellular phone, and being in a particular location, you will be caught in the virtual net of a geofence. This can happen with “great regularity,” just as in Carpenter. This is done “easily, cheaply, and effectively,” like historical CSLI data. Thus, a broader standard and increased scrutiny on these practices could render a court to determine that this use of non-physical surveillance runs afoul of the mosaic theory.

Finally, “tower dumps” could become an unfavored practice requiring a warrant if Carpenter’s rationale is extended to apply to technologies outside of the historical CSLI context. Tower dumps extract historical CSLI from every cellular phone that was connected to a specific cell site within a specified time period. By its nature, this involves more access than a regular historical CSLI

---

164 See In re Search of Info. at Premises Controlled by Google, 481 F. Supp. 3d at 732.
165 Id.
167 Id.
168 See In re Search of Info. at Premises Controlled by Google, 481 F. Supp. 3d at 737.
169 Id. at 737.
170 In fact, the FBI recently used this technique to quickly secure data on someone who entered the Capitol during the riot at the U.S. Capitol on January 6, 2021. See Ken Klippenstein & Eric
record information because it includes more user data. In fact, one federal court has observed that “[a]ny order authorizing a cell tower dump is likely to affect at least hundreds of individuals’ privacy interests.”

Tower dumps are information obtained through third-party companies, similar to historical CSLI. While it may be anonymized, and not particularized, it would still be an inquiry which exposes the totality of a person’s physical location for a certain period of time. Additionally, it would potentially reveal to law enforcement individuals’ associational groups or other organizations of a similar kind. However, the inquiry is limited to a specific cell site tower, usually for a specific period of time. While the mosaic theory states that a lot of non-searches may add up to a search, here, the technological capabilities would be a vast collection of CSLI data for a relatively limited time period. On the other hand, it seems as though it would be an invasion of privacy to state that police cannot obtain one person’s CSLI data unless armed with a warrant, but they may permissibly obtain hundreds, if not thousands of individuals’ CSLI data. Moreover, the voluntariness rationale is not met for similar reasons as laid out above: the data collection merely requires that a group of individuals have cellular phones, and that it be connected to a cell site. A lower court could reasonably conclude that tower dumps stand in violation of Carpenter’s holding because of the revealing nature of its qualitative data collection and the involuntariness of the collection itself.

However, if the Fourth Amendment was to encompass geofencing, it would be an expansion of the mosaic theory which diminishes previous Supreme Court precedent, contrary to United States v. Knotts. In Knotts, the Supreme Court held that “augment[ed]’ visual surveillance did not constitute a search” because any individual does not have a reasonable expectation of privacy in their public movements. However, it is important to distinguish the type of surveillance technology at hand. In Knotts, law enforcement used a beeper, placed into a container of chloroform by one of the defendant’s co-
conspirators. This can be distinguished from geofences for two reasons. First, law enforcement had already obtained the cooperation of a third party, one of the defendant’s co-conspirators, to whom he had voluntarily opened his circle of trust. Second, geofencing is hardly voluntary, as it catches cell phone information for any device within its parameters. Thus, a lower court could seriously question the applicability of Knotts to each of these more modern technologies.

This list is not meant to be exhaustive. There are other technologies which may run afoul of a newly revisited Fourth Amendment meant to be adapted to the digital world. In fact, the First Circuit is currently preparing to address en banc whether its position on traditional video surveillance technology should be adjusted in light of Carpenter. This is not to mention the various technologies that may be developed in the near or far future. Furthermore, it is not entirely clear how marketplace adjustments will affect individual privacy rights. Needless to say, citizens should not have to rely on whether their wireless carrier is dedicated to protecting their privacy. A new standard, providing guideposts to lead the Fourth Amendment to the digital age, will both protect citizens rights in the short-term and help define the mosaic theory in the long-term.

C. A Broader Adaptation of the Mosaic Theory Is Desirable to Provide Lower Courts with Increased Guidance

A clarified, broader standard of Carpenter is necessary to provide adequate guideposts to lower courts, so they can adapt the Fourth Amendment to a changing technological and digital landscape. Judicial decision-making can be enhanced through adapting Carpenter, with an increase in judicial efficiency; allowance of a robust deliberation and case law before the Supreme Court

---

174 Knotts, 460 U.S. at 277.
175 United States v. Moore-Bush, 982 F.3d 50 (1st Cir. 2020) (order granting rehearing en banc).
ultimately decides the issues; and ensuring that citizens receive the full protection of the Fourth Amendment while surveillance techniques develop. Giving lower courts a proper framework to address these issues will lead to more precise reasoning and better deliberation, before the Supreme Court ultimately refines the doctrine addressing digital technology. Intrinsically, this will be a positive development because it will lead to greater judicial efficiency—allowing lower courts to do their job before the novel issues ultimately reach the Supreme Court. Additionally, it will allow lower courts to properly address defendants' constitutional arguments.

Judicial efficiency will be improved as a result of a broader standard of Carpenter because lower courts will be in an adequate position to decide the issues from an informed standpoint and a refined definition of the mosaic theory. With the "deeply revealing" nature of the technology at issue and lack of voluntariness already defined, lower courts will be able to analogize and distinguish the similarities and differences of the technologies at issue in the motions to suppress as they present themselves. This will presumably lead to a greater deliberation of the issues and better reasoning. Instead of determining the issue at the Supreme Court level on a case-by-case basis, lower courts will be armed to determine the lines of the mosaic theory themselves, before the issue ultimately comes up to the Supreme Court level. Lower courts may take a diversity of approaches, all of which will better inform the Supreme Court before it makes an ultimate determination on the limitations of the doctrine.

Additionally, this approach will better inform law enforcement about the constitutionally permissible lines applicable to their investigations. As self-interested actors, law enforcement would not want to engage in any investigatory techniques which may endanger a criminal investigation. This is backed up by the Supreme Court endorsing the practice of drawing "bright-lines" to ensure law enforcement is properly informed about constitutional boundaries. In turn, this will lead to better law enforcement practices in both the short and long-term and provide for a reasonable equilibrium between enforcement of our laws and civil liberties. While some scholars prefer the Supreme Court to take an approach which emphasizes caution and greater clarity before ultimately deciding these issues, the better approach is to give lower courts greater latitude in applying

177 Most lower courts quickly analyze the issues without a thorough examination of the technology at hand. This usually involves one paragraph about the narrow holding in Carpenter. See, e.g., United States v. Moalin, 973 F.3d 977 (9th Cir. 2020); United States v. Morrel, 922 F.3d 1 (1st Cir. 2019); United States v. Coleman, No. 1:18-CR-00484-ELR-JFK, 2020 WL 5229042 (N.D. Ga. 2020).


179 See Kerr, supra note 143.
these principles, so informed decisions are made at those levels. Thus, a newly clarified standard will better inform law enforcement about the investigative decisions they will be making during the course of their work.

In the meantime, this will substantially affect parties’ rights, filling in gaps to apply a standard which can potentially conform to the Court’s formulation of the mosaic theory. With a clarified holding that lower courts can use to adapt differing factual scenarios, they will apply those to the law in a variety of ways. Thus, the legal debate surrounding the Fourth Amendment in the digital world will increase, and courts will be able to interpret a wide range of applications implicating the mosaic theory. Allowing lower courts broader latitude in applying Carpenter’s principles will increase the thoughtfulness of the lower courts when applying these concepts to new technologies to ensure the Supreme Court is able to review cases which reflect a variety of viewpoints on the nexus of technology and the Fourth Amendment.

It is important to remember that these technologies are being used by law enforcement currently. Declining to articulate a standard that can be adaptable to current and future technologies essentially render criminal defendants helpless while the mosaic theory’s boundaries are sorted out. If these non-physical surveillance technologies are implicated by the Supreme Court’s articulation of the mosaic theory, criminal defendants may be convicted while the court determines the doctrine’s scope on a case-by-case basis. Most concerning for criminal defendants is the potential to be convicted while the mosaic theory is being defined, as prosecutors will be apt to rely on the “good faith” exception to circumvent the exclusionary rule and uphold their previous convictions. Therefore, the Court should define the scope of the mosaic theory in order to ensure that these victims can avail themselves of their constitutional rights, if those are potentially at stake.

V. CONCLUSION

Because Carpenter’s narrow holding has been restrictive in allowing lower courts to reach determinations on what non-physical surveillance technologies are applicable to the mosaic theory, a broader standard based on Carpenter’s reasoning should be articulated in order to clearly define the doctrine moving forward. A standard with a clear application can be articulated while staying true to Carpenter’s rationale, hinging on the “deeply revealing nature” of the information acquired and the involuntariness of the conveyance. Moreover, this technology is presently being employed by law enforcement,

---


181 There are multiple examples of this exact scenario unfolding for criminal defendants who were convicted, in part, upon warrantless CSLI before Carpenter. See, e.g., United States v. Castro-Aguirre, 938 F.3d 927 (7th Cir. 2020); United States v. Goldstein, 914 F.3d 200 (3d Cir. 2019).

making the issue altogether more pressing for lower courts, criminal defendants, and law enforcement agencies. Finally, a standard with clear guideposts will enable lower courts to determine the mosaic theory’s doctrine moving forward into a world with exponentially increasing technological innovation.

Ben Vanston

* West Virginia College of Law, Class of 2021. I am grateful to the entirety of the West Virginia Law Review, especially Volumes 123 and 124. Without them, this Note would not be possible. Moreover, I would like to thank the entirety of the WVU College of Law faculty and staff, whom I am endlessly grateful for. Special thanks to Professor John E. Taylor, who taught an excellent criminal procedure course which planted the seed for this Note. All errors are the Author’s own.