Spring 2022

The Carpenter Shift: The Evolution of Fourth Amendment Jurisprudence in the Digital Age

Lindsey R. Mattson
lmattson@trincoll.edu

TRINITY COLLEGE

The *Carpenter* Shift: The Evolution of Fourth Amendment Jurisprudence in the Digital Age

BY

Lindsey Mattson

A THESIS SUBMITTED TO

THE FACULTY OF THE DEPARTMENT OF PUBLIC POLICY AND LAW

IN CANDIDACY FOR THE BACCALAUREATE DEGREE

WITH HONORS IN PUBLIC POLICY AND LAW

HARTFORD, CONNECTICUT
MAY 2022

Acknowledgements

I would like to express my deepest gratitude to Professor Fulco. She has served not only as my thesis advisor for the past year, but also as a mentor throughout my undergraduate career. This project would not have been possible without her guidance and support.

I must also extend my sincere thanks to Professor Falk. My interest in this thesis topic was sparked in part by the courses I have taken with him over the years. Professor Falk also generously served as the second reader for my thesis, and I am incredibly appreciative of his insightful comments and suggestions.

Lastly, I want to acknowledge the significant role my parents played in my thesis writing process. It is because of their support and belief in me that I undertook and completed this project. Words cannot express my gratitude for their unwavering encouragement and love.

Table of Contents

Chapter 1

The Early Republic and The Right to Privacy

Since before the founding of the United States, privacy concerns have earned significant political attention and sparked debate over proper legal protections. Concerns of government overreach into the private sphere first surfaced during the colonial period, when the British government issued court orders called "general warrants" and "writs of assistance."[1] These orders gave British customs officers the power to conduct non-specific searches of colonists' workplaces and homes for untaxed goods. This practice galvanized political resistance to arbitrary searches during the 18th century and formed the basis for one of the most sacred protections in the American Constitution, the Fourth Amendment.

The Fourth Amendment provides, "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."[2]

The Fourth Amendment was conceived during a time when abuses of privacy were initiated through the entering of a home, the physical search of a person, or the seizure of their belongings. The Framers did not imagine the scope of this right needed to be broader. However, by the end of the 19th century, scholars were already taking note of the Fourth Amendment's shortcomings. Most notably, legal scholars Louis Brandeis and Samuel Warren questioned the extent to which privacy would be protected by the Fourth Amendment in the face of modern technologies. In their esteemed *Harvard Law Review* article, titled "The Right to Privacy,"

[1] Orin Kerr and Barry Friedman, "Interpretation: The Fourth Amendment," National Constitution Center, accessed October 10, 2021, https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121.
[2] "The 4th Amendment of the U.S. Constitution," National Constitution Center, accessed September 30, 2021, https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv.

Brandeis and Warren suggested that a right to privacy is embedded in American common law. This right, they argued, is one that responds to the evolving needs of society.

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society…Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, – to be let alone…and the term "property" has grown to comprise every form of possession – intangible, as well as tangible.[3]

Although their article provides a direct response to privacy concerns triggered by the advent of cameras and celebrity journalism, the sentiment in "The Right to Privacy" fits well into our modern context. Today, we live in a world known as the digital age. Every piece of information, from our contacts to our health records, exists in a digital form, accessible to anyone with a phone password or subpoena. In our hyper-digitalized society, where the information capacity of computers and cellphones so greatly outweighs those of 18th century "papers and effects," the initial scope of the Fourth Amendment is insufficient. As Warren and Brandeis argued in "The Right to Privacy," new technologies necessitate new conceptions of privacy, and, with them, require enhanced protections. Forty years later, after joining the Supreme Court, Justice Brandeis would dissent in the case *Olmstead v. United States*. There he echoed a similar sentiment, once again advocating for a substantial right to privacy, sufficient for the modern age: "Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[4]

For over a century, justices and legal scholars have recognized Justice Brandeis' forewarning to be true. The language of the Fourth Amendment is inadequate to safeguard

[3] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 193–220, 193. https://doi.org/10.2307/1321160.
[4] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

privacy in the face of new technologies, and consistently requires reconsideration. In an effort to reconcile the language of the Fourth Amendment and increasing privacy concerns, the Supreme Court has grappled with adjusting the scope of the Amendment to ensure that the proper balance between state power and individual privacy endures. This has resulted in a century-long line of case law that has answered some questions, but left open many more regarding how modern technologies, both current and future, will fit into the standing legal framework. In this chapter, I explore some of the most consequential developments in Fourth Amendment jurisprudence in the digital age, highlighting the continued challenge the Court faces as it attempts to balance government interest in police surveillance and privacy concerns among the American people.

The Digital Fourth Amendment in the Supreme Court

The first Supreme Court case to dictate the trajectory of Fourth Amendment jurisprudence was *Olmstead v. United States.* In this case, Roy Olmstead was suspected of running a large-scale bootlegging operation during Prohibition. Upon suspicion, federal prohibition officers wiretapped phone lines that connected from the chief office of the operation to the homes of several conspirators. The wiretapping intercepted phone lines in the basement of the office and on the streets outside the residences of the petitioners. Over several months, the federal officers gathered evidence from phone calls made between Olmstead and other co-conspirators, revealing information about large liquor importations and other business transactions. The wiretapping implicated not only the petitioners in the case, but seventy-two other individuals who were part of the illegal operation.[5]

[5] Olmstead v. United States, 277 U.S. 438, 455 (1928).

Following their convictions of conspiracy to violate the Prohibition Act, Olmstead and the other defendants appealed to the Supreme Court. They challenged their convictions on the grounds that the wiretapping of phone calls, absent a warrant, violated both their Fourth and Fifth Amendment rights. Ultimately, a majority of the Court, including Chief Justice Taft, found Olmstead's argument unconvincing. The Court rejected the premise that a Fourth Amendment search could occur outside the strictly defined realm of "persons, houses, papers, and effects." In fact, the opinion of the Court suggested that to consider wiretapping a Fourth Amendment search, and hold the evidence to be inadmissible, would be "attributing an enlarged and unusual meaning to the Fourth Amendment."[6]

In the opinion of the Court, Chief Justice Taft adhered to the traditional common law physical trespass doctrine. This doctrine states that a Fourth Amendment search takes place only when "seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house "or curtilage" for the purpose of making a seizure" occur.[7] In this view, the Court argued that since the wiretapping did not implicate the homes or tangible effects of the petitioners, a Fourth Amendment search had not occurred. Thus, the evidence obtained through the wiretapping was permissible. Olmstead and his co-conspirators' convictions stood, and the Court solidified the common law physical trespass doctrine in Fourth Amendment jurisprudence. This decision stood until the landmark case of *Katz v. United States.* In 1967, the Court was again faced with the challenge of applying the Fourth Amendment to a new context. This time, the Court abandoned the physical trespass doctrine for a more liberal Fourth Amendment test: a reasonable expectation of privacy.[8]

[6] Id. at 438.
[7] Id. at 466.
[8] Katz v. United States, 389 U.S. 347 (1967).

In the case of *Katz v. United States*, petitioner Charles Katz challenged his conviction of transmitting betting information across state lines. Katz, who had been placing illegal bets from California to Boston and Miami, argued that his Fourth Amendment right was violated in the gathering of evidence against him. Federal law enforcement agents had attached an electronic listening and recording device to a public phone booth where Katz made his calls. The agents used this device without a warrant. The Supreme Court ruled in favor of Katz, finding the eavesdropping of Katz's phone calls by the government a violation of his Fourth Amendment rights.

The opinion of the Court, authored by Justice Stewart, demonstrated a significant legal departure from the arguments made in *Olmstead.* While a majority of justices in *Olmstead* declined to recognize phone calls as deserving of Fourth Amendment protections, the majority in *Katz* took the opposite approach. In his opinion, Justice Stewart argues that the Fourth Amendment must provide protection for oral statements, not just tangible items.[9] Furthermore, Justice Stewart rejected the government's argument that the visibility and public nature of the phone booth precluded statements uttered within it from receiving constitutional protection. Justice Stewart reasoned:

> But what he sought to exclude when he entered the booth was not the intruding eye -- it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[10]

[9] Id. at 353.
[10] Id. at 352.

Justice Stewart's opinion was monumental in Fourth Amendment jurisprudence. In holding that Katz was entitled to Fourth Amendment protections in a public phone booth, because this was an area in which constitutional protection of private phone calls extended, the Court effectively adopted a new interpretation of the Fourth Amendment. This new interpretation looked beyond the narrow language of the Fourth Amendment, to consider how modern technology changed expectations of privacy. The physical trespass doctrine would no longer control Fourth Amendment cases. Instead, the Court would apply the Fourth Amendment with the understanding that it protects "people – and not simply areas."[11]

In his famous concurring opinion, Justice Harlan took the *Katz* decision a step further. He concluded that, through the Court's analysis of Katz's right to privacy in calls made from a public phone booth, the Court had paved a new path in Fourth Amendment jurisprudence. In fact, he asserted that the Court created an entirely new test to assess Fourth Amendment cases: the reasonable expectation of privacy test.[12] This new framework required that two features be met. Justice Harlan detailed: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable.""[13] Ultimately, Justice Harlan's concurring opinion has been incredibly influential as it elucidated the new *Katz* privacy test, which is still discussed in Fourth Amendment cases today.[14]

In 1976, less than a decade after *Katz*, the Supreme Court decided a case that significantly altered Justice Harlan's reasonable expectation of privacy test. This case, *United*

[11] Id. at 353.
[12] Id. at 360 (Harlan, J., concurring).
[13] Id. at 361 (Harlan, J., concurring).
[14] Nicandro Iannacci, "Katz v. United States: The Fourth Amendment Adapts to New Technology," National Constitution Center, accessed September 28, 2021, https://constitutioncenter.org/blog/katz-v-united-states-the-fourth-amendment-adapts-to-new-technology.

States v. Miller, involved a man who was investigated for committing tax fraud. Unaccompanied by a warrant, police officers presented subpoenas to the presidents of two banks, requesting copies of Miller's bank records. The records were obtained and used to convict Miller. When the case reached the Supreme Court, Miller argued that the evidence gathered from the bank records should be dismissed because the government had conducted an unlawful Fourth Amendment search. Relying on *Katz,* Miller argued that he had a reasonable expectation of privacy in the copies of his personal records held by the banks. This case forced the Court to consider a new type of Fourth Amendment question, this time involving a third party.

In a 7-2 decision, the Court held that Miller's Fourth Amendment rights had not been violated. The opinion, authored by Justice Powell, reasoned that it was not Miller's "private papers" which had been seized, but transactional records belonging to the banks.[15] Furthermore, because Miller had voluntarily conveyed his personal information to the banks, his records were no longer subject to constitutional protection.

The Court's opinion in *United States v. Miller* established what has proven to be an extremely consequential Fourth Amendment loophole, the third-party doctrine. This new constitutional principle carved out an exception to the *Katz* reasonable expectation of privacy test, restricting information voluntarily shared with a third-party entity from receiving Fourth Amendment protection. Crucially, the third-party doctrine enables the government to access personal information disclosed to the third parties without a warrant, regardless of the defendant's expectation that their information be used for "limited purposes."[16]

The Court's creation of the third-party doctrine demonstrated a significant departure from previous Fourth Amendment rules which stated that a reasonable expectation of privacy justified

[15] United States v. Miller, 425 U.S. 435, 440 (1976).
[16] Id. at 443.

Fourth Amendment protection. Here, the Court decided to tip the scale in favor of limiting privacy protections, rather than expanding them, as it had in *Katz.* Justice Brennan disagreed with the Court's narrowing of protections for information shared to third parties. He argued: "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[17] Justice Brennan criticized the majority's finding that the voluntary nature of the bank records rendered them undeserving of constitutional protection. He suggests that this argument ignores the realities of modern society, as it forces individuals to forfeit their Fourth Amendment rights by engaging with a necessary aspect of economic life.

Three years later, in the case of *Smith v. Maryland*, the Court applied the third-party doctrine to a new set of facts. In this case, the Court held that the installation of a pen register, used to trace phone numbers dialed from the petitioner's home phone, was not a violation of his Fourth Amendment rights. The opinion of the Court, authored by Justice Blackmun, presented reasoning analogous to *Miller*. Justice Blackmun argued that Smith did not have a reasonable expectation of privacy to the phone numbers he dialed, as he was voluntarily accepting the risks of disseminating private information.

> Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[18]

[17] Id. at 451 (Brennan, J., dissenting).
[18] Smith v. Maryland, 442 U.S. 735, 743 (1979).

Smith had failed to convince the Court of his subjective expectation of privacy in his dialed phone numbers. Crucially, Justice Blackmun denied Smith's claim of an expectation of privacy in his dialed phone number because, unlike the recording device in *Katz,* the pen register here did not capture "contents of communications."[19] The Court reasoned that, although the substance of a phone call is subject to constitutional protection, the recording of dialed phone numbers is not. Furthermore, the Court declined to recognize this privacy expectation as generally "legitimate."[20] Instead, the Court applied the third-party doctrine, asserting that individuals accept the risk of their information being turned over to the government by subscribing to a phone company in the first place. Thus, the Court solidified that a warrant would not be required to access non-content-based communication shared with a third-party entity.

Like the *Miller* case, a few of the Justices did not look favorably upon this decision. In his dissenting opinion, Justice Marshall echoed the sentiment of Justice Brennan in *Miller.* First, he took issue with the Court's assertion that subscribing to a phone company requires users to forfeit their Fourth Amendment right in the numbers they dial.

> Implicit in the concept of assumption of risk is some notion of choice...By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative."[21]

Just as Justice Brennan had argued the use of a bank had become an indispensable part of economic life by the mid 1970s, Justice Marshall found the same to be true about the use of a home phone. He disputed the Court's determination that individuals could realistically choose between using a phone and accepting the risk of surveillance at a time when telephones are a

[19] Id. at 741.
[20] Id. at 744.
[21] Id. at 749 (Marshall, J., dissenting).

necessity in modern society. Justice Marshall argued that choice requires alternatives, and to a home phone, there are none. Additionally, Justice Marshall strongly disagreed with the majority opinion's assertion that phone numbers themselves do not provide enough private information to warrant a reasonable expectation of privacy. He argues that records of dialed phone numbers can reveal, for example, political affiliation or confidential calls made by journalists to their sources, both of which should be protected by a reasonable expectation of privacy. [22] Allowing the government to access these records, without a warrant, Justice Marshall argued, undermines a tenet of our "free society."[23]

Though the direct implications of *Miller* and *Smith* are largely confined to Fourth Amendment cases that involve a third party, these decisions are significant in the landscape of Fourth Amendment jurisprudence. The Court's adoption of the third-party doctrine greatly undermines the Court's prior holding in *Katz*, as it effectively limits privacy protections for information that is not in any real sense voluntarily disclosed in the digital age. This Fourth Amendment exception has become increasingly important, as individuals today disseminate larger quantities of more sensitive information to third parties as a function of the digitalization of our society. In my next chapter, I will discuss how the Court's most recent digital Fourth Amendment case narrowly limited the scope of the third-party doctrine, based in part on the reasoning in *Katz, United States v. Jones*, and *Riley v. California.*

In 2012, the Court decided another landmark Fourth Amendment case, *United States v. Jones.* In this case, the government obtained a warrant to place a global positioning system (GPS) device on a vehicle registered to Jones' wife. The warrant specified that the installation

[22] Id. at 751 (Marshall, J., dissenting).
[23] Id. at 751 (Marshall, J., dissenting).

was to occur in the District of Columbia within 10 days, but the police officers did not place the device until the 11th day and did so in the state of Maryland. The government tracked the movements of the car for 28 days, gathering more than 2,000 pages of location data.[24] This evidence led to an indictment of Jones on drug-trafficking-conspiracy charges.

The Supreme Court unanimously held that the installation of the GPS on Jones' vehicle, and the subsequent location tracking for 28 days, amounted to a search within the meaning of the Fourth Amendment, though the justices relied on significantly different rationales to reach this conclusion. The late Justice Scalia, writing for the majority, advanced an argument that the Court seemed to retire in *Katz*. He demonstrated that the Fourth Amendment's connection to property was the guiding principle in the majority's opinion. Accordingly, he argued, Jones' Fourth Amendment rights were violated when the government affixed a GPS tracking device onto his car without a valid warrant, because the common law trespass doctrine explicitly prohibits the unreasonable search of a person's tangible effects. Though the majority opinion recognized the validity of the *Katz* test in cases that involve modern technology, it declined to apply the *Katz* analysis to the *Jones* facts. In response to the government's use of the *Katz* test analysis to argue that Jones did not have a reasonable expectation of privacy in his location on public streets, Justice Scalia asserted that the Court did not need to address the validity of Jones's Fourth Amendment claims through the *Katz* framework at all.[25] Rather, Justice Scalia held that the Court's adoption of the *Katz* reasonable expectation test did not replace the common law trespass doctrine, and, thus, a property-based approach to the Fourth Amendment could suffice to decide this case. As such, Justice Scalia refused to engage with an analysis of the nature of the

[24] United States v. Jones, 565 U.S. 400, 403 (2012).
[25] Id. at 406.

technology in question – GPS surveillance. On the other hand, Justices Alito and Sotomayor filed concurring opinions, in which they found it imperative to discuss the type of technology in this case, and its implications for privacy protections beyond *Jones*.

In his concurring opinion, with which Justice Ginsburg, Breyer, and Kagan joined, Justice Alito rejected the majority opinion's application of the common law physical trespass doctrine. In line with Fourth Amendment precedent, Justice Alito argued that *Jones* must be analyzed using the *Katz* framework, as the trespass doctrine had been found to be insufficient in proving a search in modern case law.[26] Additionally, Justice Alito criticized the majority opinion for employing a legal rationale certain to lead to "incongruous results."[27] He explains that the Court's reasoning is flawed in that it would not also apply in the analogous scenario of law enforcement officers following a vehicle for an extended amount of time and using aerial surveillance tools to track an individual.[28] Furthermore, Justice Alito warns of the vague implications of the majority's opinion for the computer age. He questions how the Court's majority would rule on electronic invasions of personal property,[29] implying that the trespass doctrine is unacceptable for the privacy concerns of the digital age.

Following his critique of the majority opinion, Justice Alito puts forth a brief argument for the use of the *Katz* reasonable expectation framework. He articulates that the reasonable expectation of privacy test presents the Court with the challenge of deciphering what a "hypothetical reasonable person" expects is private from the government but argues that this analysis is critical in the digital age.[30] Justice Alito suggests that the most effective way to

[26] Id. at 419 (Alito, J., concurring).
[27] Id. at 425 (Alito, J., concurring).
[28] Id. at 412 (Alito, J., concurring).
[29] Id. at 412 (Alito, J., concurring).
[30] Id. at 427 (Alito, J., concurring).

address increasing demands for privacy, in the wake of new technologies, is by legislative remedy, but recommends the Court is best suited to protect privacy by applying the *Katz* test to Fourth Amendment cases. In this case, Justice Alito suggests that the extensive monitoring of Jones's movements "involved a degree of intrusion that a reasonable person would not have anticipated,"[31] and, thus, he concedes there was a Fourth Amendment search.

Justice Sotomayor also filed a concurring opinion in which she expands on the reasoning in Justice Alito's opinion. Justice Sotomayor agrees that the long-term surveillance of Jones's movements constituted a search under the Fourth Amendment, but she takes this argument a step further. Justice Sotomayor emphasizes the vast capabilities of the GPS, employed by the government in this case, to argue that the nature of this technology could render short-term GPS tracking in violation of a reasonable expectation of privacy.

> In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. (**"**Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on")[32]

In this passage Justice Sotomayor articulates her principal critique of the majority opinion. She believes the majority does not adequately consider the nature of the technology in this case, nor the implications its rationale has for future Fourth Amendment cases involving surveillance technologies. Justice Sotomayor warns that the invasive nature of GPS surveillance – its ability to collect intimate details of a person's life – erodes privacy protections when

[31] Id. at 430 (Alito, J., concurring).
[32] Id. at 415 (Sotomayor, J., concurring).

utilized over, both, a long period of time and a short one. Crucially, Justice Sotomayor argues that extensive GPS monitoring requires the Court to assess the reasonable expectation of privacy an individual has "in the sum of one's public movements."[33] Justice Sotomayor is concerned less with what a reasonable person expects the police have the capacity to do, as Justice Alito explains, and more with what a reasonable person expects the government will gather, or rather, not gather, about their personal life.

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[34]

While Justice Alito and Justice Sotomayor vary slightly in their interpretations of how to assess a reasonable expectation of privacy in one's movements, these concurring opinions reveal a consistent legal theory of the Fourth Amendment. Both Justices adopt an approach to Fourth Amendment jurisprudence called the mosaic theory.

The mosaic theory states that a Fourth Amendment search can occur when government activity is analyzed in "aggregate," and found to violate a reasonable expectation of privacy. In this case, the five concurring justices agreed for various reasons that the actions of the government, over the span of 28 days, when examined collectively, constituted a Fourth Amendment search. Leading Fourth Amendment scholar, Orin Kerr suggests this theory demonstrates a significant departure from the traditional "sequential" approach to the Fourth Amendment, in which police actions are examined individually and sequentially to identify

[33] Id. at 416 (Sotomayor, J., concurring).
[34] Id. at 416 (Sotomayor, J., concurring).

when, and if, a search has occurred.[35] Kerr argues that the mosaic theory effectively adds another element to the *Katz* test, asking courts to assess not simply a reasonable expectation of privacy in individual actions taken by the government, but in the sum of these actions, or according to Justice Sotomayor, what these actions reveal of one's private life. Conversely, in cases prior to *Jones*, Kerr argues that the Court has applied the *Katz* reasonable expectation test in a binary fashion, finding a search has occurred when the police surveillance violated a private space, or not, if the police remain in public spaces.[36]

The mosaic theory, Kerr argues, is well-intentioned in the digital age.[37] The theory attempts to remedy the increasing privacy concerns that arise when new technology is adopted by law enforcement and enables courts to analyze when, and if, a search has occurred when there is no clear trespass, but Kerr suggests it is misguided.[38] The mosaic theory leaves open critical questions, such as how much aggregated data amounts to a search, and requires judges to draw arbitrary lines regarding this question.[39] Though Kerr suggests the mosaic theory is misguided, and advocates for the continued use of a traditional application of the *Katz* reasonable expectation test, this theory has become increasingly important in Fourth Amendment jurisprudence. Since *Jones*, both the Supreme Court and lower courts have used the mosaic theory approach to analyze new Fourth Amendment cases, finding it to be particularly useful in the digital age.

---

[35] Orin S. Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review* 111, no. 3 (2012): 311–54. https://repository.law.umich.edu/mlr/vol111/iss3/1/.
[36] Kerr, "The Mosaic Theory of the Fourth Amendment."
[37] Orin S. Kerr, "Implementing Carpenter," in *The Digital Fourth Amendment* (Oxford University Press, Forthcoming, 2018), https://papers.ssrn.com/abstract=3301257.
[38] Kerr, "The Mosaic Theory of the Fourth Amendment."
[39] Kerr, "The Mosaic Theory of the Fourth Amendment," 314.

Two years after *United States v. Jones*, the Court delivered a decision in *Riley v. California,* presenting a legal rationale distinguished from the Fourth Amendment cases that came before it. In *Riley,* the Court examined whether the search incident to arrest rule extends to permit law enforcement officers to search an arrested person's cell phone without a warrant. The Court held it does not.

The petitioner in this case David Riley was initially stopped by the police for driving with expired registration tags. The police discovered Riley's license had been suspended, impounded his car, and proceeded to search its contents. During this search, the police officers found two handguns under the hood of Riley's car and arrested him for possession of firearms.

In addition to the search and seizure of Riley's car, an officer seized Riley's cell phone. Both the officer and a detective searched the contents of the smartphone, finding evidence that Riley belonged to a gang. Using evidence obtained from Riley's phone, including photographs that connected Riley to a previous shooting, the state charged Riley with multiple offenses related to the prior shooting. Additionally, the evidence that Riley belonged to a gang allowed the state to enhance Riley's sentence. He was sentenced to 15 years in prison.

Writing for a unanimous Court, Chief Justice Roberts argued that the search of Riley's phone was unconstitutional. The search incident to arrest rule, which the government relied on to search the contents of Riley's phone, was established to protect the safety of the arresting officer from dangerous weapons and to prevent the destruction of evidence.[40] Chief Justice Roberts argued neither criteria applies to data stored on modern day cell phones. While the opinion of the Court recognizes an interest in searching the body of the device to ensure there is not, for example, a razor blade between the phone and its case,[41] the sensitive content of the data poses

[40] Riley v. California, 573 U.S. 373, 383 (2014).
[41] Id. at 387.

no similar risk to the safety of the arresting officer. In response to the second standard for a search incident to arrest, the prevention of the destruction of evidence, the Court held this argument also fails when applied to cell phones. The Chief Justice notes, first, that remote wiping is entirely anecdotal as a means by which arrested persons destroy the contents of their cellphone to hide evidence.[42] However, even if this were a prevalent concern, arresting officers can prevent remote wiping by disconnecting a cell phone from a network. The Court held that the data stored on modern day smartphones does not pose any risk for the arresting officer, and, also, cannot be deemed vulnerable to destruction between an individual's arrest and the securing of a warrant.

The second part of Chief Justice Roberts' opinion presents a comprehensive understanding of the implications for modern cellphones in Fourth Amendment case law, the likes of which had not yet been recognized by a clear majority of the Supreme Court. In the opinion, the Chief Justice argues that the quantity and quality of data that smartphones hold distinguishes this modern technology from all analogous "effects," such as an arrestee's wallet or cigarette box.[43] Chief Justice Roberts notes that the modern-day cell phone "collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record."[44] In addition to the immense quantity of revealing information that is stored on a smartphone, the opinion highlights the complicating factor of cloud computing.[45] Modern day cell phones are designed both to hold information directly on the device and access information stored on remote servers. Thus, the

[42] Id. at 389.
[43] Id. at 393.
[44] Id. at 394.
[45] Id. at 397.

Court argues, trying to analogize the modern-day cell phone, or the types of information on it, to pre-digital counterparts is implausible. Chief Justice Roberts asserts: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life."[46]

Chief Justice Roberts' opinion in *Riley* was revolutionary in Fourth Amendment jurisprudence for two reasons. It symbolized a new direction for Fourth Amendment case law, where the Court considered the privacy concerns posed by modern day smartphones and declined to find searches of cell phones analogous to pre-digital counterparts. Additionally, this ruling quite simply limited police power. By holding that a warrant would be required to search the contents of a cell phone incident to arrest, the Court applied the concept Warren and Brandeis had introduced a century earlier: new technologies necessitate new ideas of privacy and demand enhanced protections.

A Legal Theory of Fourth Amendment Jurisprudence

As I have conveyed through a discussion of some of the most important Fourth Amendment cases in the digital age, Fourth Amendment jurisprudence is remarkably complex. Over time, the Supreme Court has grappled with challenges of applying the law to new technologies, altering the scope of the Fourth Amendment, and redefining the criteria of a Fourth Amendment search. What has resulted is a line of case law that resolves some privacy questions but leaves open many others. Most importantly, how will technologies unaddressed by the Court fit into the existing legal framework, and with what rationale will the Court decide future cases?

[46] Id. at 403.

For decades, scholars and judges have criticized the Fourth Amendment's messy legal framework, arguing the law is "a mass of contradictions and obscurities."[47] While it may appear that the Court engages in random and conflicting applications of the Fourth Amendment, subject to change depending on the type of technology, or set of facts, there exists a compelling and valuable defense for modern Fourth Amendment jurisprudence.

Orin Kerr suggests the explanation and justification for the Court's perceived inconsistencies is a theory called equilibrium adjustment.[48] Kerr argues that throughout the history of Fourth Amendment jurisprudence, the Court has remained consistent in one key area. It has always decided cases with the goal of reconciling disruptions in power between the state and individuals, as new technologies upset the prior balance.[49] As Kerr describes it, "equilibrium adjustment is a judicial response to changing technology and social practice. When new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[50] Kerr conceives this theory on the principle that the Fourth Amendment is unstable. The Fourth Amendment, Kerr argues, is inherently vulnerable to the evolution of tools which expand the police's power to investigate and a criminal's power to commit crimes.[51] When new tools and technologies enable either the state or the citizen to upset the balance of power that existed prior to the tool or technology's existence, the Court must utilize equilibrium adjustment as "a correction mechanism."[52]

---

[47] Craig M. Bradley, "Two Models of the Fourth Amendment," *Michigan Law Review* 83, no. 6 (May 1985): 1468–1501, 1468, https://doi.org/10.2307/1288896.
[48] Orin S. Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," *Harvard Law Review* 125 (December 20, 2011): 476–543. https://harvardlawreview.org/2011/12/an-equilibrium-adjustment-theory-of-the-fourth-amendment/.
[49] Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment."
[50] Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 480.
[51] Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 486.
[52] Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 488.

Crucially, Kerr makes the argument that by and large judges engage in equilibrium adjustment, even across the ideological spectrum. One of the key premises upon which Kerr argues that decades of Fourth Amendment jurisprudence embody equilibrium adjustment principles, is that judges with different constitutional approaches – pragmatists, originalists, and living constitutionalists – all exercise this "judicial instinct" in Fourth Amendment cases.[53] While some judges explicitly recognize a need for Fourth Amendment adjustment, others do so implicitly.

Throughout this chapter, I have discussed some of the Supreme Court's most important Fourth Amendment decisions. These decisions demonstrate Kerr's theory of equilibrium adjustment at work. Kerr points to Justice Brandeis' dissent in *Olmstead v. United States*, as a salient example of this theory. In his dissent, Justice Brandeis argued that the Court erred in its narrow reading of the Fourth Amendment when it did not find wiretapping to be a Fourth Amendment search. He warned that developments in technology make necessary new interpretations of the law, to ensure privacy protections remain intact. He wrote: "subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[54] This argument, Kerr notes, is the quintessential example of the equilibrium adjustment approach. Justice Brandeis articulated that the Court has a duty to bring Fourth Amendment protections in line with new tools employed by the government that upset the balance of power the Framers intended to preserve.

[53] Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 488.
[54] Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

In the case of *United States v. Katz*, the majority of the Court engaged in equilibrium adjustment just as Justice Brandeis did in Olmstead. Justice Stewart argued that the technology used by the police, to listen and record Katz's phone calls, violated his right to keep private the substance of his phone calls, and thus, under the equilibrium adjustment theory required a strengthening of privacy protections. Additionally, Justice Harlan's concurring opinion took Justice Stewart's equilibrium adjustment a step further by establishing a new Fourth Amendment test that forced the Court to consider a search unconstitutional if it violated a reasonable expectation of privacy. This test constitutes an especially clear exercise in equilibrium adjustment, as it explicitly considers how changing technology reshapes the societal understanding of privacy. While the reasonable expectation of privacy test does not necessarily expand privacy protections, as seen in *Miller* and *Smith*, it does provide the Court with a more substantial litmus test to determine when the balance of police power and individual privacy has been compromised.

In the case of *United States v. Jones*, while the justices reached the same conclusion by different means, Kerr argues that all three decisions used the mechanism of equilibrium adjustment to formulate their rationales.[55] In his article defending the theory of equilibrium adjustment, Kerr argues that Justice Scalia engaged in equilibrium adjustment through an originalist framework.[56] Justice Scalia argued that the reasonable expectation of privacy test could not be applied to public locations of a car, and thus employed the trespass doctrine to reach his desired level of protection in this case. Though Justice Scalia reached a narrower decision on privacy than Justices Alito and Sotomayor, he nevertheless attempted to restore the balance

[55] Orin S. Kerr, "Defending Equilibrium-Adjustment," *Harvard Law Review Forum* 125 (May 18, 2012): 84–90. https://harvardlawreview.org/2012/05/defending-equilibrium-adjustment/.
[56] Kerr, "Defending Equilibrium Adjustment," 88.

between government interest and individual privacy through the framework of the equilibrium adjustment theory.

Kerr argues that Justice Alito's concurrence reveals that he engaged in equilibrium adjustment using the *Katz* reasonable expectation of privacy test. Justice Alito suggested that the extensive GPS monitoring used in *Jones* exceeded what a reasonable person expected from police surveillance.[57] Additionally, because in the pre-computer age no sort of long-term invasive surveillance would have been reasonable to expect, Justice Alito asserted that the Court must strengthen privacy protection to fix the balance that skewed towards too powerful police tools.

Finally, Kerr argues that Justice Sotomayor's concurring opinion also engaged in equilibrium adjustment. In fact, Justice Sotomayor explicitly stated that the government's use, or rather misuse, of GPS monitoring "may alter the relationship between citizen and government in a way that is inimical to democratic society."[58] As a result of the upset in balance between police power and individual privacy, Justice Sotomayor contends that continued surveillance of one's locations, which reveals an intimate portrait of one's life, is a Fourth Amendment search. Justice Sotomayor, like Justice Alito tipped the scale towards greater privacy protections to restore a limit on police power that existed before the use of GPS surveillance.[59]

Orin Kerr's theory of equilibrium adjustment postulates that the Court engages in adjusting the scope of the Fourth Amendment when faced with modern tools and technologies that upset a balance of power between the police and citizens. While for some justices this looks like retaining the balance that existed at the time of the adoption of the Fourth Amendment,

[57] Kerr, "Defending Equilibrium Adjustment," 88-89.
[58] Kerr, "Defending Equilibrium Adjustment," 89.
[59] Kerr, "Defending Equilibrium Adjustment," 88.

others seek to maintain the balance of power that existed before the tool or technology in question came into use. Both methods of judicial decision making are forms of equilibrium adjustment and both, according to Kerr, are "instinctual."

The theory of equilibrium offers a concise explanation for the course of Fourth Amendment jurisprudence over the past century. In an effort to maintain the balance between police power and individual privacy, the Court has consistently considered the implications of new technologies and new tools employed by both police officers and criminals and ruled to strengthen or weaken privacy protections to restore the prior balance. Though Kerr concedes this theory does not provide a way to predict how the Court might respond to future technologies and practices, it does suggest that the Court rests its Fourth Amendment decisions on the need to preserve a constant balance between the powers of the police to investigate crimes and the power of people to be secure in their right to privacy.

Considering the rapidly changing technology in the digital age, legal scholars and judges alike have recognized the challenges of utilizing a traditional application of the Fourth Amendment. The terms "houses, papers, and effects" cannot be understood as comparable to the cellphones we carry in our pockets or the computers we keep on our desks, nor can traditional understandings of reasonable expectations of privacy be applied to the world of modern technology. In responding to these challenges, the Supreme Court has played a significant role in shaping Fourth Amendment jurisprudence, engaging in continuous equilibrium adjustment to maintain the balance between police power and individual privacy. In my next chapter, I will discuss the Court's most recent decision in this line of digital Fourth Amendment case law. I will return to a discussion of the third-party doctrine and its implications for privacy in the digital age, consider where the Court stands in terms of adopting the mosaic theory approach to the

Fourth Amendment, and argue that the Court demonstrated another attempt at equilibrium adjustment in the landmark case *Carpenter v. United States.*

Chapter 2

The Supreme Court's next and most recent decision concerning the Fourth Amendment in the digital age came in 2018, when the Court handed down its decision in the landmark case *Carpenter v. United States*.[60] Here, for the first time, the Court was asked to consider the constitutionality of obtaining a collection of historical cell site location information without a warrant. In a decision that would effectively reshape the *Katz* reasonable expectation of privacy test and shrink the long-standing third-party doctrine, the Court ruled that the government's acquisition of an individual's cell site location information, or CSLI, over an extended period constituted a Fourth Amendment search. *Carpenter* established that a warrant is required when the government wants to obtain a person's historical CSLI for more than seven days.[61]

Carpenter v. United States

In 2011, four men were arrested on suspicion of having been involved in a string of armed robberies in Detroit, Michigan. During the ensuing investigation, one of the suspects cooperated with the FBI and turned over the phone numbers of 15 accomplices, each involved in at least one of the several robberies.[62] Among these individuals was Timothy Ivory Carpenter, who at trial was identified as the leader of the operation.[63] Upon receiving the names and phone numbers of Carpenter and several other suspects, the government submitted three applications for court orders to access the historical cell phone location records belonging to Carpenter and

[60] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[61] Id. at 2217 n.3.
[62] Brief for Petitioner at 5, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402), https://www.aclu.org/legal-document/united-states-v-carpenter-brief-petitioner.
[63] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

the other suspects.[64] These court orders, issued under the Stored Communications Act Section 2703(d), require the government meet a lesser standard than the probable cause required for warrant to access digitally stored electronic communications. Section 2703(d) of the SCA provides that the government may require the disclosure of customer records information if it "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[65] Magistrate judges granted the orders and the government was able to obtain 127 days – of the requested 152 days – worth of Carpenter's cell site location information.[66]

Cell site location information is produced and recorded every time a cell phone connects to a cell tower. Cell phones connect to cell towers constantly, for example when the user makes or receives a phone call, sends or receives a text message, and even when cell phones perform routine data connections.[67] Cell phones connect to cell sites even when the device is not in use but is simply turned on.[68] Historical CSLI refers to records of prior cell tower connections, which reveal the past locations of cell phones, and the cell phone user. These records can be held by service providers for various business purposes for up to five years.[69]

The CSLI records collected for Timothy Carpenter's cell phone revealed 12,898 location points spanning 127 days.[70] This information allowed the government to access Carpenter's

[64] Brief for Petitioner, 5.
[65] Stored Communications Act, 18 U.S.C. § 2703(d).
[66] Brief for Petitioner, 6-7.
[67] Brief for Petitioner, 4.
[68] Brief for Electronic Privacy Information Center (EPIC) et al. as Amici Curiae Supporting Petitioner at 18, Carpenter v. United States 138 S. Ct. 2206 (2018) (August 14, 2017) (No. 16-402). https://epic.org/wp-content/uploads/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.
[69] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).
[70] Brief for Petitioner, 8.

location an average of 101 times per day, over the course of more than four months,[71] and place Carpenter in the general area of the robberies at around the same time as the crimes were committed. When Carpenter moved to suppress the historical CSLI, arguing that the government had conducted an unlawful Fourth Amendment search, the district court denied his motion. The court denied Carpenter's claims to a reasonable expectation of privacy in his historical CSLI and found the third-party doctrine applicable to the case. More than four months' worth of CSLI were used against Carpenter at trial, and a jury convicted him of six robberies, with additional counts for carrying a firearm. Carpenter was sentenced to more than 100 years in prison.[72]

A panel of the Sixth Circuit Court of Appeals affirmed the decision. The judges differentiated CSLI from what Carpenter argued was comparable GPS data, arguing that the CSLI records belonged to the cellular service providers for business purposes, not the user of the phone. Thus, the court reasoned, Carpenter's Fourth Amendment rights had not been implicated in the government's seizure of his long term historical CSLI, and the third-party doctrine governed this case.

In 2017, Carpenter's case came before the Supreme Court. Carpenter first set out to convince the Court that the CSLI records in this case were comparable to the highly sensitive and revealing GPS location information in *Jones*, which five justices agreed was deserving of constitutional protection. In *Jones*, five justices found that people have a reasonable expectation of privacy in the long-term GPS monitoring of their physical movements because this information can reveal personal details about one's private life and associations.[73] Furthermore, a majority of the justices in *Jones* conceded that, prior to the digital age, the data generated by a

[71] Brief for Petitioner, 8.
[72] Brief for Petitioner, 9.
[73] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)

GPS device over an extended period of time could not have possibly been gathered by traditional surveillance methods. Therefore, the justices argued that the government's use of GPS surveillance to track the whereabouts of a suspect exceeded society's expectations of what the police can learn about an individual.[74]

In *Carpenter*, the petitioner argued that the government's acquisition of 127 days of CSLI violated Carpenter's reasonable expectation of privacy, and for similar reasons five justices found GPS data violated a reasonable expectation of privacy in *Jones.* First and foremost, the petitioner highlighted that the information gathered by the government in this case was generated by a cell phone – a device which 95% of Americans use and carry constantly throughout their everyday lives.[75] Cell phone users bring their devices to work, school, on public transportation, to appointments, and, for 12% of Americans, even in the shower.[76] The location details collected by a modern-day cell phone can reveal some of the most intimate details of a person's life, including when an individual is in their own home. Furthermore, in his oral argument before the Court, Carpenter's attorney Nathan Wessler argued that the detailed and intimate nature of cell phone location data makes it even more deserving of Fourth Amendment protection than the GPS data gathered in *Jones*. While Wessler conceded that the data generated by CSLI is less precise than that of a GPS device, he argued that GPS tracking lacks a critical feature of CSLI. GPS tracking devices, Wessler explained, are limited to obtaining information for the location points of a car, but cell phones travel in most people's pockets to every location they visit, including doctor's offices, shops, and inside the home.[77] Thus, even though each CSLI data point

[74] Id. at 430 (Alito, J., concurring).
[75] Oral Argument at 25:30, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402), https://www.supremecourt.gov/oral_arguments/audio/2017/16-402.
[76] Brief for Petitioner, 17.
[77] Oral Argument at 26:40, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

in this case was less precise than data points of a GPS, the locations in which these data recorded location information were far more invasive. Additionally, Wessler notes that between the time Carpenter's CSLI was obtained and when the case reached the Supreme Court, an increase in cell towers, particularly in urban areas, and a significant increase in data usage resulted in the generation of greater and more detailed CSLI.[78] The petitioner highlighted for example, that instead of simply collecting location information at the start and end of a phone call, historical CSLI has advanced to the point where data is collected for text messages, checking email, and many involuntary actions, including when social media apps contact a network for new messages.[79]

Wessler argued that long-term tracking of CSLI triggers a reasonable expectation of privacy that individuals have in their physical movements and in the intimate portrait this data creates, and, crucially, that the historical nature of this information strengthens the petitioner's demand for constitutional protection. Prior to the development of historical CSLI records, law enforcement was limited in the amount of information it could learn about a suspect, retrospectively. As the petitioner notes, police officers could have only gained knowledge about a suspect's historical location records by combining, for example, employee time cards, store receipts, or fragments of security camera footage.[80] These modes of surveillance, the petitioner argued, "pale in comparison to the unprecedented surveillance time machine that CSLI provides."[81] Because the wealth and intimacy of knowledge conveyed by historical CSLI could never have been obtained using traditional tools of investigation, and goes far beyond what

[78] Oral Argument at 27:05, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).
[79] Brief for Petitioner, 28.
[80] Brief for Petitioner, 18.
[81] Brief for Petitioner, 11.

people expect law enforcement can access, Carpenter asserted that he had a reasonable expectation of privacy, that society would also deem reasonable, to his historical CSLI.

The petitioner's second main argument aimed to convince the Court that the third-party doctrine could not govern this case. Carpenter claimed that the nature of historical CSLI is so unlike the types of information addressed in *Smith* and *Miller*, both in sensitivity and in how the information is generated, that the third-party doctrine could not be mechanically applied in this case.

First, the petitioner articulated that the "sensitive and personal" nature of historical CSLI sets it apart, significantly, from the limited records in both *Smith* and *Miller*.[82] In those pre-digital age cases, the information obtained by the government conveyed only several days of dialed phone numbers,[83] and several months of banking records,[84] respectively. The key difference here, the petitioner argued, is that in neither of those earlier cases could the government have used those records to generate a comprehensive, long term, and detailed account of a person's "locations, movements, and associations."[85] Thus, the petitioner argued, the Court must find that the sensitivity of the information in Carpenter's case greatly outweighs the privacy concerns in those pre-digital cases.

Additionally, the petitioner argued that the information presented in this case is not conveyed voluntarily "in any meaningful way."[86] In this case, the government argued that the risk of having one's location information disclosed to the government is assumed when a person decides to carry a cell phone.[87] The petitioner argued, however, that adopting this argument

[82] Brief for Petitioner, 36.
[83] Smith v. Maryland, 442 U.S. 735 (1979).
[84] United States v. Miller, 425 U.S. 435 (1976).
[85] Oral Argument at 2:53, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).
[86] Brief for Petitioner, 39.
[87] Brief for Petitioner, 39.

would be inconsistent with how the Court has previously treated modern day cell phone use. In *Riley*, for example, the Court held that smartphones have become a necessary part of daily life: "cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[88] Consistent with this understanding of the pervasiveness and necessity for cell phone use in modern society, Carpenter reasoned that the Court must find that simply owning and carrying a cell phone does not suffice to meet the voluntary standard for applying the third-party doctrine. The petitioner further asserted that the production of location data also cannot be seen as voluntary. While it may be assumed that cell phone users understand that they must be near a cell tower to communicate over the phone, the petitioner explained, it is "outlandish to extrapolate from that minimum knowledge the conclusion that people knowingly and voluntarily disclose their every movement to the government."[89] Furthermore, many of the ways in which CSLI is produced do not require action to be taken by the user. By simply having one's cell phone turned on, a user is subject to constant tracking by CSLI generation. "There is no way to avoid the aggregation and retention of this location information short of turning off or disabling the phone."[90] In fact, the petitioner points out that cellular service providers do not allow for users to opt-out of location tracking and logging, as is the case with many cell phone apps that track phone user's location.[91] Carpenter argued that, not only is this sharing of location information involuntary, but it is also inescapable. Where the Court found a level of voluntariness on the part of the individuals in *Smith* and *Miller*, and, thus, a reduced privacy interest in both types of limited information, the Court could not determine the same here. Carpenter argued he did not, in

[88] Riley v. California, 573 S. Ct. 373, 385 (2014).
[89] Brief for Petitioner, 44.
[90] Brief for Petitioner, 42.
[91] Brief for Petitioner, 56.

any sense, voluntarily convey his sensitive and private CSLI. Therefore, he retained a reasonable expectation of privacy in this information even though it was held by a third-party.

The petitioner made one final argument regarding the third-party doctrine and historical CSLI. Carpenter claimed that, if the Court were to extend the third-party doctrine to such sensitive and involuntarily conveyed information as historical CSLI, other forms of digital information – including contents of communication – would be reviewed under this obsolete doctrine.[92] The petitioner highlights that the "so-called 'internet of things'" has made it so that even information regarding home appliances, a person's body, nutrition, and sexual activity are recorded and stored on third-party servers.[93] The petitioner warned that if the Court were to accept the government's argument that the third-party doctrine governs this case, a plethora of additional deserving information would lose Fourth Amendment protection.

Carpenter concluded that the Court must require the government to get a warrant, supported by probable cause, to obtain long term historical CSLI. Because Carpenter was entitled to a reasonable expectation of privacy in his CSLI, as the petitioner demonstrated, a warrantless search of this information is a violation of the Fourth Amendment. The petitioner urged the Court to accept that any acquisition of historical CSLI must be accompanied by a warrant.

During oral arguments, Carpenter's lawyer argued that the Stored Communications Act, the privacy law upon which the government acquired Carpenter's CSLI, is unsuitable to guide law enforcement conduct as it relates to historical CSLI. Wessler explained that in 1986, when Congress passed the Stored Communications Act, "less than one half of one percent of

[92] Brief for Petitioner, 44.
[93] Brief for Petitioner, 45-6.

Americans had a cell phone and only 1,531 cell sites existed in the United States.[94] When the SCA was amended in relevant part in 1994, the percentage of Americans who had cell phones only increased to about nine percent, and the number of cell sites across the country remained under 18,000.[95] In 2017, 95 percent of Americans had cell phones,[96] and the number of cell sites in the United States was around 300,000.[97] Wessler argued that Congress had not anticipated either "the contemporary ubiquity of cell phones," or "the volume and precision of CSLI that would be retained by service providers," in the digital age.[98] The SCA is out of touch with the privacy interests that have emerged in recent decades. Therefore, the petitioner argued, "no deference to this outdated legislative scheme is warranted with respect to CSLI."[99]

The Court's Ruling

In 2018, the Court delivered its ruling in *Carpenter v. United States*. In a 5-4 decision, a majority of the Court held that the governments' acquisition of long-term CSLI was a Fourth Amendment search.[100] The Court determined that people have a reasonable expectation of privacy in their aggregated location data, even when that information is collected and held by a third-party. Thus, the Court established that, at least in some sensitive cases, the third-party doctrine does not automatically override privacy interests.

Chief Justice Roberts wrote the opinion for the Court, joined by Justices Breyer, Kagan, Ginsburg, and Sotomayor. The Chief Justice begins the opinion with an overview of the type of

[94] Brief for Petitioner, 50.
[95] Brief for Petitioner, 50.
[96] Oral Argument at 25:30, Carpenter v. United States, 138 S. Ct. 2206, 2208 (2018) (No. 16-402).
[97] Brief for Petitioner, 50.
[98] Brief for Petitioner, 50.
[99] Brief for Petitioner, 49.
[100] Carpenter v. United States, 138 S. Ct. 2206, 2208 (2018).

information at issue in the case, CSLI. Reminiscent of the petitioner's argument, he highlights the pervasiveness of cell phone use in modern day, as well as the constant, automatic, and involuntary nature by which CSLI is recorded and retained by cell service providers.[101] The Chief Justice then explains that the Court's approach to Fourth Amendment cases involving innovative surveillance tools has historically recognized that the Fourth Amendment protects "certain expectations of privacy."[102] Thus, the goal of the Court is – and has been – to ensure that, as modern technology advances and redefines police powers, the Fourth Amendment continues to adequately protect '"the privacies of life" against 'arbitrary power.'"[103]

> As 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 the government that existed when the Fourth Amendment was adopted."[104]

Following the Chief Justice's emphasis on the Court's responsibility to protect privacy interests against unreasonable police powers, he asserts that this case does not "fit neatly under existing precedents."[105] Rather, this case implicated a set of decisions involving a person's reasonable expectation of privacy in their movements and locations, and cases involving information voluntarily disclosed to a third-party entity. In *Jones,* the Court held that the government's installation of a GPS device on the petitioner's car, and the subsequent tracking of his movements and locations, amounted to a Fourth Amendment search – with five justices accepting that a search occurred because of a reasonable expectation of privacy. Here, the CSLI

[101] Id. at 2211-2.
[102] Id. at 2213.
[103] Id. at 2214 (quoting Boyd v. United States, 116 U.S. 616 at 630 (1886)).
[104] Id. at 2214 (quoting Kyllo v. United States, 533 U.S. 27 at 34 (2001)).
[105] Id. at 2214.

was distinct in that it involved information held by a third party. Ultimately, however, the Chief Justice argued that the third-party doctrine could not be applied to the facts in *Carpenter*.[106]

Accepting several of the key arguments made by the petitioner, Chief Justice Roberts asserted that the unique nature of the CSLI in this case challenged a traditional application of the third-party doctrine. In holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," the Court concluded a Fourth Amendment search had occurred.[107]

In his reasoning, Chief Justice Roberts articulates several key factors which led the majority to find a reasonable expectation of privacy in a person's CSLI records. First, the Chief Justice highlights the detailed, revealing, and intimate nature of location information.

> As with GPS information, the time-stamped data 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."[108]

The Court, Chief Justice Roberts argued, has already recognized that the long-term monitoring of a person's every move exceeds what society expects the police have the capacity to learn. This same expectation exists here. Furthermore, the Chief Justice accepted the petitioner's argument that historical CSLI raises heightened privacy concerns compared to GPS information. Cell phones, unlike cars, he argued, follow the user into nearly every place they go.[109] Collecting a person's CSLI, it follows, can equate to "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone user."[110]

---

[106] Id. at 2217.
[107] Id. at 2217.
[108] Id. at 2217 (quoting Jones, at 415 (Sotomayor, J., concurring)).
[109] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).
[110] Id. at 2218.

The opinion also highlights a significant privacy interest in historical CSLI because of its retrospective quality. The Chief Justice again references the idea that society expects practical limitations to stand in the way of police surveillance, but that these practical limitations have diminished in the face of modern technologies. Prior to the digital age, the government was constrained by "a dearth of records and the frailties of recollection," the Chief Justice argued. [111] Today, on the other hand, CSLI allows the government to trace the past locations of all cell phone users going back years, merely depending on the policies of service providers.[112] Crucially, this retrospectivity, unique to historical CSLI, enables the information to implicate all phone users, not just criminal suspects. The Chief Justice asserts that "only the few without cell phones could escape this tireless and absolute surveillance."[113]

Additionally, despite the government's argument that the CSLI presented in this case is less precise than the GPS data in *Jones*, Chief Justice Roberts asserts that the Court must consider where the technology is headed. He writes, "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or development.'"[114] Furthermore, the Chief Justice recognized, as the petitioner pointed out, that the records gathered here were a product of the technology at the beginning of the decade. Not only has CSLI become more accurate, but the majority asserted it is quickly approaching the precision of GPS data.[115] Here, the Chief Justice explicitly accounts for the continuous development of CSLI that is likely to come and pose even greater privacy concerns than the records present in the case.

[111] Id. at 2218.
[112] Id. at 2218.
[113] Id. at 2218.
[114] Id. at 2218 (quoting Kyllo v. United States, 121 S. Ct. 2038).
[115] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

Chief Justice Roberts then explains why the third-party doctrine cannot apply in this case. He contends with the petitioner that the government fails to appreciate the evolution of tracking in the digital age. The Chief Justice argues not only has modern CSLI made every cell phone user susceptible to constant tracking, but the nature of the tracking has also changed: "Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."[116] The majority of the Court found that the "exhaustive chronicle of location information"[117] that long-term CSLI produces could not be compared to the limited personal information in *Smith* and *Miller.* Thus, the Chief Justice asserts, "the Government…is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information."[118]

The Court also asserted, as the petitioner argued, that CSLI was distinct from the types of information in *Smith* and *Miller* in voluntariness – defeating the second rationale of the third-party doctrine. Given that the Court asserted both that having a cell phone is "indispensable to participation in modern society,"[119] and that "a cell phone logs a cell-site records by dint of its operation, without any affirmative action on the part of the user," the majority held that CSLI in "no meaningful sense" requires the user to assume the risk of the whole of their movements being exposed.[120]

Though the Court held that the third-party doctrine did not apply to Carpenter's long-term historical CSLI in this case, the majority opinion claimed the decision was "a narrow

[116] Id. at 2219.
[117] Id. at 2219.
[118] Id. at 2219.
[119] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[120] Id. at 2220.

one."[121] Chief Justice Roberts explained that this decision did not disturb *Smith* and *Miller*, nor answer questions about real-time CSLI or "call into question conventional surveillance techniques and tools."[122] In my next chapter I will illuminate the merits of the majority's claim that *Smith* and *Miller* remain intact post-*Carpenter*.

The Chief Justice concluded that the Court's finding of a Fourth Amendment search in this case necessitates a warrant for future government acquisition of historical CSLI.[123] The majority argued that the criteria for obtaining CSLI under a SCA court order is out of line with the privacy interest in this type of record. Therefore, if the government wants to gain access to CSLI, it must first obtain a warrant issued on probable cause.

The Chief Justice finishes the majority opinion by reiterating the Court's reasoning for limiting the scope of the third-party doctrine in this case and extending Fourth Amendment protection to historical CSLI:

> In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.[124]

Kerr & Ohm on *Carpenter*

Since the Supreme Court delivered its decision in *Carpenter v. United States*, Fourth Amendment scholars have devoted significant attention to interpreting the Court's opinion, attempting to understand the new Fourth Amendment test and the Court's legal reasoning. In this

[121] Id. at 2220.
[122] Id. at 2220.
[123] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
[124] Id. at 2223.

section, I will explore some of the key takeaways that scholars in the field have highlighted as they have examined the Court's landmark decision.

Leading Fourth Amendment scholar Orin Kerr has dedicated two chapters of his forthcoming book, titled *The Digital Fourth Amendment*, to dissecting the *Carpenter* opinion. In them, he explains how the decision changed Fourth Amendment jurisprudence and provides a guide for how lower courts can apply the new *Carpenter* legal framework.[125] Kerr first argues that *Carpenter* reshaped the *Katz* reasonable expectation test from an analysis of privacy interests in places and things to an analysis of what certain information has the capacity to reveal.[126] Kerr explains that a close analysis of Fourth Amendment case law reveals the Court has, until *Carpenter*, focused its decisions on a reasonable expectation of privacy in places and things.[127] He asserts *Katz* did not end the place-based doctrine.[128] Rather, Kerr argues that the *Katz* reasonable expectation of privacy test historically asked whether a person had a reasonable expectation of privacy in a place or thing because it was "sufficiently home-like to merit Fourth Amendment rights."[129] Kerr asserts that *Carpenter* represents the first major break from this precedent, ushering in a new privacy test that "focuses on how much the government can learn about a person regardless of the place or things from which the information came."[130] The post–*Carpenter* test asks whether technology has lifted a prior limit on government power that society has recognized as reasonable.

Kerr suggests that the Court's reformulation of the *Katz* test was a product of equilibrium adjustment. Kerr's theory of equilibrium adjustment states that when new technologies transform

[125] Kerr, "Implementing Carpenter."
[126] Kerr, "Implementing Carpenter," 1.
[127] Kerr, "Implementing Carpenter," 3.
[128] Kerr, "Implementing Carpenter," 5.
[129] Kerr, "Implementing Carpenter," 6.
[130] Kerr, "Implementing Carpenter," 6.

government power, and, in turn threaten citizens' privacy, the Court adjusts Fourth Amendment rules "to restore preexisting limits on that power."[131] In *Carpenter,* Kerr argues, a majority of the Court demonstrated concerns that people can no longer protect their private information in the digital age. "The sensitive records have moved," Kerr writes.[132] "A majority of the Justices felt they needed a new way for the Fourth Amendment to protect private information wherever it went."[133] So, Kerr argues, equilibrium adjustment led the Court to adopt a new Fourth Amendment approach in response to privacy concerns in the digital age. This approach focuses on how technologies have enabled the police to use surveillance tools which were previously nonexistent rather than on our reasonable expectation so privacy with regard to particular items or places.

Interestingly, Kerr argues that the Court's case for equilibrium adjustment here was premature. The state of CSLI, he asserted, was not quite as invasive and revealing as the Court claimed.[134] Kerr explains that the evidence in the case only placed Carpenter within the span of a half-mile to two miles from a cell tower when a call was made or ended.[135] This range indicated only the general neighborhood in which Carpenter's phone was located.[136] Though Kerr concedes the amount of information the government obtained was extensive, he emphasizes that the reality of CSLI's precision and invasiveness does not quite live up to the Court's description of it as "deeply revealing," an "exhaustive chronicle" of one's movements, or "absolute surveillance."[137] In his opinion, the Chief Justice explains that the Court must respond to the

[131] Kerr, "Implementing Carpenter," 8.
[132] Kerr, "Implementing Carpenter," 8.
[133] Kerr, "Implementing Carpenter," 8.
[134] Kerr, "Implementing Carpenter," 10-1.
[135] Kerr, "Implementing Carpenter," 12.
[136] Kerr, "Implementing Carpenter," 12.
[137] Kerr, "Implementing Carpenter," 13.

direction in which CSLI is headed – one of "GPS-level precision,"[138] but Kerr finds this argument unconvincing. Kerr recommends the Court engage in equilibrium adjustment once a new technology has stabilized, and not in an effort to predict what protections may be necessary in the future.[139] Nevertheless, Kerr argues that the Court did create a framework that can apply to other digital technologies that do raise the kinds of privacy concerns expressed in *Carpenter*.[140] Kerr provides a three-requirement test, consistent with the Court's opinion in *Carpenter*, for applying these new Fourth Amendment rules to various other categories of records.

First, Kerr identifies that the records collected must be "available because of digital technology."[141] Kerr argues that a *Carpenter* search should only be triggered when the information "could not be collected in a pre-digital age."[142] This requirement, Kerr explains, comes directly out of the language in the majority opinion of *Carpenter.* The Chief Justice distinguished the CSLI in this case because, as a result of "seismic shifts in digital technology,"[143] CSLI is "an entirely different species"[144] of record, that did not "fit neatly under existing precedents."[145] As the majority opinion articulated, long-term CSLI generation has changed expectations about what law enforcement can do and ultimately earned Fourth Amendment protection because it was incomparable to any record that came before it. Thus, Kerr argues, *Carpenter* does not implicate traditional surveillance tools that existed prior to the digital age.[146] Again, Kerr argues that this feature of a *Carpenter* search is premised on

[138] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[139] Kerr, "Implementing Carpenter," 15.
[140] Kerr, "Implementing Carpenter," 11.
[141] Kerr, "Implementing Carpenter," 16.
[142] Kerr, "Implementing Carpenter," 16.
[143] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[144] Id. at 2222.
[145] Id. at 2214.
[146] Kerr, "Implementing Carpenter," 17.

equilibrium adjustment.[147] In prior Fourth Amendment cases, the Court found searches occurred when a modern technology implicated privacy concerns akin to those in a protected place, like the home. For example, in *Katz*, the Court held that a person is entitled to Fourth Amendment protection in a phone booth, as it raised similar privacy concerns to those of a home. Kerr explains that, unlike this traditional framework, the Court now understands that new technologies and the internet are entirely different and new Fourth Amendment rules for these digital age technologies are necessary.

Kerr also maintains that a record must be created "without…meaningful voluntary choice" to meet the requirements of a *Carpenter* search.[148] In *Carpenter*, the Court held that the third-party doctrine could not apply to CSLI because the tracking was inescapable – the Court found it implausible that having a cell phone is a voluntary choice in modern society given its pervasiveness in all aspects of daily life. Thus, Kerr concludes that the Court in *Carpenter* recognized there are some types of information that we are essentially required to reveal by virtue of participating in modern life.[149] The Fourth Amendment covers this type. Understood as yet another form of equilibrium adjustment, Kerr asserts that the Court reimagined what voluntariness means in the digital age. Crucially, though, Kerr emphasizes the majority opinion's assertion that *Carpenter* does not upset the precedent of *Smith* and *Miller*. Rather, Kerr argues *Carpenter* narrowly tailored the third-party doctrine, or placed an "equilibrium-adjustment cap" on it.[150] While information that is inevitably shared for participation in modern society post-

[147] Kerr, "Implementing Carpenter," 18.
[148] Kerr, "Implementing Carpenter," 20.
[149] Kerr, "Implementing Carpenter," 21.
[150] Orin Kerr, "Understanding the Supreme Court's Carpenter Decision," *Lawfare* (blog), June 22, 2018, https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision.

Carpenter will receive protection, Kerr argues that information which is *not* conveyed for necessary participation in modern life is likely left unprotected.[151]

Kerr argues that the final *Carpenter* requirement is that the record in question "be of a kind that tends to reveal an intimate portrait of a person's life typically beyond legitimate state interest."[152] Kerr highlights that *Carpenter* prevents the government from being able to access a great deal of private and personal information about individuals, especially information irrelevant to criminal investigations, by limiting its access to records which have the tendency to reveal such intimacies.[153] This decision relied on the Court's long-standing commitment to protecting information that reveals "the privacies of life," with a high level of scrutiny. In Justice Sotomayor's concurrence in *Jones*, she emphasizes that extensive location tracking has the potential to reveal intimate details of one's life including their "familial, political, professional, religious, and sexual associations."[154] As many judges have agreed, these personal facts are of no legitimate interest to the government, and in fact, consist of some of the most intimate facts that people generally avoid sharing with the government.[155] Thus, the Court also established that when a new technology reveals intimate and personal details of a person's life it is likely to receive *Carpenter* protection.

In his interpretation, Kerr argues that while *Carpenter* constitutes a premature effort of equilibrium adjustment, it is a "resounding win" for the theory which aims to retain the proper balance of police powers and privacy protections.[156] Kerr explains that the *Carpenter* Court broke away from a traditional understanding of the *Katz* privacy test, to one that examines

[151] Kerr, "Implementing Carpenter," 22.
[152] Kerr, "Implementing Carpenter," 22.
[153] Kerr, "Implementing Carpenter," 22.
[154] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).
[155] Kerr, "Implementing Carpenter," 24-6.
[156] Kerr, "Implementing Carpenter," 1.

whether technology enables police conduct to violate our expectations, rather than whether the source of the information is deserving of a privacy claim. Kerr also understands that *Carpenter* established a new test, likely to apply to digital technologies novel in the digital age that gather information about individuals without their voluntary choice and tend to reveal the intimate details of people's lives. Ultimately, Kerr demonstrates that the Court was able to, once again, bring Fourth Amendment doctrine in line with the privacy concerns of the digital age in *Carpenter*, and rebalance the scale to ensure modern day technologies do not enable the government to encroach on personal privacy in ways previously unimaginable.

Paul Ohm, another prominent scholar of information privacy and the law, has also written about the Court's decision in *Carpenter v. United States*. In his article for the *Harvard Journal of Law and Technology*, Ohm argues that *Carpenter* brought a "series of revolutions" to Fourth Amendment jurisprudence.[157] Ohm begins by defending the multi-factor test that came out of *Carpenter* but suggests that a rule which he calls technological equivalence may end up becoming the most influential *Carpenter* rule in the future.[158] Ohm also asserts that the Court's recognition of a "tech exceptionalism" had led to a revolution in Fourth Amendment reasoning by redefining the *Katz* reasonable expectation test. Ohm's interpretation reflects similarities to Kerr's ideas of equilibrium adjustment and the changes the *Carpenter* Court made to legal reasoning in the face of modern technology. However, Ohm celebrates the Court's eagerness to extend Fourth Amendment protections to evolving technologies in a way that Kerr critiques.

Ohm interprets the *Carpenter* multi-factor test as arising from the concluding statements of Chief Justice Roberts' opinion. "When the police seek to obtain information about individual

[157] Paul Ohm, "The Many Revolutions of Carpenter," *Harvard Journal of Law and Technology* 32, no. 2 (Spring 2019): 357–416, 358, https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech357.pdf.
[158] Ohm, "The Many Revolutions of Carpenter," 360.

behavior contained in a private party's database," Ohm writes, "the court examines (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."'[159] In his analysis of these three factors, Ohm largely reiterates the defense for this test that the Chief Justice provides in his opinion. The Court ruled the acquisition of long term CSLI was a search because location information in aggregate can reveal deeply personal facts about one's life – triggering the first factor; the technology runs against everyone and is retrospective in nature – triggering the second factor; and CSLI is largely inescapable in the modern day and automatically generated – fulfilling the third factor of the test. Ohm argues these factors provide guidance for determining whether an individual has a reasonable expectation of privacy in a particular database, and then if third-party doctrine applies.[160] However, Ohm suggests that a rule which has been implicitly endorsed by seven justices on the Court – the rule of technological equivalence – may end up becoming the most frequently cited *Carpenter* rule.[161]

Ohm argues that this rule of tech equivalence stems from the Court's opinion in *Kyllo v. United States,*[162] a case where the Court held the police needed to obtain a warrant to use a thermal imaging device on the outside of a person's home. In that case, the majority's key argument was that the thermal imaging device enabled the government to explore features of the interior of a home that it could have only otherwise known by physically entering the home. In *Kyllo*, the Court established a principle which Ohm argues *Carpenter* expanded upon. Ohm writes that the rule of technological equivalence states that "if a technology, or a near-future

[159] Ohm, "The Many Revolutions of Carpenter," 361 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018)).
[160] Ohm, "The Many Revolutions of Carpenter," 369-70.
[161] Ohm, "The Many Revolutions of Carpenter," 360.
[162] Kyllo v. United States, 533 U.S. 27 (2001).

improvement, gives police the power to gather information that is the 'modern-day equivalent' of activity that has been held to be a Fourth Amendment search, the use of that technology is also a search."[163]

Ohm articulates three specific rules of technological equivalence which can help guide future Fourth Amendment cases more easily than the *Carpenter* multi-factor test. The first of these three rules stipulates that the Fourth Amendment protects information from new technologies that reveal "details from inside the home."[164] Ohm explains that this line of reasoning likely extends Fourth Amendment protections to "devices that comprise the Internet of Things," like Amazon and Google smart homes and advanced thermostats.[165] Here, the rule of technological equivalence need not require that courts assess the sensitivity of the information. As the Court found in *Kyllo,* "all details [of the home] are intimate details."[166] Ohm argues that the simplicity of this framework, compared to the multi-factor test, is compelling and might result in this becoming a key factor in future decisions.[167]

The second conceptualization of the rule of technological equivalence references the law of bailment. The law of bailment, most fundamentally, states that when an individual entrusts another with their property, the bailee has a legal duty to protect the items they are holding.[168] Ohm points out that Justices Kennedy and Gorsuch, two dissenting justices in *Carpenter*, have expressed support for the law of bailment as a legal rationale for limiting the third-party doctrine.[169] In his *Carpenter* dissent, Justice Gorsuch writes: "Just because you entrust your data–in some case, your modern-day papers and effects–to a third party may not mean you lose

[163] Ohm, "The Many Revolutions of Carpenter," 360.
[164] Ohm, "The Many Revolutions of Carpenter," 395.
[165] Ohm, "The Many Revolutions of Carpenter," 395.
[166] Kyllo v. United States, 533 U.S. 27, 37 (2001).
[167] Ohm, "The Many Revolutions of Carpenter," 396.
[168] Ohm, "The Many Revolutions of Carpenter," 397.
[169] Ohm, "The Many Revolutions of Carpenter," 397.

any Fourth Amendment interest in its contents."[170] Ohm argues that because a larger majority of the Court supports the tech equivalence rule of bailment, rather than the complex three-factor test the majority put forth, this could guide future third-party Fourth Amendment cases.

The third application of the rule of technological equivalence applies to private communications. Ohm notes that all nine justices on the *Carpenter* Court conceded that the content of email messages must be protected by the Fourth Amendment.[171] Since the 1878 case of *Ex Parte Jackson*, which held a warrant was required to open sealed letters from the United States postal service,[172] one appellate court has extended this protection of physical mail to email messages.[173] Relying on this tech equivalence argument, Ohm suggests this Court's recognition of Fourth Amendment rights in email messages, or modern day letters, might lead courts to protect other forms of electronic communications.[174] The rule of technological equivalence to private communication could become the test in future content-related Fourth Amendment cases.

Ohm argues that this broad rule of technological equivalence has revolutionized Fourth Amendment reasoning. Beginning with the majority opinion in *Kyllo*, the Court has been developing this Fourth Amendment standard which grants Fourth Amendment protection to digital information that traditionally could have only been discovered through a Fourth Amendment search. *Carpenter*, Ohm asserts, solidified this rule.

Finally, Ohm argues that throughout the opinion in *Carpenter*, and beginning with *Riley*, the Court, and specifically the Chief Justice, has demonstrated "a belief in the exceptional nature of the modern technological era."[175] The Court's tech exceptionalism, Ohm argues, has led to

[170] Carpenter v. United States, 138 S. Ct 2206, 2268-69 (2018) (Gorsuch, J., dissenting).
[171] Ohm, "The Many Revolutions of Carpenter," 398.
[172] Ex Parte Jackson, 96 U.S. 727 (1877).
[173] United States v. Warshak, 631 F. 3d 266 (6th Cir. 2010).
[174] Ohm, "The Many Revolutions of Carpenter," 398.
[175] Ohm, "The Many Revolutions of Carpenter," 399.

several revolutions in legal reasoning. The revolution I will focus on here explains that tech exceptionalism led the *Carpenter* Court reinvent the *Katz* reasonable expectation of privacy test.[176]

Ohm highlights that *Katz* test has long been understood as consisting of two parts: First, it asks whether a person exhibited a subjective reasonable expectation of privacy, and second, whether society is ready to recognize that expectation as reasonable. Overtime scholars have debated whether the Court actually considers subjective expectations of privacy, or, instead, if it decides for the American people "the kind of society the Constitution seeks to protect."[177] Ohm argues that *Carpenter* settles confusion over this test.

> *Carpenter* selects the normative over the descriptive: the role of the courts is to protect the balance of power between the state (in the form of the police) and the people, refusing to let technological change eviscerate individual privacy and security from the state."[178]

In this passage, it is clear Ohm recognizes the Court's equilibrium adjustment in *Carpenter*. He explains that the Court's tech exceptionalism empowered it to take a proactive role uniquely necessary for the privacy concerns of the digital age. Ohm interprets *Carpenter* as the Court placing barriers in the way of invasive policing techniques as it saw the CSLI becoming more precise and invasive in the future. Kerr argues the same about equilibrium adjustment. While Kerr argues this equilibrium adjustment was premature because the Court reacted to the direction the technology was heading, not its state at the time of the decision, Ohm celebrates this forward-thinking approach.

> The unprecedented, rapidly changing nature of technology also causes the Court to relax its rules about restricting its attention to the record evidence before it…In *Carpenter* and *Riley*, the Court refused to resign itself to this fate. Instead, it relaxed, just slightly, its practices by peeking a little at the present and the future."[179]

[176] Ohm, "The Many Revolutions of Carpenter," 360.
[177] Ohm, "The Many Revolutions of Carpenter," 386.
[178] Ohm, "The Many Revolutions of Carpenter," 386.
[179] Ohm, "The Many Revolutions of Carpenter," 408.

The tech exceptionalism which Ohm identifies as driving much of the majority opinion in *Carpenter* has led the Court to treat technologies of the digital age differently than the technologies that came before them. The Chief Justice reasoned in *Carpenter* that the Court must take account of where the cell site location technology is heading and protect against the privacy harms to be caused in the future. Ohm praises Chief Justice Roberts for his reasoning and his recognition of the rapid-changing nature of technologies in the digital age.[180]

Both Kerr and Ohm argue that *Carpenter* infused several changes into Fourth Amendment law. These scholars concede that the majority opinion reshapes the *Katz* reasonable expectation test, though they argue it did so in distinct ways. Kerr argues *Carpenter* shifted the test to address how our expectations of police powers have changed in the digital age, while Ohm claims *Carpenter* replaced the traditional test altogether, ushering in a new proactive role for the judiciary to play in safeguarding privacy interests from future harms. Kerr suggests the Court's decision rests on a wrongfully portrayed set of facts, constituting a premature act of equilibrium adjustment, while Ohm celebrates the *Carpenter* Court's willingness to adjust the Fourth Amendment to account for developing technologies. Though these scholars provide nuanced understandings of the Court's motivation to extend Fourth Amendment protection to historical CSLI, and interpret the Court's opinion in different ways, both scholars contend that *Carpenter* constitutes a large shift in Fourth Amendment jurisprudence that rests on the principles of equilibrium adjustment and the Court's commitment to revisiting Fourth Amendment doctrines as new technologies render old laws ineffective. In my next chapter, I will examine the merits of these scholar's interpretation of the *Carpenter* test and its doctrinal shifts, as the post-*Carpenter* legal landscape has developed over the past several years. This chapter

[180] Ohm, "The Many Revolutions of Carpenter," 404.

will closely examine Fourth Amendment scholar Matthew Tokson's empirical analysis of *Carpenter*'s effect on Fourth Amendment law in lower courts, as well as address his predictions after *Carpenter*.

One final consideration of the *Carpenter* decision is the Court's possible endorsement of the mosaic theory approach to the Fourth Amendment, which asserts that some data in aggregate poses greater privacy harms than individual pieces of information, justifying a reasonable expectation of privacy to a certain amount of data. Throughout the majority opinion, Chief Justice Roberts emphasizes the "long-term" nature of the CSLI collected in *Carpenter*. The justices who joined the majority demonstrate great concern for the extensive collection of location information, and, consequently, what this data in aggregate has the potential to reveal about a person. But, as scholars point out, one of the most confusing aspects of the *Carpenter* decision was the Court's decision to hold seven days of CSLI a search, but potentially not less than this amount.[181] Though not defended explicitly in the opinion, the third footnote of the *Carpenter* opinion specifies that a search of CSLI data occurs when more than seven days of the information is obtained by the government without a warrant.[182] The Chief Justice writes: "it is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[183] As Kerr notes, "*Carpenter* thus leaves a big question unanswered: If the massive scale of digital surveillance justifies new Fourth Amendment regulation, is it only digital surveillance on a massive scale that counts?"[184] In their interpretations of the opinion, Kerr and Ohm explore this consequential legal issue, conceding that the Court might have adopted the mosaic theory approach in *Carpenter*.

[181] Ohm, "The Many Revolutions of Carpenter," 374.
[182] Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3.
[183] Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3.
[184] Kerr, "Implementing Carpenter," 37.

Both Kerr and Ohm suggest that the opinion in *Carpenter* leaves open the possibility that the Court applied the mosaic theory approach to the Fourth Amendment, as the Court held the long-term collection of CSLI was a search. As Kerr argues, the mosaic theory is rooted in equilibrium adjustment.[185] This theory attempts to remedy the reality that short-term and long-term surveillance pose different privacy risks. But, while Kerr argues the theory is "well-meaning,"[186] he asserts it must be rejected as a Fourth Amendment approach.

The largest problem for the mosaic theory, Kerr asserts, is that it requires incredibly arbitrary line drawing.[187] Not only will courts have to grapple with "how long is long enough," or how much information is required to constitute a search, but Kerr also notes that by the time specific rules are set for different forms of technology, it is likely that "technological change would have made the rules obsolete."[188] Given the sheer number of questions that the mosaic theory raises, in trying to distinguish how much surveillance, or data, amounts to a Fourth Amendment search, Kerr argues this theory should be rejected. Additionally, Kerr suggests that the mosaic theory approach forces the courts into a tedious case-by-case analysis, wherein judges "act more like legislators and number-crunchers than judges."[189]

Ohm argues, more decisively than Kerr, that the language in the *Carpenter* opinion actually "in effect endorses the mosaic theory of privacy."[190] In his discussion of the Court's second *Carpenter* test factor – "depth, breadth, and comprehensive reach,"[191] Ohm suggests that the Court indicated the quantity of CSLI was one of the most important factors that led the Court to conclude a search took place in *Carpenter*. Ohm further argues that based on the Court's

[185] Kerr, "Implementing Carpenter," 35.
[186] Kerr, "Implementing Carpenter," 37.
[187] Kerr, "Implementing Carpenter," 37.
[188] Kerr, "Implementing Carpenter," 37.
[189] Kerr, "Implementing Carpenter," 38.
[190] Ohm, "The Many Revolutions of Carpenter," 373.
[191] Carpenter v. United States, 138 S. Ct 2206, 2223 (2018).

emphasis of these factors, it implies that a single datum of CSLI would not trigger a search, and only a collection of CSLI does.[192] Hence, an application of the mosaic theory.

Still, like Kerr, Ohm argues that the mosaic theory is itself problematic. He notes that the Court declined to root its seven-day distinction in *Carpenter* in any real reasoning,[193] revealing the imprecision of mosaic theory line drawing. Looking forward, Ohm asserts that weighing the quantitative facts of different types of data to distinguish when a search has occurred is "sure to be the source of confusion in the lower court – and inside police stations."[194]

Kerr and Ohm agree that the mosaic theory approach to the Fourth Amendment may have been employed by the Court in *Carpenter*, but suggest this approach is ill equipped to answer the many questions that arise when courts weigh the privacy interests against police surveillance. In my next chapter, I will address how the mosaic theory has fared in lower courts post-*Carpenter*.

In this chapter I have discussed the most important arguments leading up to and coming out of the Supreme Court's most recent digital Fourth Amendment case, *Carpenter v. United States*. I have examined how the Court's understanding of a reasonable expectation of privacy has evolved in the face of more pervasive and invasive technology and how the long-standing third-party doctrine has diminished in the digital age. Additionally, I explored the work of Fourth Amendment scholars Kerr and Ohm in order to understand the *Carpenter* test that emerged and the legal arguments upon which the majority decided the case. Crucially, I highlight Orin Kerr's assertion that *Carpenter* is yet another example of equilibrium adjustment, and that in doing so the Court carved out new Fourth Amendment rules for the technologies of the digital age. I have also discussed Ohm's analysis of the Court's tech exceptionalism, which has enabled the Court

[192] Ohm, "The Many Revolutions of Carpenter," 374.
[193] Ohm, "The Many Revolutions of Carpenter," 374.
[194] Ohm, "The Many Revolutions of Carpenter," 375.

to take a more active role in safeguarding privacy interests in the face of rapidly developing technologies. Finally, I illuminate one of the key legal issues that remained unclear after *Carpenter* – the mosaic theory – and discuss how scholars respond to this lingering legal question. In my next chapter, I will examine the patterns of post-*Carpenter* lower court decisions and analyze specific opinions. Doing so will allow me to assess how the Supreme Court's guidance, as well as the predictions of Fourth Amendment scholars, have fared in the several years since the Court's decision.

Chapter 3

Carpenter in the Lower Courts

The two previous chapters of this thesis have explored how, over the course of nearly a century, the Supreme Court has developed and reshaped Fourth Amendment doctrine as rigid rules fail to cover new privacy threats in the digital age. I have also discussed several prominent Fourth Amendment scholars' interpretations of the Supreme Court's most recent digital privacy case, *Carpenter v. United States*, highlighting areas of consensus and contention. Ultimately, scholars agree that the Court demonstrated an appreciation for the unique privacy harms posed by modern technologies and surveillance methods, whether the Court's legal reasoning signaled a break from precedent or not. Here, I will explore *Carpenter*'s legacy in the lower courts, highlighting how these courts have clarified the *Carpenter* doctrinal shift and how they have grappled with the ambiguity of the mosaic theory in the post-*Carpenter* landscape.

As I discussed in my previous chapter, Fourth Amendment scholars debate both the legal rationale of the *Carpenter* decision and the test established by the majority opinion. Kerr suggests that the *Carpenter* rationale signals a shift away from the traditional Fourth Amendment *Katz* test, but that this test only extends to types of surveillance techniques and tools which are unique to the digital age.[195] Additionally, Kerr suggests *Carpenter* only covers information from digital-age technologies that is particularly revealing and involuntarily disclosed.[196] Ohm argues that the *Katz* test was replaced by the Court's new *Carpenter* test, which can be derived from the factors described in Chief Justice Roberts' concluding remarks in the majority opinion.[197] Ohm

[195] Kerr, "Implementing Carpenter," 16.
[196] Kerr, "Implementing Carpenter."
[197] Ohm, "The Many Revolutions of Carpenter," 361.

also suggests that several rules of technological equivalence may see more support than the Chief Justice's multiple-factor test in the future.[198] Matthew Tokson's interpretation diverges from those of Kerr and Ohm, as he argues *Carpenter* was consistent with a line of Fourth Amendment cases. He suggests that the Court has consistently placed greater weight on protecting against privacy harms than adhering to other doctrinal demands.[199] Additionally, Tokson suggests *Carpenter* did not set out a clear test, but instead vaguely discussed several factors which led the Court to find that the long-term collection of CSLI was a search.[200]

Now, scholars no longer need to speculate about how *Carpenter* has affected Fourth Amendment law. In the past four years, lower courts have begun to answer the open-ended questions of *Carpenter*, thereby developing and solidifying the doctrinal shifts of the Court's most recent digital privacy case. Some scholars have noted that the phenomenon exhibited here is common following transformative decisions in the Supreme Court.[201] For example, Evan Caminker and Richard Re both emphasize that Supreme Court precedents often require lower courts to further interpret and shape the law.[202] Furthermore, when the Court's decision is ambiguous, lower court development of the law becomes even more crucial, as it can foster a "precedential dialogue" between the Supreme Court and lower courts.[203] Tokson explains that

[198] Ohm, "The Many Revolutions Carpenter," 360.
[199] Matthew Tokson, "42nd Annual Foulston-Siefkin Lecture: The Next Wave of Fourth Amendment Challenges After Carpenter," *Washburn Law Journal* 59 (January 16, 2020): 1–24, 8, https://papers.ssrn.com/abstract=3520366.
[200] Tokson, "The Next Wave of Fourth Amendment Challenges After Carpenter," 5-6.
[201] Matthew Tokson, "The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021," *Harvard Law Review* 135 (May 10, 2022): 1790–1852, 1806.
[202] Evan H. Caminker, "Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?," *Supreme Court Review* 2018, (2019): 411–81, 452, https://doi.org/10.1086/702164.; Richard M. Re, "Narrowing Supreme Court Precedent from Below," *Georgetown Law Journal* 104 (December 8, 2015): 921–71, 947. https://papers.ssrn.com/abstract=2699607.
[203] Re, "Narrowing Supreme Court Precedent from Below," 927.

the Court may look to lower court interpretations and extensions of new precedent to better inform its rulings in the future and make clear the legal change that results from its decisions.[204]

Tokson refers to *Carpenter* as the "quintessential" landmark Supreme Court case that has required further interpretation in the lower courts.[205] Through lower courts' interpretations of *Carpenter*, Tokson suggests we can gauge how *Carpenter* will be understood and applied in future cases.[206] Furthermore, Tokson highlights that the workability of *Carpenter* in the lower courts legitimizes the decision and "may also bolster arguments for preserving and extending it."[207] While the Supreme Court has stated that it may be appropriate to revisit prior decisions if they become unworkable in the lower courts, the widespread adoption of *Carpenter* suggests lower courts have handled the ambiguity of the decision coherently.[208] Additionally, Tokson notes that the number of cases interpreting *Carpenter* narrowly has decreased over time, as familiarity with the decision has increased,[209] substantiating further the claim that *Carpenter*'s ambiguity has allowed for productive lower court development of this legal shift. In my next section, I will illuminate some of Tokson's key findings from his analysis of the direct impact of *Carpenter* in lower court Fourth Amendment cases. In the ensuing analysis, I will specifically discuss Tokson's research regarding the role of the *Carpenter* factors in determining lower court case outcomes and highlight Tokson's conclusions about the *Carpenter* test that have emerged during the past few years.

[204] Tokson, "The Aftermath of Carpenter," 1806.
[205] Tokson, "The Aftermath of Carpenter," 1806.
[206] Tokson, "The Aftermath of Carpenter," 1806.
[207] Tokson, "The Aftermath of Carpenter," 1795.
[208] Tokson, "The Aftermath of Carpenter," 1795.
[209] Tokson, "The Aftermath of Carpenter," 1795.

Tokson: An Empirical Study of Fourth Amendment Law

Tokson has conducted the most comprehensive study of the impact of *Carpenter v. United States* to date, analyzing the 857 federal and state court rulings to cite *Carpenter* from its publication in June of 2018 through March of 2021.[210] Tokson finds that lower courts have largely complied with *Carpenter*, and argues that the large number of decisions that cite *Carpenter* reflects the "enormous impact" of the case in Fourth Amendment law.[211] In his research, Tokson determined that of the 857 cases to cite *Carpenter* in his data set, 399 of those cases applied *Carpenter* substantively to assess whether a search had taken place.[212] The remainder of these cases only cited the decision in more general discussions of Fourth Amendment law.[213] Still, Tokson suggests the impact of the decision is significant and growing. For example, across the data set of determinative yes-or-no rulings, Tokson finds that the proportion of cases which applied a strong pre-*Carpenter* third-party doctrine decreased by five percentage points between 2018 and the end of 2020.[214] This indicates that, as lower courts have grown more familiar with *Carpenter*'s "reformation of the third-party doctrine," they are increasingly complying with its guidance.[215]

Tokson also demonstrates, persuasively, that the impact of *Carpenter* can be examined through lower court's applications of *Carpenter* factors in determining case outcomes. There are several influential *Carpenter* factors which Tokson, and other scholars glean from the language of Chief Justice Roberts' opinion. The first is the revealing nature of the data or information,

[210] Tokson, "The Aftermath of Carpenter," 1791.
[211] Tokson, "The Aftermath of Carpenter," 1808.
[212] Tokson, "The Aftermath of Carpenter," 1808.
[213] Tokson, "The Aftermath of Carpenter," 1808.
[214] Tokson, "The Aftermath of Carpenter," 1839.
[215] Tokson, "The Aftermath of Carpenter," 1839.

which can be gauged by the information's "tendency to disclose sensitive or intimate details." Through this factor, courts examine whether the government was able to learn private information that is deeply revealing about the subject of a search, including their habits, social practices, and associations.[216] The second factor is the amount of information gathered, which indicates that extensive collection of personal data is significant and can give rise to a Fourth Amendment violation.[217] Tokson identifies a third possible *Carpenter* factor, which Ohm finds critical to the Court's rationale in *Carpenter*, the factor of the number of people affected by a surveillance tool or technology.[218] Because the Court referenced "the comprehensive reach" of a type of surveillance, scholars have concluded that the number of people affected by a surveillance practice may be influential in future Fourth Amendment decisions.[219] Tokson highlights the fourth and fifth potential *Carpenter* factors, inescapability and automatic disclosure of information.[220] He argues that these concepts are related,[221] and concedes that the Court indicated inescapability of the technology and automatic, involuntary disclosure of information might be requirements for protection under *Carpenter*.[222] Lastly, Tokson mentions a sixth factor, the cost of a surveillance tool or technique.[223] Tokson notes that the *Carpenter* Court recognized the cheap and efficient nature of gathering CSLI, and thus lower courts may differentiate Fourth Amendment searches from non-searches based on the cost of the surveillance technique or technology.[224] While Tokson argues that *Carpenter* "gave no concrete

[216] Tokson, "The Aftermath of Carpenter," 1801.
[217] Tokson, "The Aftermath of Carpenter," 1801-2.
[218] Ohm, "The Many Revolutions of Carpenter," 373.
[219] Tokson, "The Aftermath of Carpenter," 1802.
[220] Tokson, "The Aftermath of Carpenter," 1803.
[221] Tokson, "The Aftermath of Carpenter," 1825.
[222] Tokson, "The Aftermath of Carpenter," 1803.
[223] Tokson, "The Aftermath of Carpenter," 1804.
[224] Tokson, "The Aftermath of Carpenter," 1804.

test to guide future decisions,"[225] he does note that these factors clearly shaped the *Carpenter* decision and have influenced lower court decisions in the post-*Carpenter* era.

Tokson devotes a significant amount of attention to analyzing the impact of each *Carpenter* factor in lower court rulings. According to his analysis, of the 399 cases that substantively applied *Carpenter*, 217 resolved a Fourth Amendment issue in a determinative yes-or-no ruling.[226] Among these cases, 129 decisions mentioned at least one of the *Carpenter* factors in assessing a Fourth Amendment claim, and 112 of those cases stated at least one of the *Carpenter* factors clearly favored a certain party.[227] Based on his evaluation of the prevalence and influence of each *Carpenter* factor, Tokson concludes that the most frequently discussed factors are the revealing nature of the information in question, the amount of data collected, and the automatic nature of the disclosure of the particular data.[228]

Tokson determined that lower courts cited the *Carpenter* factor of the revealing nature of the information, or its ability to reveal intimate and private details of an individual, in a total of 93 decisions.[229] In 69 of the 70 lower court rulings that discussed the revealing nature of the information, and came to a determinative ruling, the court's analysis of the information's capacity to reveal intimate information was dispositive in the case.[230] In other words, the court's analysis of this factor was influential in the court's determination at a rate of 98.6%.[231] Tokson highlights that lower courts "almost never failed to find a search after determining that surveilled data was revealing, and never found a search after determining that surveilled data was

[225] Tokson, "The Aftermath of Carpenter," 1805.
[226] Tokson, "The Aftermath of Carpenter," 1821.
[227] Tokson, "The Aftermath of Carpenter," 1821
[228] Tokson, "The Aftermath of Carpenter," 1822.
[229] Tokson, "The Aftermath of Carpenter," 1823.
[230] Tokson, "The Aftermath of Carpenter," 1823.
[231] Tokson, "The Aftermath of Carpenter," 1823.

unrevealing."[232] Tokson's analysis of the cases demonstrates that, when the revealing nature of the data at issue is discussed, it is the most influential *Carpenter* factor in resolving a Fourth Amendment claim.

The prevalence and influence of this factor aligns with the predictions of Kerr, Ohm, and Tokson. Across each of their differing interpretations, these scholars highlight that the revealing nature of the information was significant in *Carpenter*, and, thus, that it would prevail as a highly significant consideration in future decisions.[233] Furthermore, Tokson argues that the intimacy of the information sought in Fourth Amendment cases has been a crucial concern since *Katz v. United States*.[234] So, *Carpenter*'s emphasis of this factor, and its subsequent influence in lower courts, demonstrates consistency with prior Fourth Amendment jurisprudence.

The *Carpenter* factor related to the amount of data collected was also both prevalent and influential when applied to lower court cases.[235] This factor was mentioned in 116 cases, and 71 of the 77 cases to reach a determinative decision did so because of the amount factor, whether it ruled in favor of a search or not.[236] Tokson also notes the significant influence of this factor, as it indicated the decision at a rate of 92.2%.[237] The prevalence and influence of this factor in lower court cases is likely unsurprising to Kerr, Ohm, and Tokson, who all note the significance of the Court's discussion of the amount of CSLI gathered in *Carpenter*. Lower courts' adoption of this *Carpenter* factor does, however, go against the advice of Kerr and Ohm who are particularly wary of an adoption of the mosaic theory.[238] In fact, Kerr suggests that the *Carpenter* framework

[232] Tokson, "The Aftermath of Carpenter," 1823.
[233] Kerr, "Implementing Carpenter"; Ohm, "The Many Revolutions of Carpenter"; Tokson, "The Next Wave of Fourth Amendment Challenges."
[234] Matthew Tokson, "The Emerging Principles of Fourth Amendment Privacy," *George Washington Law Review* 88 (July 23, 2019): 1–75,16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3425321.
[235] Tokson, "The Aftermath of Carpenter," 1823.
[236] Tokson, "The Aftermath of Carpenter," 1823.
[237] Tokson, "The Aftermath of Carpenter," 1823.
[238] Kerr, "Implementing Carpenter," 35-39; Ohm, "The Many Revolutions of *Carpenter*," 375-376.

should not include an evaluation of the amount of information collected, as it leads to arbitrary line drawing and inconsistent results.[239] I will discuss the relationship between lower courts' consideration of the amount of information in a case and the mosaic theory later in this chapter.

According to Tokson, the automatic nature of the data disclosure was mentioned less frequently than the revealing nature or amount of data collected, but was similarly influential when discussed.[240] This *Carpenter* factor was mentioned in 61 cases, 46 of which delivered a determinative ruling.[241] Of the 46 cases, 44 of them indicated that the automatic factor determined the decision.[242] This factor indicated the decision at a significantly high rate of 95.7%.[243] This finding favors each of the scholars' interpretations of the importance of automaticity when courts determine the voluntary disclosure of information to a third-party. Across their varying interpretations of *Carpenter*, Kerr, Ohm, and Tokson all predicted that the automatic disclosure of information would tip the scale in favor of finding a search. Interestingly, Tokson notes that this factor was the most likely of the three *Carpenter* factors that were most commonly cited to disfavor finding a search.[244] In 38 of the determinative rulings, lower courts found automatic nature disfavored a search, while only 8 decisions held automaticity favored one.[245] For clarity, though, Tokson explains that when courts assessed the automatic nature in these cases, they often concluded that disclosure was not automatic and, thus, the Fourth Amendment could not protect the data.[246]

[239] Kerr, "Implementing Carpenter," 38.
[240] Tokson, "The Aftermath of Carpenter," 1823.
[241] Tokson, "The Aftermath of Carpenter," 1823.
[242] Tokson, "The Aftermath of Carpenter," 1823.
[243] Tokson, "The Aftermath of Carpenter," 1823.
[244] Tokson, "The Aftermath of Carpenter," 1823.
[245] Tokson, "The Aftermath of Carpenter," 1823.
[246] Tokson, "The Aftermath of Carpenter," 1823.

Tokson also examined the *Carpenter* factors of the inescapable nature of the technology or surveillance, the cost, and the number of people surveilled, finding each of these factors far less prevalent in lower court rulings. Lower courts explicitly mentioned the inescapable nature of the technology or surveillance in 36 cases, 16 of which came to a determinative ruling.[247] Tokson notes that while this *Carpenter* factor was less frequently discussed in lower court rulings, it was quite influential for case outcomes.[248] In 15 of the 16 cases to cite the inescapability factor, and reach a determinative yes-or-no ruling, the decision was indicated by the court's inescapability factor analysis.[249] Tokson highlights that this *Carpenter* factor was most likely to favor the government as it led to the finding of a search in only two cases.[250] In the case of *United States v. Trader*, for example, the 11th Circuit held that the acquisition of a person's email and IP addresses from a third party – the phone app Kik – was constitutional even under the *Carpenter* analysis.[251] The court reasoned that the email addresses and IP addresses at issue did not fall under the purview of *Carpenter*, as Trader voluntarily and affirmatively conveyed these pieces of information to the messaging application from which the government sought information. The court emphasizes that the defendant had taken no steps to avoid the disclosure of his information, and, therefore the third-party doctrine governed the case.[252] This finding confirms Kerr's interpretation that *Carpenter* only extends to information which is expressly, involuntarily and automatically conveyed to a third-party.[253] Tokson reports that this factor was "to be the most

[247] Tokson, "The Aftermath of Carpenter," 1823-24.
[248] Tokson, "The Aftermath of Carpenter," 1823-24.
[249] Tokson, "The Aftermath of Carpenter," 1824.
[250] Tokson, "The Aftermath of Carpenter," 1823.
[251] United States v. Trader, 981 F.3d 961 (11th Cir. 2020).
[252] Id. at 967.
[253] Kerr, "Implementing Carpenter," 20.

likely to favor the government when addressed by courts," much as Kerr anticipated and recommended.[254]

The *Carpenter* factor of the cost of the surveillance was similarly less prevalent, but still influential when discussed. Tokson notes this factor was mentioned in 34 lower court cases, with 15 of those cases delivering determinative rulings.[255] The *Carpenter* cost factor analysis indicated how the court would decide a case at a rate of 86.7%, with 13 of the 15 determinative holdings demonstrating that this factor analysis informed the court's decision.[256] In the Washington Supreme Court case *State v. Muhammad*, for example, seven members of the court held that the pinging of a cell phone to generate real-time CSLI violated the Fourth Amendment in light of the *Carpenter* decision.[257] The court specifically referenced Chief Justice Roberts' assertion that CSLI, compared to more traditional surveillance tools, is more inexpensive and efficient.[258] Furthermore, the court emphasized technology's ability to change the relationship between the police and citizens when the surveillance is of such a low cost.[259] Though Kerr does not consider this factor in his analysis, and Ohm does so only briefly, Tokson highlights the privacy harms posed by low-cost surveillance.[260] He argues that privacy harms greatly increase as the cost of surveillance tools decrease, because "cheap and easy" police practices erode the practical limits that historically confine police powers.[261] The influence of this factor, when it was mentioned, in lower court cases reflects Tokson's assertion that the cost of surveillance is important to consider when assessing the harm posed by a technology or surveillance tool.

[254] Tokson, "The Aftermath of Carpenter," 1824.
[255] Tokson, "The Aftermath of Carpenter," 1824.
[256] Tokson, "The Aftermath of Carpenter," 1824.
[257] State v. Muhammad, 451 P.3d 1060 (Wash. 2019).
[258] Id. at 1071-72.
[259] Id. at 1072.
[260] Tokson, "The Next Wave of Fourth Amendment Challenges."
[261] Tokson, "The Next Wave of Fourth Amendment Challenges," 7.

Though Tokson demonstrates that the less frequently cited *Carpenter* factors of inescapability and cost were still influential when they appeared in court decisions, he determines that the *Carpenter* factor of the number of people affected by a surveillance method has had little influence in resolving Fourth Amendment issues.[262] Tokson notes, the "number factor" was only mentioned in 15 cases, 6 of which delivered a determinative ruling.[263] Furthermore, in half of these determinative rulings, the courts plainly rejected the number of people affected by the technology or surveillance as a factor for determining a search.[264] Tokson concludes that the explicit rejection of the *Carpenter* factor of the number of people affected by a technology or surveillance in lower court cases likely indicates the irrelevance of this factor in post-*Carpenter* law.

While a few of the *Carpenter* factors, including the revealing nature of the information, the amount of data collected, and the automatic nature of disclosure influenced a significant number of lower court cases following the Supreme Court's ruling, Tokson's research affirms his assertion that the *Carpenter* opinion did not establish a clear test. Tokson finds that lower courts have rarely discussed all or even most of the *Carpenter* factors together, and largely ignored the *Carpenter* factors that did not influence the outcome of the case.[265] Tokson argues, "this reflects the absence of a clear doctrinal command regarding the specific standard that courts should apply," and "gives courts license to consider all, some, or none of the factors as they see fit."[266] Nevertheless, Tokson notes that overtime this flexibility and ambiguity have allowed lower courts to define a "relatively clear," emerging *Carpenter* test for Fourth Amendment searches.[267]

[262] Tokson, "The Aftermath of Carpenter," 1824.
[263] Tokson, "The Aftermath of Carpenter," 1824.
[264] Tokson, "The Aftermath of Carpenter," 1824.
[265] Tokson, "The Aftermath of Carpenter," 1822.
[266] Tokson, "The Aftermath of Carpenter," 1822.
[267] Tokson, "The Aftermath of Carpenter," 1831.

Based on their prevalence and influence, Tokson asserts that the emerging *Carpenter* test consists of at least three factors: "the revealing nature of the data captured, the amount of data captured, and whether the data was disclosed to a third party automatically."[268] Additionally, Tokson finds that these three factors are themselves strongly correlated – especially between revealing nature and amount – and with case outcomes in lower courts. [269] The impact of these factors in lower court decisions, as well as their correlation in determining outcomes indicates further that these factors make up the prevailing *Carpenter* framework. Tokson emphasizes the impact of these combined factors in post-*Carpenter* Fourth Amendment cases: "In cases where the government obtains a substantial amount of revealing data that was collected automatically from a user, courts will very likely find a search."[270] Conversely, when the government obtains a small amount of non-revealing data from a third-party that a user voluntarily discloses information to, Tokson concludes, no search will be found.

Though Tokson, and other scholars, anticipated the inescapability of a technology or surveillance as well as its cost to be influential in lower court cases post-*Carpenter*, Tokson finds that courts have yet to incorporate these factors into a consistently applied test.[271] As for the factor of the number of people affected by a technology, Tokson concludes this factor largely does not matter for case outcomes.[272] Ultimately, Tokson notes that, while the lower courts have largely indicated the *Carpenter* test consists of an analysis of the nature, amount, and voluntary disclosure of the information, the persistent inconsistency of lower court decisions leaves open the possibility for other factors, such as cost, to be incorporated, or for courts to combine factors

[268] Tokson, "The Aftermath of Carpenter," 1831.
[269] Tokson, "The Aftermath of Carpenter," 1825.
[270] Tokson, "The Aftermath of Carpenter," 1831.
[271] Tokson, "The Aftermath of Carpenter," 1831.
[272] Tokson, "The Aftermath of Carpenter," 1832.

in the future.[273] Lower courts thus far have clarified the jurisprudential changes of *Carpenter v. United States* by beginning to formulate the new multi-factor *Carpenter* test, but a consistently applicable *Carpenter* framework remains undeveloped.[274] As I will explain in a later section, part of this inconsistency rests in the *Carpenter* amount factor, which will require clarification for consistent applicability of the *Carpenter* framework in Fourth Amendment cases.

In addition to exploring the development of the *Carpenter* factor analysis in lower courts, Tokson's study also examines two key arguments made by prominent scholars, Kerr and Ohm. He first looks at Orin Kerr's suggestion that *Carpenter* established a factor which Tokson calls the "the digital-age technology factor."[275] In his analysis of the *Carpenter* opinion, Orin Kerr suggests that the *Carpenter* framework is limited to modes of surveillance and technologies novel in the digital age.[276] In other words, Kerr posits that *Carpenter* does not apply to traditional types of surveillance or their digital equivalents. Kerr emphasizes that the Court found CSLI to be "an entirely different species" of data, leaving existing precedent unbothered.[277] He also stresses that the majority claimed *Carpenter* did not "call into question conventional surveillance techniques and tools."[278]

In his study, Tokson weighs Kerr's claim against lower court rulings. He concludes that Kerr's assertion is overstated: "There is little evidence in the dataset that courts consider digital age technology a requirement for Fourth Amendment protection under *Carpenter*."[279] In fact, Tokson found that only one case in the entire dataset presented digital nature as a factor worth

[273] Tokson, "The Aftermath of Carpenter," 1832-33.
[274] Tokson, "The Aftermath of Carpenter," 1834.
[275] Tokson, "The Aftermath of Carpenter," 1828.
[276] Kerr, "Implementing Carpenter," 16-17.
[277] Kerr, "Implementing Carpenter," 16.
[278] Kerr, "Implementing Carpenter," 16.
[279] Tokson, "The Aftermath of Carpenter," 1829.

considering.[280] Furthermore, Tokson notes that several post-*Carpenter* cases extended Fourth Amendment protection to data derived from pre-digital age surveillance tools and their equivalents,[281] precisely what Kerr argued would not happen. In the case of *People v. Tafoya*, for example, the Colorado Court of Appeals found that the government's use of a pole camera to monitor the property around a suspect's home for three-months was an unconstitutional search.[282] In September of 2021, the Colorado Supreme Court affirmed the judgment of the court of appeals.[283] In its decision, the Supreme Court of Colorado explicitly references *Carpenter*'s precedent as a guide: "Together, *Jones* and *Carpenter* suggest that when government conduct involves continuous, long-term surveillance, it implicated a reasonable expectation of privacy. Put simply, the duration, continuity, and nature of surveillance matter when considering all the facts and circumstances in a particular case."[284] Tokson notes that this case disproves Kerr's suggestion that the *Carpenter* framework does not apply to pre-digital age surveillance tools and technologies. Additionally, in 2020, the Ohio Court of Appeals extended Fourth Amendment protection to blood and urine samples taken for emergency medical purposes.[285] In its analysis, this court explicitly relied on *Carpenter*, stating the Supreme Court's precedent established a test for assessing the intimate nature of the information sought and the extent of voluntary disclosure.[286] Here, the court applied an interpretation of the *Carpenter* framework to a traditional practice, without any consideration for Kerr's digital-age technology factor.

While Tokson concludes that Kerr's digital-age technology factor has not been adopted as one of the *Carpenter* test factors in lower court analyses, he does find support for a more

[280] Tokson, "The Aftermath of Carpenter," 1829.
[281] Tokson, "The Aftermath of Carpenter," 1829.
[282] People v. Tafoya, 490 P.3d 532 (Colo. App. 2019).
[283] People v. Tafoya, 494 P.3d 613 (Colo. 2021).
[284] Id. at 620.
[285] State v. Eads, 154 N.E.3d 538 (Ohio Ct. App. 2020).
[286] Id. at 14.

nuanced and "subtle relationship" between the digital-age factor and lower court case outcomes.[287] Tokson notes that, of the 217 determinative lower court rulings in the data set, 159 involved digital-age information, such as CSLI and IP addresses.[288] The other 58 cases that reached a determinative ruling addressed pre-digital age information or its equivalents.[289] Of the cases that addressed digital-age data, courts found a search in 57 cases.[290] On the other hand, among the cases involving pre-digital age data, courts found a search in only 9.[291] Tokson's analysis reveals that cases involving data of the digital age found a search at a rate of 35.8%, while cases involving pre-digital age data, found a search at a rate of 15.5%.[292] Therefore, courts are more likely to find a search in cases involving technologies and tools of the digital age rather than traditional types of data and surveillance techniques.[293] Even though lower courts do not explicitly refer to the modern nature of the data or surveillance technique, this factor does seem to correlate significantly with rulings of a search. Tokson concludes: "Lower courts have not adopted an interpretation of *Carpenter* that would limit its protection exclusively to digital data. But digital data is more likely to be protected than non-digital data in cases applying *Carpenter*."[294] So, while Kerr interprets *Carpenter*'s scope to be narrow, limited to technologies and surveillance tools novel in the digital age, post-*Carpenter* litigation demonstrates the *Carpenter* framework is broader than Kerr expected. The *Carpenter* test has changed Fourth Amendment rules for new technologies, and, in many cases, old ones too.

[287] Tokson, "The Aftermath of Carpenter," 1829.
[288] Tokson, "The Aftermath of Carpenter," 1829.
[289] Tokson, "The Aftermath of Carpenter," 1829.
[290] Tokson, "The Aftermath of Carpenter," 1829.
[291] Tokson, "The Aftermath of Carpenter," 1829.
[292] Tokson, "The Aftermath of Carpenter," 1829.
[293] Tokson, "The Aftermath of Carpenter," 1829.
[294] Tokson, "The Aftermath of Carpenter," 1830.

Tokson also discusses the merit of Kerr and Ohm's argument that the Court in *Carpenter* reshaped the *Katz* reasonable expectation of privacy test. While Ohm argues this point more forcefully than Kerr does, both scholars suggest that the emerging *Carpenter* test changed Fourth Amendment jurisprudence by eroding the prior *Katz* framework. Kerr argues that the traditional *Katz* test was reshaped from an analysis of the places and things in which people are entitled to a reasonable expectation of privacy, to an analysis of how much the government can learn about us by obtaining our information, regardless of the source.[295] Ohm suggests that *Carpenter* reinvented the *Katz* test with its multi-factor test and potential rules of technological equivalence.[296] Rather than gauge societal expectations of privacy, Ohm suggests that the Court in *Carpenter* adopted a normative role,[297] as it assessed the privacy risks posed by not only the state of CSLI in the present but also that of the future.[298]

Through Tokson's analysis of lower court decisions, he finds Kerr and Ohm's assertions that the *Katz* test was reshaped or replaced in *Carpenter* are largely unsubstantiated. First, Tokson notes that 88 determinative lower court rulings did not mention the *Carpenter* factors.[299] While Tokson explains that many of these cases refrained from discussing *Carpenter* factors because the data in question was either analogous to the CSLI in *Carpenter*, or involved a Fourth Amendment issue affirmed in *Carpenter*, several of these cases were simply resolved under the Court's long-standing *Katz* framework.[300] Moreover, even in the cases which did analyze Fourth Amendment claims using the *Carpenter* factors, most courts referred to the *Katz* test and discussed the subject's reasonable expectation of privacy.[301] For example, in two cases discussed

[295] Kerr, "Implementing Carpenter," 6.
[296] Ohm, "The Many Revolutions of Carpenter," 386.
[297] Ohm, "The Many Revolutions of Carpenter," 398.
[298] Ohm, "The Many Revolutions of Carpenter," 408.
[299] Tokson, "The Aftermath of Carpenter," 1827.
[300] Tokson, "The Aftermath of Carpenter," 1827.
[301] Tokson, "The Aftermath of Carpenter," 1827-28.

above, *People v, Tafoya* and *State v. Eads*, these courts applied *Carpenter* factor analyses, yet also extensively referenced the *Katz* reasonable expectation of privacy approach. Tokson concludes: "there is no indication that *Carpenter* has misplaced or usurped *Katz* as the primary framework of Fourth Amendment search law, as some commentators predicted. Rather, *Carpenter* has augmented or modified the *Katz* inquiry while leaving its general framework in place."[302]

Nevertheless, Tokson's study demonstrates that *Carpenter*'s impact on lower court Fourth Amendment cases has been immense. Not only have courts increasingly adhered to *Carpenter*'s narrowing of the third-party doctrine, but they have widely accepted parts of the *Carpenter* factor framework introduced by the Supreme Court in 2018. Lower courts have begun to develop an emerging *Carpenter* test, which consists of the revealing nature of the information, the amount, and the voluntary nature of disclosure, while keeping intact the *Katz* reasonable expectation of privacy test. Looking forward, though, Tokson asserts that further clarity of this test is needed.[303] He reiterates that many lower courts consider a select number of *Carpenter* factors, relevant to the decision, while ignoring the other factors from the Court's decision.[304] "The time has come for courts to abandon this practice," Tokson writes.[305] Instead, he argues courts should develop a consistent set of factors, even if these factor tests vary across jurisdictions.[306] Tokson concludes that this clarification would allow for more coherent Fourth Amendment jurisprudence in the wake of *Carpenter*, and significantly more predictability. In my next section I will explore a key route by which lower courts and, eventually the Supreme Court,

[302] Tokson, "The Aftermath of Carpenter," 1828.
[303] Tokson, "The Aftermath of Carpenter," 1848.
[304] Tokson, "The Aftermath of Carpenter," 1848.
[305] Tokson, "The Aftermath of Carpenter," 1848.
[306] Tokson, "The Aftermath of Carpenter," 1848.

can and should solidify the *Carpenter* amount factor in Fourth Amendment doctrine to build on the progress of lower courts in developing the law after *Carpenter*.

The Mosaic Theory post-*Carpenter*

As I have discussed throughout this thesis, the mosaic theory has lingered in Fourth Amendment jurisprudence since before its endorsement by five Supreme Court justices in *United States v. Jones*.[307] The mosaic theory approach to the Fourth Amendment states that a collection of information obtained by the government may implicate privacy concerns greater than those of each individual piece of information. In other words, individuals have a greater privacy interest in collections of their data, as opposed to isolated pieces of information. As Orin Kerr explains, "the mosaic theory is therefore premised on aggregation: it considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic."[308] Scholars have suggested that the Court in *Carpenter* possibly endorsed the mosaic theory. In considering the amount of data obtained in *Carpenter*, the Court determined that 127 days of CSLI was a search but asserted less than seven days of CSLI collection was not.[309] As one scholar argues, had the Court used the traditional sequential approach in *Carpenter*, assessing each government action in isolation, the issue of duration in *Carpenter* would have been immaterial.[310] So, while the Court did not explicitly endorse the

[307] Matthew B. Kugler and Lior Jacob Strahilevitz, "Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory," *The Supreme Court Review* 2015 (January 2016): 205–63, https://doi.org/10.1086/686204.
[308] Orin S. Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review* 111, no. 3 (2012): 311–54. https://repository.law.umich.edu/mlr/vol111/iss3/1/.
[309] Carpenter v. United States, 138 S. Ct. 2206, 2217-18 (2018).
[310] Robert Fairbanks, "Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter," *Berkeley Journal of Criminal Law 2021* (June 23, 2021): 71–119, 74, https://doi.org/10.15779/Z38DZ03287.

mosaic theory approach in *Carpenter*, it did "at least open the door" for lower courts to either accept or reject this holistic approach.[311]

Lower court rulings since *Carpenter* affirm this insight. First, the adoption of the mosaic theory by lower courts is evident in the *Carpenter* test that has emerged. As Tokson highlights, the amount of data collected in lower court cases was the most prevalent *Carpenter* factor, mentioned in 116 total decisions in the dataset.[312] Lower courts citing *Carpenter* largely adhered to the *Carpenter* principle, which built on the *Jones* concurrences, that privacy harms generally tend to increase as the amount of data collected increases.[313] In the case of *People v, Tafoya*, the Colorado Supreme Court emphasized the effect of the continuity and duration of the surveillance on Tafoya's reasonable expectation of privacy.[314] The court referenced Justice Alito's argument in *Jones* that people generally expect there to be practical limits on police power precluding constant, infallible, and long-term tracking.[315] The court found that this expectation applied to the surveillance here, too. The court reasoned that three months of "continuous" pole camera surveillance, examining the curtilage of Tafoya's home, fell outside the scope of what society expects of law enforcement.[316] Additionally, the court held that the government gathered a similarly "precise" and "comprehensive" record to those in *Jones* and *Carpenter*.[317] In another case, *Commonwealth v. Wilkerson*, involving historical CSLI, the Supreme Judicial Court of Massachusetts ruled that the government's collection of more than six hours of CSLI amounted to a search.[318] In the opinion, the court specifically addressed the constitutional concerns raised

[311] Fairbanks, 74.
[312] Tokson, "The Aftermath of Carpenter," 1823.
[313] Tokson, "The Emerging Principles of the Fourth Amendment," 19-20.
[314] People v. Tafoya, 494 P.3d 613, at 622-23 (Colo. 2021).
[315] Id. at 622.
[316] Id. at 622.
[317] Id. at 622.
[318] Commonwealth v. Wilkerson, 486 Mass. 159, 156 N.E.3d. 754 (Mass. 2020)

by the collection of "extended" CSLI,[319] and explained that the amount of data was particularly pertinent to the determination in the case. Here, too, the court displayed a clear application of the mosaic theory framework.[320]

Additionally, in lower court cases which ultimately did not find a search, several courts justified their rulings using the mosaic theory framework. In the case *People v. Edwards*, for example, the Bronx Supreme Court determined that the government's use of only two days of historical CSLI did not amount to a Fourth Amendment search.[321] In this case, the court differentiated the short-term CSLI from the extensive data in *Carpenter*, arguing that two days' worth of this location information was targeted and specific enough that it did reveal intimate details in the way long-term surveillance does. "The difference between long-term and short-term CSLI data is stark," the court reasoned, because "long-term data can be likened to filming a person's entire life for weeks, or months, or even years; short-term CSLI data is like taking a single snapshot of that person on the street."[322] Here, the court employed the mosaic theory approach to determine that *Carpenter* did not cover short-term CSLI, explaining that the privacy harms posed by only two days of data collection did not equate to the harms posed in *Carpenter*. As Tokson's comprehensive study highlights, and lower court rulings corroborate, the amount of information collected by the government has been a significant factor in many lower court decisions since *Carpenter*.[323] The mosaic theory has allowed many lower courts to further develop *Carpenter*'s factor test and remain loyal to the Supreme Court's emphasis on the need to evaluate the amount of surveillance collected.

[319] Id. at 767.
[320] Fairbanks, 76.
[321] People v. Edwards, 63 Misc. 3d 827 (N.Y. Sup. Ct. 2019)
[322] Id. at 832.
[323] Tokson, "The Aftermath of Carpenter," 1823.

Still, the mosaic theory is not binding Fourth Amendment law.[324] Since the Court did not explicitly endorse the mosaic theory in *Carpenter*, it failed to provide clear guidance for lower courts going forward. While some courts have applied the mosaic theory, other have not. For example, in the case of *People v. Simpson*, a Supreme Court in New York ignored the amount factor of CSLI collection.[325] Here, the court argued that the *Carpenter* opinion focused more on the violation of a reasonable expectation of privacy in one's physical movements learned through any CSLI, in effect working around the question of surveillance duration.[326] Other courts have gone a step further to attack the mosaic theory approach explicitly. In the controversial case of *United States v. Tuggle*, the United States Court of Appeals for the Seventh Circuit upheld the government's long-term pole camera surveillance of the outside of Tuggle's home and his surrounding property.[327] While Tuggle moved to suppress the eighteen months of pole camera surveillance, he failed to convince the court that a Fourth Amendment search occurred. Tuggle asserted that, even if the court found short-term pole camera surveillance was permissible under *Carpenter*, it should recognize that the extensive surveillance at issue in the case was more invasive than a small collection of pole camera surveillance, and thus constituted a search.[328] However, the court declined to apply the mosaic theory, arguing that the information conveyed by the pole-cameras outside of Tuggle's home did not implicate the privacy concerns of the extensive tracking in *Jones* or *Carpenter*, which tracked location information across private and public spaces, and did so retrospectively.[329] Here, the Seventh Circuit explained that the mosaic theory has an "obvious line-drawing problem."[330] Furthermore, if the court were to draw a line, it

[324] United States v. Tuggle, 4 F.4th 505, at 520 (7th Cir. 2021).
[325] Fairbanks, 97.
[326] People v. Simpson, 62 Misc. 3d 374, at 676. (N.Y. Sup. Ct. 2018).
[327] United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).
[328] United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).
[329] Id. at 524.
[330] Id. at 526.

"risks violating Supreme Court precedent and interfering with Congress's policy-making function."[331] In *United States v. Tuggle*, the Seventh Circuit went even beyond declining to apply the mosaic theory approach to the facts of the case and also rejected the mosaic theory as a viable Fourth Amendment framework. While the Supreme Court's ambiguous attitude towards the mosaic theory in *Carpenter* has led some lower courts to adopt the framework, and many to at least discuss the factor of the amount of information in their decisions,[332] it has also left room for explicit rejection and criticism by lower courts. Crucially, these varying interpretations have led to contradictory conclusions in Fourth Amendment law. While the Supreme Court of Colorado held in *People v. Tafoya* that three months of pole-camera surveillance was a search, the Seventh Circuit in *United States v. Tuggle* ruled that eighteen months of the same surveillance was not. Surely, the justices on the Supreme Court, and the framers of the Fourth Amendment for that matter, did not intend for two lower courts to arrive at opposite conclusions when applying Fourth Amendment precedent. So, the question remains, what to do with the mosaic theory.

The Future of the Mosaic Theory

Orin Kerr has long denounced the mosaic theory approach to the Fourth Amendment.[333] Most notably, Kerr criticizes the theory for requiring "arbitrary and likely endless line-drawing,"[334] as Judge Flaum echoed in his opinion in *United States v. Tuggle*.[335] Kerr suggests that the theory raises never-ending questions about how much surveillance amounts to an intimate mosaic, what types of surveillance can qualify under the theory, and whether continuous

[331] Id. at 526.
[332] Tokson, "The Aftermath of Carpenter," 1823.
[333] Kerr, "The Mosaic Theory of the Fourth Amendment."
[334] Kerr, "Implementing Carpenter," 38.
[335] United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).

long-term surveillance means that there can be no period of time during the surveillance in which the device is either dormant or not in use.[336] Furthermore, Kerr suggests that even if judges took on the burden of answering these questions, they would likely fail in their efforts.[337]

Kerr suggests that the mosaic theory is "well intentioned."[338] It is premised on equilibrium adjustment, as it attempts to regulate emerging police powers made possible by digital age technology, but Kerr asserts this theory does not bode well in the quickly evolving age of "computerization."[339]

> The challenge of answering the questions raised by the mosaic theory has particular force because the theory attempts to regulate use of changing technologies… As a result, the constantly evolving nature of surveillance practices can lead new questions to arise faster than courts might settle them. Old practices would likely be obsolete by the time the courts resolved how to address them, and the newest surveillance practices would arrive and their legality would be unknown.[340]

Instead of adopting the mosaic theory, Kerr has long endorsed the traditional "sequential" approach to the Fourth Amendment.[341] The sequential approach instructs that each police action be analyzed in isolation to determine when and if at a certain point a search occurred. For example, in *United States v. Jones*, the majority opinion employed the sequential approach to find a search occurred.[342] Under the trespass doctrine, Jones' Fourth Amendment right was violated the moment the government affixed the GPS tracking device to his vehicle.[343] Kerr argues, compared to the complexity of searches under the mosaic theory, searches under the sequential approach are "simple points."[344]

---

[336] Kerr, "The Mosaic Theory of the Fourth Amendment," 333.
[337] Kerr, "Implementing Carpenter," 38.
[338] Kerr, "The Mosaic Theory of the Fourth Amendment," 353.
[339] Kerr, "The Mosaic Theory of the Fourth Amendment," 353.
[340] Kerr, "The Mosaic Theory of the Fourth Amendment," 347.
[341] Kerr, "The Mosaic Theory of the Fourth Amendment."
[342] Kerr, "The Mosaic Theory of the Fourth Amendment," 317.
[343] Kerr, "The Mosaic Theory of the Fourth Amendment," 317.
[344] Kerr, "The Mosaic Theory of the Fourth Amendment," 329.

Though a majority of the Court in *Carpenter* endorsed the mosaic theory approach to the Fourth Amendment, Kerr has remained committed to the sequential approach. Following *Carpenter*, he simply created a digital-age analogue to the sequential approach, which he calls the "Source Rule."[345] As an extension of Kerr's purported *Carpenter* test, the source rule provides Fourth Amendment protection to any and all information derived from a *Carpenter* technology or surveillance technique.[346] Kerr states, "As long as the information reveals some fact about that person's records derived from the regulated technology, the revealing of information should count as a search. One datum is just as protected as the entire database. It's all protected." [347] While Kerr argues that the Source Rule approach is overly inclusive,[348] as small amounts of surveillance would constitute a Fourth Amendment search, this approach raises concerns far greater than being too protective.

Under the guidance of the Kerr's Source Rule, information collected from databases and technologies that fail to meet Kerr's *Carpenter* test criteria will not be protected. As he explains in his analysis of *Carpenter*, "Pre-digital records and their modern equivalents are exempt, sort of like a constitutional grandfather clause. Only new kinds of records that the digital age has enabled can trigger the new search doctrine."[349] Given the vast breadth of technologies and surveillance techniques that are still being litigated post-*Carpenter*, the Source Rule is actually under-inclusive. Under Kerr's strict approach, pole camera surveillance, for example, receives no protection under the *Carpenter* framework. Regardless of the revealing nature of the footage, or the length of time one's home may be surveilled, the Source Rule says warrantless pole camera

[345] Kerr, "Implementing Carpenter," 40.
[346] Kerr, "Implementing Carpenter," 40.
[347] Kerr, "Implementing Carpenter," 40.
[348] Kerr, "Implementing Carpenter," 42.
[349] Kerr, "Implementing Carpenter," 16.

surveillance is permissible. This clearly contradicts the spirit and language of the majority opinion in *Carpenter.*

As Tokson notes, lower court rulings that declined to find that continuous pole-camera surveillance constitutes a search often reach this conclusion because they assert there is not a reasonable expectation of privacy in the exterior or surroundings of one home which are exposed to the public.[350] In *United States v. Tuggle* for example, the Seventh Circuit court held that Tuggle did not have a reasonable expectation of privacy outside of his house or in the area around it, because he had not attempted to shield this area from the public and, thus, he knowingly exposed these areas to public view.[351] Tokson argues this reasoning was rejected by the court in *Carpenter*. "The Court emphasized that mere exposure of something to third parties will not necessarily render it unprotected by the Fourth Amendment," Tokson explains.[352] "When a surveillance practice is especially invasive, comprehensive, and/or inescapable, it may be prohibited by the Fourth Amendment regardless of whether the information it captures might, in theory, be observed by others."[353] Given the Court's rejection of a strict application of the third-party doctrine in *Carpenter*, finding disclosure does not always eliminate Fourth Amendment protection. As a result, Tokson explains that a similar argument must apply to pole cameras. Under the guidance of *Carpenter*, the fact that one exposes the outside of their home or curtilage to onlookers does not suffice to eliminate Fourth Amendment protection in the constant tracking of this area. Additionally, Tokson notes that *Carpenter*'s emphasis on the invasive nature of continuous CSLI applies to continuous pole camera surveillance.[354] While courts may

[350] Tokson, "The Next Wave of Fourth Amendment Challenges," 18.
[351] United States v. Tuggle, 4 F.4th 505, 513-14 (7th Cir. 2021).
[352] Tokson, "The Next Wave of Fourth Amendment Challenges," 18.
[353] Tokson, "The Next Wave of Fourth Amendment Challenges," 18.
[354] Tokson, "The Next Wave of Fourth Amendment Challenges," 18.

try to distinguish pole camera surveillance from the types of information in *Jones* and *Carpenter*,[355] there are no grounds for such a distinction. In the same way the Court found that continuous CSLI tracking creates "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years,"[356] long-term pole camera surveillance has the capacity to do the same. In *People v. Tafoya*, one court argued that "pole camera surveillance shares many of the troubling attributes of GPS tracking…[and] this record 'reflects a wealth of detail' about him and his associations."[357] *Carpenter* extends to pole camera surveillance. This type of information has the capacity to reveal explicit, intimate details when aggregated over a period of time. If Kerr's Source Rule were to be adopted, the privacy harms posed by pole camera surveillance would go unchecked, as this technology is not a product of the digital age. Thus, the Source Rule must be rejected. The mosaic theory must be accepted instead.

The case for the mosaic theory is stronger than its alternative and outweighs its drawbacks. While the Source Rule ostensibly has the virtue of clarity, this functions more like expediency. The Source Rule creates broad definitive rules for new technologies which Kerr suggests deserve *Carpenter* protection, while leaving unprotected data derived from non-digital age sources. This approach trades crucial analyses of our privacy interests, which grow more compelling as the amount of surveillance collected does, for easily applicable, overinclusive, and underinclusive rules. Our Fourth Amendment rights, especially in the rapidly evolving digital age, should not be protected through the whichever approach is most straight-forward. Rather, they should be protected through a framework that is adaptable and responsive to real and emerging privacy harms. The mosaic theory is that framework even if the application of the

[355] United States v. Tuggle 4 F.4th 505, 513-14 (7th Cir. 2021).
[356] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[357] People v. Tafoya, 494 P.3d 613, 622 (Colo. 2021).

theory will require courts to partake in line-drawing. As discussed above, lower court disagreements over the framework demonstrates the complexity of this practice. But, as Tokson notes, line-drawing is required in all areas of the law.[358] Furthermore, he asserts that lower courts seem "perfectly capable of distinguishing between different durations or quantities of surveillance."[359] Indeed, a more explicit endorsement of the mosaic theory would not upend Fourth Amendment jurisprudence, as Kerr implies. Tokson's study demonstrates that lower courts widely accept the guidance from *Carpenter* that the amount of information obtained is a constitutionally relevant factor.[360] Thus, courts across the country already have experience with the mosaic theory, whether that phrase has appeared in their decisions or not.

Additionally, the mosaic theory fits neatly into the existing *Katz* framework, as courts have demonstrated. When determining whether a search has occurred, courts have examined whether the duration of a surveillance violates a reasonable expectation of privacy because of the intimate details that aggregated information has the tendency to reveal.[361] Additionally, the Supreme Court and various lower courts have adopted Justice Alito's analysis from his *Jones* concurrence that reasonable expectations of privacy are intertwined with what people believe law enforcement has the power to do. The longer, more continuous, and more invasive a surveillance is, the more likely it is to violate our reasonable expectation of privacy for both reasons.[362] Courts with experience assessing duration as a consideration in a *Katz* analysis will have no trouble adopting a clearer mosaic theory approach to the Fourth Amendment.

---

[358] Matthew Tokson, "The 'Mosaic Theory' and the Aftermath of Carpenter," *Dorf on Law* (blog), August 3, 2020, http://www.dorfonlaw.org/2020/08/the-mosaic-theory-and-aftermath-of.html.
[359] Tokson, "The 'Mosaic Theory' and the Aftermath of Carpenter."
[360] Tokson, "The Aftermath of Carpenter," 1823.
[361] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[362] Tokson, "The Emerging Principles of Fourth Amendment Privacy."

Beyond the practicality argument for embracing this Fourth Amendment approach, there are other compelling reasons the Supreme Court should invoke a stronger version of the mosaic theory. First, as Professor Paul Rosenzweig argues in his defense of the mosaic theory, the theory is "scientifically accurate."[363] In the digital age, data aggregations are unequivocally more valuable than pieces of data in isolation. Rosenzweig notes, "large data aggregation are how the government tracks potential terrorists who travel internationally, and it is how Google knows what ads to serve you."[364] In other words, reality demonstrates that more information is learned when more data is collected. The law, Rosenzweig argues, ought to reflect this.[365] Rosenzweig supports this normative claim by arguing that the Supreme Court has previously decided cases with at least the partial goal of "accommodating technological reality."[366] Arguably, the Court has decided each landmark digital Fourth Amendment case since *Katz* with technological reality in mind, and in few, namely *Kyllo* and *Carpenter*, with the technological reality of the future in mind as well. Rosenzweig claims that the Court must adapt to the reality of the large-scale data collection made possible by the digital age, and the mosaic theory provides the best framework for doing so.

Lastly, as Kerr himself notes, the mosaic theory is premised on equilibrium adjustment.[367] While Kerr argues the theory is a misguided approach to equilibrium adjustment,[368] other scholars commend this approach for its relevance in the digital age. As Rosenzweig argues, the theory's consistency with technological reality is powerful. The mosaic theory gives courts a framework to address how long-term surveillance violates privacy in ways

[363] Paul Rosenzweig, "In Defense of the Mosaic Theory," *Lawfare* (blog), November 29, 2017, https://www.lawfareblog.com/defense-mosaic-theory.
[364] Rosenzweig.
[365] Rosenzweig.
[366] Rosenzweig.
[367] Kerr, "The Mosaic Theory of the Fourth Amendment," 353.
[368] Kerr, "The Mosaic Theory of the Fourth Amendment," 353.

that smaller-scale surveillance simply cannot. Courts can then expand Fourth Amendment protections or refine them based on the surveillance method's ability to violate a reasonable expectation of privacy. Surely, the mosaic theory is not a bright-line rule, but its flexibility is a virtue. Short-term CSLI should not be a search. The Supreme Court has agreed,[369] and so do lower courts.[370] But only the mosaic theory enables courts to determine that longer-term CSLI collection has the power to erode privacy protections in a unique way. Data collections create mosaics of peoples' routines, relationships, and deeply personal activities. In the digital age, the amount of data the government can collect is constitutionally salient. No framework other than the mosaic theory suffices to safeguard the unique privacy harms of the modern digital era.

While this thesis does not aim to defend against every aspect of the mosaic theory's approach to the Fourth Amendment, it does suggest the mosaic theory is the most defensible framework under which courts should address modern Fourth Amendment issues. The theory's compatibility with both the emerging *Carpenter* test in lower courts and the long-standing *Katz* reasonable expectation of privacy doctrine indicate that an explicit endorsement would fit seamlessly into Fourth Amendment jurisprudence. Furthermore, the mosaic theory's roots of equilibrium adjustment make it the most attractive approach for the Fourth Amendment in the digital age, as its flexibility allows for constant adaptation when necessary.

As lower courts continue to develop the law after *Carpenter*, referencing the intimacy of the information and the amount collected in some cases, but ignoring them in others, it seems plausible that the mosaic theory will continue to receive inconsistent application. Ultimately, the Court may soon be faced with a Fourth Amendment question that requires a stronger endorsement of the mosaic theory. It is in the best interest of *Carpenter*'s legitimacy and, most

[369] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[370] People v. Edwards, 63 Misc. 3d 827 (N.Y. Sup. Ct. 2019).

importantly, Fourth Amendment rights themselves, that the Court holds decisively that the mosaic theory framework should inform jurisprudence in the digital age.

Conclusion

In this thesis I have discussed the Supreme Court's most influential Fourth Amendment cases from the early 18th century through its most recent landmark decision in 2018. I have explored how the Court reshaped Fourth Amendment doctrine from a traditional property-based approach, first developed in *Olmstead,* to a reasonable expectation of privacy test, established in *Katz*. I then examined how the Supreme Court has incorporated new Fourth Amendment rules to address emerging technologies in the digital age. Namely, in the case of *United States v. Jones,* the majority rooted its decision in the traditional trespass-doctrine, but a five-justice majority joined concurring opinions that endorsed a Fourth Amendment approach which addresses how the amount of surveillance changes our reasonable expectations of privacy. This approach, called the mosaic theory, has become a critical aspect of Fourth Amendment law in the era of modern technology, and I dedicate the end of my third chapter to defending the merits of this framework. Additionally, my first chapter discusses the Supreme Court's creation of the third-party doctrine, as it played a crucial role in *Carpenter v. United States,* where it was eventually narrowed by the Court.

Throughout this thesis, I reference leading Fourth Amendment scholar Orin Kerr's poignant observation that the Supreme Court has consistently engaged in a practice called equilibrium adjustment when administering the Fourth Amendment. As new technologies and law enforcement practices develop, upsetting the prior balance between citizens and the government, equilibrium adjustment moves the Court to reshape Fourth Amendment protections

to restore this balance. Equilibrium adjustment is particularly necessary in the digital age. The Court in *Riley* expressed this view, when it found that the search of a cellphone was uniquely distinct from any other category of personal belongings, specifically that it was incomparable to the search of a person's wallet. The Chief Justice recognized the power of modern technology to reframe expectations of privacy and necessitate enhanced Fourth Amendment protections, and the Court responded accordingly. This exercise of equilibrium adjustment continued through the Court's next, and most recent decision, *Carpenter v. United States*.

The second chapter of this paper closely examines *Carpenter v. United States,* where the Court held that the third-party doctrine could not apply to the long-term acquisition of a person's historical cell site location information. I discuss the key arguments of Chief Justice Roberts' opinion, specifically his assertion that extensive CSLI collection has the power, much like GPS data, to reveal intimate and private details of one's life. This chapter also breaks down Orin Kerr and Paul Ohm's interpretations of this decision, finding disagreements in the doctrinal shifts initiated by the decision and the *Carpenter* test established. These scholars do, however, agree that the Supreme Court in *Carpenter* possibly endorsed the mosaic theory approach to the Fourth Amendment. These scholars argue that the Court's emphasis on the extensive nature of the CSLI collection in *Carpenter*, and the Chief Justice's reliance on the *Jones* concurrences, indicate the Court may have used the mosaic theory to reach its decision. Both Kerr and Ohm argue that this theory should be rejected for its difficult administrability, while Tokson indicates support for courts' consideration of the amount of data collected.

Finally, the third chapter of this paper examined how lower courts have interpreted *Carpenter*. This chapter compares the interpretations of Fourth Amendment scholars, described in the second chapter, to Matthew Tokson's comprehensive empirical study of *Carpenter*'s

impact in Fourth Amendment law. Tokson finds that lower courts have not only largely complied with the *Carpenter* decision, but also effectively developed and refined the recent doctrinal shift. Tokson's research also points to the conclusion that lower courts have revealed an emerging *Carpenter* test, in which the nature of the data, the amount gathered, and the automatic nature of disclosure all significantly influence decisions applying the *Carpenter* rationale. Tokson notes that, while this emerging test brings some clarity to the *Carpenter* shift, the Supreme Court needs to provide lower courts with a clearer, more consistent multi-factor test they can apply to all Fourth Amendment cases in the future.

The third chapter also explores *Carpenter*'s endorsement of the mosaic theory approach to the Fourth Amendment. I consider both adoption and rejection of this framework in lower court decisions since *Carpenter*, and ultimately argue that this theory provides an effective way for courts to determine Fourth Amendment searches. The mosaic theory is flawed. This thesis does not attempt to resolve all of its issues, but it does articulate why, particularly in the digital age, acceptance of this approach is the most desirable choice for consistency with doctrinal developments and loyalty to the long-standing tradition of equilibrium adjustment.

BIBLIOGRAPHY

Bradley, Craig M. "Two Models of the Fourth Amendment." *Michigan Law Review* 83, no. 6 (May 1985): 1468–1501. https://doi.org/10.2307/1288896.

Brief for Petitioner, Carpenter v. United States 138 S. Ct. 2206 (2018), (No. 16-402), https://www.aclu.org/legal-document/united-states-v-carpenter-brief-petitioner.

Brief for Electronic Privacy Information Center (EPIC) et al. as Amici Curiae Supporting Petitioner, Carpenter v. United States, 138 S. Ct. 2206 (2018) (August 14, 2017) (No. 16-402). https://epic.org/wp-content/uploads/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.

Caminker, Evan H. "Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?" *Supreme Court Review 2018* (2019): 411–81. https://doi.org/10.1086/702164.

Fairbanks, Robert. "Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter." *Berkeley Journal of Criminal Law 2021* (June 23, 2021) 71–119. https://doi.org/10.15779/Z38DZ03287.

Iannacci, Nicandro. "Katz v. United States: The Fourth Amendment Adapts to New Technology." National Constitution Center. Accessed September 28, 2021. https://constitutioncenter.org/blog/katz-v-united-states-the-fourth-amendment-adapts-to-new-technology.

Kerr, Orin S. "An Equilibrium-Adjustment Theory of the Fourth Amendment." *Harvard Law Review* 125 (December 20, 2011): 476–543. https://harvardlawreview.org/2011/12/an-equilibrium-adjustment-theory-of-the-fourth-amendment/.

Kerr, Orin S. "Defending Equilibrium-Adjustment." *Harvard Law Review Forum* 125 (May 18, 2012): 84–90. https://harvardlawreview.org/2012/05/defending-equilibrium-adjustment/.

Kerr, Orin S. "Implementing Carpenter." In *The Digital Fourth Amendment*. Oxford University Press, Forthcoming, 2018. https://papers.ssrn.com/abstract=3301257.

Kerr, Orin, and Barry Friedman. "Interpretation: The Fourth Amendment." National Constitution Center. Accessed October 10, 2021. https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121.

Kerr, Orin S. "The Mosaic Theory of the Fourth Amendment." *Michigan Law Review* 111, no. 3 (2012): 311–54. https://repository.law.umich.edu/mlr/vol111/iss3/1/

Kerr, Orin S. "Understanding the Supreme Court's Carpenter Decision." *Lawfare* (blog), June 22, 2018. https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision.

Kugler, Matthew B., and Lior Jacob Strahilevitz. "Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory." *The Supreme Court Review* 2015 (January 2016): 205–63. https://doi.org/10.1086/686204.

McCubbin, Sabrina. "Summary: The Supreme Court Rules in Carpenter v. United States." *Lawfare* (blog), June 22, 2018. https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

National Constitution Center. "The 4th Amendment of the U.S. Constitution." Accessed September 30, 2021. https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv.

Ohm, Paul. "The Many Revolutions of Carpenter." *Harvard Journal of Law and Technology* 32, no. 2 (Spring 2019): 357–416. https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech357.pdf.

Oral Argument, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402). https://www.supremecourt.gov/oral_arguments/audio/2017/16-402.

Re, Richard M. "Narrowing Supreme Court Precedent from Below." *Georgetown Law Journal* 104 (December 8, 2015): 921–71. https://papers.ssrn.com/abstract=2699607.

Rosenzweig, Paul. "In Defense of the Mosaic Theory." *Lawfare* (blog), November 29, 2017. https://www.lawfareblog.com/defense-mosaic-theory.

Tokson, Matthew. "The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021." *Harvard Law Review* 135 (May 10, 2022): 1790–1852. https://harvardlawreview.org/wp-content/uploads/2022/04/135-Harv.-L.-Rev.-1790.pdf.

Tokson, Matthew. "The Emerging Principles of Fourth Amendment Privacy." *George Washington Law Review* 88 (July 23, 2019): 1–75. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3425321.

Tokson, Matthew. "42nd Annual Foulston-Siefkin Lecture: The Next Wave of Fourth Amendment Challenges After Carpenter." *Washburn Law Journal* 59 (January 16, 2020): 1–24. https://papers.ssrn.com/abstract=3520366.

Tokson, Matthew. "The 'Mosaic Theory' and the Aftermath of Carpenter." *Dorf on Law (*blog*)*, August 3, 2020. http://www.dorfonlaw.org/2020/08/the-mosaic-theory-and-aftermath-of.html.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193–220. https://doi.org/10.2307/1321160.