Masterpiece or Mess:

The Mosaic Theory of the Fourth Amendment Post-*Carpenter*

Robert Fairbanks*

In Carpenter v. United States, the Supreme Court potentially adopted what has been called the mosaic theory of the Fourth Amendment. The mosaic theory, which looks at the type and amount of information the government gathered in the aggregate, represents a significant departure from traditional Fourth Amendment doctrine. This potential adoption of the mosaic theory has left the lower courts in a difficult position where they must grapple with a variety of problems presented by the doctrine.

This Note aims to explore the post-Carpenter state of the law among the lower courts. It begins by examining lower court decisions that have adopted the mosaic theory. Next, it turns to lower court decisions that declined to apply the mosaic theory. Finally, it discusses broader takeaways and lessons that have emerged from the post-Carpenter cases.

Introduction....72
I.Cases that Applied the Mosaic Theory....76
A. Cell Site Location Information....76
B. GPS Tracking of Vehicles....82
C. Automatic License Plate Readers....84
D. Pole Cameras....88
E. Telephony Metadata....91
F. Aerial Surveillance....92
II.Cases Where Courts Declined to Apply the Mosaic Theory....96

DOI:https://doi.org/10.15779/Z38DZ03287

* J.D candidate, 2022, University of California, Berkeley, School of Law. The author is appreciative to the members of the Berkeley Journal of Criminal Law for all their assistance and hard work during the publishing process. He'd also like to thank Cheyenne Smith for her invaluable advice (and much needed criticism). And lastly, the author thanks Professor Orin Kerr for his guidance and inspirational tweets.

A. Cell Site Location Information.....96
B. GPS Tracking of Vehicles:.....98
C. Pole Cameras.....101
III.Takeaways 103
A. Cell Site Location Information.....103
B. GPS Tracking of Vehicles.....105
C. Automatic License Plate Readers.....106
D. Pole Cameras.....106
E. Big Picture.....107
Conclusion 113
Appendix A.....116
Appendix B.....117

INTRODUCTION

"BIG BROTHER IS WATCHING YOU."[1] The fear of omnipresent government surveillance, famously articulated in George Orwell's *1984*, has persisted across generations and into the present. A majority of Americans "are at least somewhat concerned about how much data is collected about them by . . . the government."[2] This concern is grounded in reality; modern technology has provided the government with a breadth of surveillance techniques against which most are powerless.[3] Not immune to such concerns, the Supreme Court has entered the fray and tried to do its part to avoid a *1984*-esque future while still permitting law enforcement to do its job effectively.[4] Unfortunately, in doing so, one of the Court's

---

[1] GEORGE ORWELL, 1984, 2 (Signet Classics 1950) (1949).

[2] Brooke Auxier & Lee Rainie, *Key Takeaways on Americans' Views About Privacy, Surveillance and Data-Sharing*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/; *see also* SARAH E. IGO, THE KNOWN CITIZEN 5 (2018) ("Privacy, it scarcely needs saying, looms large today. If the drumbeat of headlines and bestsellers is to be believed, Americans are in the midst of an unprecedented privacy crisis —under 'relentless surveillance,' on the road to a fully transparent society, and with 'no place to hide.'") (footnote omitted).

[3] *See* UNITED NATIONS OFFICE ON DRUGS AND CRIME, CURRENT PRACTICES IN ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF SERIOUS AND ORGANIZED CRIME 2 (2009), https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (providing examples of electronic surveillance techniques); *see also* David C. Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 385–87 (2013) (describing the extent of modern surveillance).

[4] *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011) (explaining "that the Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the

more recent efforts created a mess that lower courts are now struggling to work through.

In *Carpenter v. United States*,[5] the Supreme Court, grappling with the realities of modern surveillance technology and fears of Big Brother,[6] potentially adopted what has been called the mosaic theory of the Fourth Amendment.[7] Relevant here, one of the key issues in *Carpenter* was whether the defendant had a reasonable expectation of privacy in his historical[8] cell site location information ("CSLI").[9] The Court held that the defendant indeed had a reasonable expectation of privacy in his historical CSLI and the government's acquisition of those records was a Fourth Amendment search.[10] In reaching its conclusion, the Court stressed the particularly revealing nature of historical CSLI, which could allow the government "near perfect surveillance" of any cell phone user's physical location, revealing all sorts of intimate details about their life.[11] But the Court ruled narrowly, suggesting that the acquisition of less than seven days of CSLI may not be a search.[12] It also left open the question of how

---

status quo level of protection").

[5] Carpenter v. United States, 138 S. Ct. 2206 (2018). For a thorough description of the case see Orin S. Kerr, *Implementing Carpenter* (UNIV. SOUTHERN CALIFORNIA LAW LEGAL STUDIES WORKING PAPER 18–29, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257; Elle Xuemeng Wang, Note, *Erecting a Privacy Wall Against Technological Advancements: The Fourth Amendment in the Post*-Carpenter *Era*, 34 BERKELEY TECH. L.J. 1205 (2019).

[6] *See* United States v. Howard, 426 F. Supp. 3d 1247, 1249 (M.D. Ala. 2019) (describing *Carpenter* as the Supreme Court's "recent attempt to adapt the [Fourth] Amendment to twenty-first-century fears that Big Brother is watching").

[7] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Gray & Citron, *supra* note 3; Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y SPECIAL ISSUE 1 (2012).

[8] Historical CSLI is used to track past movements as opposed to real-time CSLI which is used to track location contemporaneously.

[9] *See Carpenter*, 138 S. Ct. 2206 at 2216 ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."). "CSLI refers to information cell phones convey to nearby cell towers. Info from several towers can be used to 'triangulate' a phone's location." Stephanie Lacambra, *Cell Phone Location Tracking or CSLI: A Guide for Criminal Defense Attorneys*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/files/2017/10/30/cell_phone_location_information_one_pager_0.pdf (last visited Jan. 16, 2021).

[10] *Carpenter*, 138 S. Ct. 2206 at 2216.

[11] *Id.* at 2217–18.

[12] *See id.* at 2217 n.3 (holding "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our

to treat real-time CSLI.[13]

In differentiating between the acquisition of various durations and types of CSLI, the Court adopted, or at least opened the door to, the mosaic theory. In essence, the mosaic theory looks at the government's investigative action and asks whether the type and amount of information gathered, when viewed in the aggregate, is so revealing that the action should be considered a Fourth Amendment search, even if the individual data points do not reveal that much in isolation.[14] Put in terms of the mosaic metaphor, the individual data point is a singular tile, which viewed by itself is largely meaningless. But when combined with other data points a clearer picture emerges, just like when many tiles are combined to create a beautiful mosaic. Without enough tiles, no mosaic will emerge. As a result, any given investigative technique might in one case be considered a search, while in another case the same technique may not be considered a search because the aggregated data revealed less information. The mosaic theory contrasts with what has been called the sequential approach, the traditional method of determining when government action is a search.[15] In the sequential approach, the question is binary; any given government action either is or is not a search. It does not consider how revealing any aggregate of the information gathered ends up being. Using *Carpenter* as an example, had the Court applied the sequential approach, the duration of the accessed CSLI would have been irrelevant.

---

purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

[13] *Id.* at 2220.

[14] *See* Kerr, *supra* note 7, at 320 ("Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group. The mosaic theory is therefore premised on aggregation: it considers whether a set of non-searches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic."); Gray & Citron, *supra* note 3 at 390 ("The fundamental insight behind the mosaic theory is that we can maintain reasonable expectations of Fourth Amendment privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of that whole."); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 205. ("The mosaic theory of the Fourth Amendment holds that, when it comes to people's reasonable expectations of privacy, the whole is greater than the sum of its parts. More precisely, it suggests that the government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic.").

[15] *See* Kerr, *supra* note 7, at 315–16 ("Fourth Amendment analysis traditionally has followed what I call the sequential approach: to analyze whether government action constitutes a Fourth Amendment search or seizure, courts take a snapshot of the act and assess it in isolation.").

The move from the sequential approach to the mosaic theory has created substantial uncertainty among lower courts. Rather than being a masterpiece that allows courts to deftly draw lines through difficult technology-related Fourth Amendment questions, the Supreme Court's potential adoption of the mosaic theory has left the present state of the law a mess. Lower courts cannot agree on when, if at all, to apply the mosaic theory. When a court does decide to use it, the court is faced with a major line-drawing problem. But despite its issues, the mosaic theory offers courts a wide degree of flexibility and latitude, a tempting prospect in the ever-changing face of developing technology. This Note explores the current state of the mosaic theory in a post-*Carpenter* world. I provide summaries of post-*Carpenter* cases where courts applied the mosaic theory along with descriptions of similar cases where courts declined to do so.

Before I continue, I would like to provide a few words on what this Note is not. It is not meant to be an exhaustive history and explanation of the Fourth Amendment or the mosaic theory. Nor do I attempt to solve or fix the mosaic theory.[16] I also do not discuss the closely related issue of the post-*Carpenter* future of the third-party doctrine with regards to modern technology, such as service provider data.[17] I merely aim to provide a picture of how the lower courts have applied (or have not applied) the mosaic theory in the roughly two years since *Carpenter* and provide some insights on lessons learned.

In Part I, I examine post-*Carpenter* cases that have used the mosaic theory. Depending on the relevancy of the specific facts to the court's reasoning and the depth of the court's mosaic theory analysis, I spend varying amounts of time describing each case. In Part II, I turn to cases involving the same technology-based investigatory techniques where the courts did not apply the mosaic theory and instead relied on the sequential approach. I summarize the courts' decisions for each investigatory technique and detail the courts' reasoning behind applying the sequential approach rather than the mosaic theory. Finally, in Part III, I discuss takeaways that emerged from the post-*Carpenter* cases. I begin Part III with case-specific takeaways, and then move on to the bigger picture.

---

[16] *See generally* Slobogin, *supra* note 7 (explaining how to overcome the difficulties in implementing the mosaic theory).

[17] *Compare* United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) ("Thus, the government's warrantless acquisition from Kik of the IP address data at issue here in no way gives rise to the unusual concern that the Supreme Court identified in *Carpenter*. . . .") *with* United States v. Kidd, 394 F. Supp. 3d 357, 368 (S.D.N.Y. 2019) ("Still . . . it may caution against the categorical approach found in most of the post-*Carpenter* cases holding that there is no reasonable expectation of privacy in IP address information.").

I. CASES THAT APPLIED THE MOSAIC THEORY

In light of *Carpenter*, some courts have embraced the mosaic theory for a variety of technology-based investigatory techniques: CSLI, GPS tracking of vehicles, automatic license plate readers ("ALPR"), pole cameras, telephony metadata, and aerial surveillance.

A. Cell Site Location Information

CSLI is the information cell phones transmit to nearby cell towers. By looking at CSLI information from multiple towers, law enforcement can track a suspect's movements over a given period of time in the past or in real-time.[18] In applying the mosaic theory to CSLI, courts have drawn a variety of lines as to what duration of historical and real-time CSLI constitutes a search.[19] I begin by looking at historical CSLI, starting with the shortest duration of CSLI considered a search.

In *Commonwealth v. Wilkerson*, the Supreme Judicial Court of Massachusetts held that "[c]ollecting more than six hours of CSLI data invades a defendant's reasonable expectation of privacy, and, therefore, under the Fourth Amendment to the United States Constitution and Article 14 of the Massachusetts Declaration of Rights, requires a warrant supported by a showing of probable cause."[20] While the court provided minimal insight into its determination that six hours of CSLI data constituted a search, it is clear that the court adopted the mosaic theory. It mentioned, "[t]he collection of ***extended*** CSLI data raises significant constitutional concerns."[21] Later, the court noted, "when determining whether a search has occurred, the relevant inquiry is the ***amount*** of data that the government receives, not that which it ultimately seeks to introduce at trial."[22] The focus on the duration of CSLI accessed by the government fits squarely within the mosaic theory's framework.

---

[18] *See* Lacambra, *supra*, note 9.

[19] Near the end of the publication process for this Note, the Seventh Circuit applied the mosaic theory to find that the short-term use of a real-time CSLI was not a search. While I do not include the case in this Note's analysis due to time constraints, I flag it for the reader's consideration. *See* United States v. Hammond, No. 19-2357, 2021 WL 1608789, at *9–11 (7th Cir. Apr. 26, 2021) (holding "that [law enforcement] did not conduct a Fourth Amendment 'search' by requesting the real-time CSLI of a suspect for multiple armed robberies, for whom officers had probable cause, where the officers only collected real-time CSLI for a matter of hours while the suspect travelled on public roadways, and law enforcement limited its use of the CSLI to the purpose of finding the armed suspect who they had reason to believe was likely to engage in another armed robbery").

[20] Commonwealth v. Wilkerson, 156 N.E.3d 754, 766 (2020).

[21] *Id.* at 767 (emphasis added).

[22] *Id.* at 768 (internal citations omitted) (emphasis added).

Further clarifying the court's use of the mosaic theory is its citation to *Commonwealth v. Estabrook*.[23] *Estabrook,* a pre-*Carpenter* case, held that less than six hours of CSLI data was not a search under Article 14 of the Massachusetts Declaration of Rights, while two weeks' worth of data was a search.[24] The court noted, "the Commonwealth may obtain historical CSLI for a period of six hours or less relating to an identified person's cellular telephone from the cellular service provider without obtaining a search warrant, because such a request does not violate the person's constitutionally protected expectation of privacy." The court's willingness to reach different outcomes based on the duration of the government's data access provides further evidence of its adoption of the mosaic theory, even pre-dating *Carpenter*.

Unfortunately, the opinion in *Estabrook* failed to clarify why it drew the line at six hours for a search; it simply emphasized the importance of establishing a bright line rule.[25] But while the reasoning may be lacking, the outcome is clear. Short-term CSLI data from a period of six hours or less is not a search while anything more is a search.[26]

It is less clear if the Supreme Judicial Court actually intended to cover Fourth Amendment searches in *Wilkerson*.[27] The *Wilkerson* court cited both *Carpenter* and *Estabrook* in its holding.[28] But *Carpenter* did not address the question of short-term CSLI[29] and *Estabrook* was decided

---

[23] *See id.* at 766.

[24] Commonwealth v. Estabrook, 472 Mass. 852, 858 (2015).

[25] *See id.* at 858 n.11.

[26] *Wilkerson*, 156 N.E.3d at 766. The Supreme Judicial Court held the same in a slightly earlier case but offered even less explanation as to the difference between short-term and long-term CSLI data, so I focus on Wilkerson instead. *See* Commonwealth v. Hobbs, 125 N.E.3d 59, 67 n.9 (2019) ("The Commonwealth need not obtain a warrant, however, if it requests six hours or less of 'telephone call' CSLI.") (internal citation omitted).

[27] Orin Kerr (@OrinKerr), TWITTER (Nov. 5, 2020, 1:08 PM), https://twitter.com/OrinKerr/status/1324458620923252736.

[28] *Wilkerson*, 156 N.E.3d at 766.

[29] Carpenter v. United States, 138 S. Ct. 2206, 2238 n.3 (2018) ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

under the Massachusetts Declaration of Rights, not the Fourth Amendment.[30] Perhaps the court did not mean to make this particular ruling under the Fourth Amendment.[31] While this is possible, it doesn't strike me as likely. Rather, I think the court decided that, in light of *Carpenter*, the mosaic theory applied to CSLI in the Fourth Amendment context, and so aligned its Article 14 decisions with subsequent Fourth Amendment CSLI cases, keeping the line at six hours.[32] If that is the case, it is significant. Six hours is a much lower threshold than any of the other courts that have applied the mosaic theory to CSLI and found a search.

Addressing longer periods of data access, in *State v. Gibbs*, the Court of Appeals of South Carolina held that the government's acquisition of five days' worth of historical CSLI was a search.[33] The court held that "CSLI collection for a period of five days does not adequately curtail the Court's privacy concerns so as to render the five-day CSLI collection not a search pursuant to the Fourth Amendment."[34] Without going into detail, the court focused its concern on the nature of CSLI, "revealing not only [the defendant's] particular movements, but through them his familial, political, professional, religious, and sexual associations."[35] Notably, as with *Carpenter*, the court did not mention the time period in which historical CSLI could be used without a warrant. Thus, the court left open the possibility of not applying the mosaic theory in future cases and determining that any use of CSLI is a search, regardless of duration. But, because the decision relied on the duration of the CSLI that the government accessed, I included it as a case which, at a minimum, could be applying the mosaic theory.

By contrast, in *People v. Edwards*, the Bronx Supreme Court held that the government's use of two days' worth of historical CSLI was not

---

[30] Commonwealth v. Estabrook, 472 Mass. 852, 854 (2015) (concluding "that a defendant's reasonable expectation of privacy protected under art. 14 of the Massachusetts Declaration of Rights is not violated where the Commonwealth requests up to six hours of historical CSLI without obtaining a search warrant.").

[31] Orin Kerr (@OrinKerr), TWITTER (Nov. 5, 2020, 1:13 PM), https://twitter.com/OrinKerr/status/1324459894737571842 ("Not sure if it's just a stray phrase, or if the court meant to say const rulings are now applied to be federal, too.").

[32] *Hobbs* supports this as the citation to *Carpenter* included a parenthetical addressing the Fourth Amendment while the citation to *Estabrook* included a parenthetical addressing Article 14 of the Massachusetts Declaration of Rights. *See* Commonwealth v. Hobbs, 125 N.E.3d 59, 67 (2019).

[33] State v. Gibbs, No. 2017-001846, 2020 WL 4814266 at *1, *4 (S.C. Ct. App. Aug. 19, 2020).

[34] *Id.* at *4.

[35] *Id.* (cleaned up).

a search.[36] Noting that the Supreme Court had "expressly carved out" short-term CSLI from *Carpenter*, the court used the mosaic theory to determine that a two-day period of CSLI revealed little about an individual:

> By way of contrast, in this court's view, *short-term* CSLI data that is carefully targeted to a specific time in order to determine whether defendant was present at the scene of a crime that was committed in a public place is *not* a search, and is therefore not subject to Fourth Amendment warrant requirements.
>
> The difference between long-term and short-term CSLI data is stark: *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.[37]

While the court clearly explained differences between short-term and long-term CSLI, it was not clear as to why it considered two days short-term. The court attempted to answer this question by noting that the government only used the CSLI data to determine the defendant's location at the crime scene.[38] But two days of collection gathered far more information than a single location, and undoubtedly revealed more about the defendant's private life. The court determined that two days' worth of CSLI data wasn't enough time to reveal "all of defendant's movements over an extended period of time,"[39] but it failed to address the distinction between the seven days of CSLI in *Carpenter* and the two days at issue here. The court emphasized the government's limited purpose for acquiring the CSLI data,[40] but the government's intention did not change the amount of information it learned from the data it acquired. Thus, if governmental intent becomes a factor in a mosaic theory analysis, courts may permit the government to acquire significant amounts of data, so long as it only uses a certain amount for specific reasons during its prosecution.

When using the mosaic theory, courts have applied similar reasoning from historical CSLI cases to cases involving real-time CSLI collection. In *People v. Tham Bui*, the Court of Appeal for the Sixth District of California held that the government's use of one-and-a-half hours of real-time CSLI to locate a suspect was not a search.[41] The court focused on two factors in differentiating the present case from *Carpenter*: the short

---

[36] People v. Edwards, 63 Misc. 3d 827, 828, 831 (N.Y. Sup. Ct. 2019).

[37] *Id.* at 832 (emphases in original) (internal citations omitted).

[38] *Id.*

[39] *Id.* at 831.

[40] *Id.*

[41] People v. Tham Bui, No. H044430, 2019 WL 1325260 at *21 (Cal. Ct. App. Mar. 25, 2019), *review denied* (July 10, 2019), *cert. denied sub nom.* Tham Bui v. California, 140 S. Ct. 409, 205 L. Ed. 2d 232 (2019).

timeframe law enforcement used the CSLI and their purpose for using it.[42] The court reasoned that for the one-and-a-half hours that law enforcement used CSLI, it actively pursued the defendant as he drove on public roads.[43] As such "[h]e had no reasonable expectation of privacy in his real time location or movements in a vehicle on public streets."[44] The court highlighted that law enforcement merely attempted to locate the defendant and did not collect information against him, although the court allowed the government to use that information in its subsequent prosecution.[45]

While the court held that the use of real-time CSLI was not a search in this case, it specifically acknowledged that it had:

> not decided that obtaining real-time CSLI is never a search or that real-time CSLI can be used to track a cell phone, and presumably its user, into a private home or business. . . . Neither have we suggested that use of real-time CSLI to conduct surveillance of an individual over a more extended period would not constitute a search.[46]

Interestingly, the court limited the applicability to future cases when it centered its holding on the fact that law enforcement located the defendant on public roads.[47] The court failed to address if its holding would apply had the defendant ultimately been located at his home, or another private residence. Notably, law enforcement could not have been aware whether the defendant would remain in a public space while it accessed CSLI.

The court did explain its reasoning for declining to address the issue of longer term, real-time CSLI. It emphasized Justice Sotomayor's concurrence in *United States v. Jones*,[48] where she expressed concern about pervasive governmental surveillance and the potential for abuse when the government has "unrestrained power to assemble data that reveal private aspects of identity."[49] Here, the court stated that the brief use of CSLI was only intended "to help visually locate [the suspect] and arrest him on public streets," apparently unconcerned with the government's potential to learn more about the defendant's private aspects of identity through CSLI.[50]

---

[42] *Tham Bui*, 2019 WL 1325260 at *21.
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring).
[49] People v. Tham Bui, No. H044430, 2019 WL 1325260 at *21 (Cal. Ct. App. Mar. 25, 2019).
[50] *See id.* at *21–22.

Similarly, in *Sims v. State*, the Court of Criminal Appeals of Texas held that the use of three hours' worth of real-time CSLI to locate the defendant was not a search.[51] The court clearly decided to apply the mosaic theory, noting "[w]hether a particular government action constitutes a 'search' or 'seizure' does not turn on the content of the CSLI records; it turns on whether the government searched or seized 'enough' information that it violated a legitimate expectation of privacy."[52] The court reasoned that *Carpenter* applied to real-time CSLI in addition to historical CSLI.[53] However, three hours was not "'enough' information that it violated a legitimate expectation of privacy" because the location records did not reveal the privacies of life at issue in *Carpenter*.[54] As with *Tham Bui*, the court limited its ruling to the present facts, stating "[w]hether a person has a recognized expectation of privacy in real-time CSLI records must be decided on a case-by-case basis."[55]

In *United States v. Walker*, the District Court for the Eastern District of North Carolina held that the government's actions did not constitute a search when it obtained records listing the phone numbers and locations of all cellular devices within a certain radius, known as a tower dump, to identify the defendant.[56] The court used the mosaic theory to differentiate the tower dump from the use of CSLI in *Carpenter*, highlighting that a tower dump did not provide significant information about any single individual's movement.[57] Noting that the CSLI did not cover an extended period of time, the court reasoned:

> Instead, the CLSI [sic] tower dump information gathered here is more akin to "conventional surveillance techniques" and tools, such as security cameras and fingerprint collections, which capture data from every individual who came into contact with the crime scene in the manner revealed by the technology at issue.[58]

Essentially, a tower dump is the briefest period for which the government can use CSLI because it only captures a single moment. The

---

[51] Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App. 2019), *cert. denied*, 139 S. Ct. 2749 (2019). Over the course of those three hours, the suspect's phone was pinged multiple times (but less than five). *Id.* at n.18.

[52] *Id.* at 645–46.

[53] *Id.* at 645 n.15 ("The nature of real-time CSLI records are not meaningfully different than in Carpenter.").

[54] *Id.* at 646 (cleaned up).

[55] *Id.*

[56] United States v. Walker, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *1, *5 (E.D.N.C. July 20, 2020).

[57] *See id.* at *7–8.

[58] *Id.* at *8 (internal citations omitted).

court reasoned that the tower dump did not allow the government to track the movement of a suspect over time, "chronicling that individual's private life for days," but merely provided a singular location where the suspect had once been.[59] Therefore, the privacy concerns in *Carpenter* did not apply.[60]

While not a CSLI case, the Superior Court of Pennsylvania reached a similar conclusion in *Commonwealth v. Dunkins*. It held that law enforcement's use of WiFi connection data, used in a similar manner as CSLI from a tower dump, was not a search.[61] Law enforcement used the WiFi connection data from an entire college dorm to narrow down its list of suspects.[62] It eventually arrested the defendant after identifying him as the only male logged into the WiFi who was not a dorm resident.[63] The court differentiated the present case from *Carpenter* in two ways. To the court, it was significant that the data could only track individuals on the campus wireless network, making it a more limited form of surveillance than the CSLI in *Carpenter*.[64] Relatedly, the campus had an internet use policy that allowed for the collection and disclosure of all internet data.[65] More relevant here, the court compared the WiFi connection data with data obtained from a tower dump:

> In this case, Appellant fails to acknowledge the *Carpenter* decision did not invalidate "tower dump" requests by law enforcement to identify all of the devices that were connected to one particular cell site during a particular interval. . . .
>
> The campus police did not target a specific individual or attempt to track an individual's movements but instead merely sought to compile a list of all the devices signed on to the WiFi in the Hassler dorm at the time of the robbery.[66]

In other words, the information used by law enforcement did not sufficiently form a mosaic of any individual's movements, it was only a single snapshot in time.

B. GPS Tracking of Vehicles

Compared to CSLI, fewer courts have applied the mosaic theory

---

[59] *Id.* at *7–8.
[60] *Id.* at *8.
[61] Commonwealth v. Dunkins, 229 A.3d 622, 625 (2020), *appeal granted*, No. 118 MAL 2020, 2020 WL 4462644 (Pa. Aug. 4, 2020).
[62] *Id.*
[63] *Id.* at 629.
[64] *Id.*
[65] *Id.*
[66] *Id.*

to GPS tracking of vehicles. But from the cases thus far, courts have applied similar reasoning in establishing the necessary duration for when the government's use of GPS location data of a vehicle becomes a search.

In *United States v. Diggs*, the District Court for the Northern District of Illinois, Eastern Division held that the government conducted a search when it acquired a month's worth of a vehicle's GPS data.[67] The court held that accessing the long-term GPS data was a search because it "fit[] squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*."[68] The data in question provided:

> time-stamped entries giving the Lexus's approximate street address (usually at the block level, such as "5701-5799 S Campbell Ave, Chicago, IL, 60629") each time it was turned on, approximately every five minutes while it was being driven, and each time it was parked. According to the detective, "[g]reater detail" beyond those approximate street addresses "c[ould] be extracted from the map points" using "the software program that manages the GPS data," which allowed the detective to "narrow[ ]" each recorded location "to specific latitude and longitude way points."[69]

In explaining the privacy concerns at issue, the court discussed several different ideas. Comparing the present case to *Carpenter*, it highlighted that "accessing a historical database of GPS information—means that '[w]hoever the suspect turns out to be, he has effectively been tailed' for the entire period covered by the database."[70] It found the retrospective nature of the GPS data particularly significant because it provided information to law enforcement that was "otherwise unknowable."[71] Furthermore, the court found that "[t]he GPS data provide[d] a precise, comprehensive record of [the defendant's] public movements over the course of a month."[72] The court recognized that the defendant was not the exclusive driver of the car but "given the duration and level of detail of the GPS data, the possibility that some of the data does not reflect [the defendant's] movements does not push the government's acquisition of the data back over the line at which it became a search."[73]

---

[67] United States v. Diggs, 385 F. Supp. 3d 648, 649 (N.D. Ill. 2019), *reconsideration denied*, No. 18 CR 185, 2020 WL 208826 (N.D. Ill. Jan. 14, 2020).

[68] *Id.* at 652.

[69] *Id.* at 650 (internal citations omitted).

[70] *Id.* at 652 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2218).

[71] *Id.*

[72] *Id.*

[73] *Id.*

Contrastingly, in *Kinslow v. State*, the Court of Appeals of Indiana held that the government did not conduct a search when it used approximately six hours of GPS tracking data.[74] After intercepting a package containing drugs, law enforcement inserted a GPS tracking device into the package.[75] The defendant eventually picked up the package and law enforcement subsequently stopped and arrested him after six hours of tracking.[76] The court focused its analysis on both a *Jones*-type trespass test[77] and the lack of a reasonable expectation of privacy based on the package specifically, but briefly considered a reasonable expectation of privacy argument based on *Carpenter* and the GPS data in a footnote.[78] The court held that the CSLI at issue in *Carpenter* implicated the "privacies of life" but here, "[b]ecause the tracking of [the defendant] lasted only approximately six hours and because the electronic devices used here do not provide an intimate window into a person's life, we find that *Carpenter* has no bearing on this case."[79]

C. Automatic License Plate Readers

Automatic License Plate Readers ("ALPR") "are high-speed, computer-controlled camera systems that . . . capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server."[80] While courts have been willing to apply the mosaic theory to ALPRs, they have unanimously found that the usage of ALPRs to track individuals does not constitute a search.

In *Commonwealth v. McCarthy*, the Massachusetts Supreme Judicial Court concluded that the government's use of data generated by four

---

[74] Kinslow v. State, 129 N.E.3d 810, *1–2 (Ind. Ct. App.), *transfer denied*, 134 N.E.3d 1020 (Ind. 2019).

[75] *Id.* at *1.

[76] *Id.*

[77] United States v. Jones, 565 U.S. 400, 404–05 (2012).

[78] *Kinslow*, 129 N.E.3d 810, *2–3.

[79] *Id.* at *9 n.6. While it's possible to read the court's opinion as applying a sequential approach in differentiating GPS data from CSLI, the inclusion of the length of time the tracking took place suggests the court at least considered the rationale underlying the mosaic theory.

[80] *Automated License Plate Readers (ALPRs)*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/automated-license-plate-readers-alpr (Aug. 28, 2017).

ALPRs did not constitute a Fourth Amendment search.[81] Police were investigating the distribution of heroin from a residence.[82] While surveilling the location, the police observed a vehicle and added its license plate number to an ALPR list set to notify officers whenever it crossed over one of two bridges.[83] Using historical ALPR data, they also created a spreadsheet containing the dates, times, directions, and lanes that the vehicle had traveled on the two bridges over approximately ten weeks.[84] The spreadsheet showed that the vehicle had crossed the bridges a total of forty-eight times.[85] The police eventually arrested the defendant after receiving an alert that the vehicle had crossed one of the bridges.[86]

As a preliminary matter, the court explicitly adopted the mosaic theory as the "theoretical foundation" for deciding the case because "the color of a single stone depicts little, but by stepping back one can see a complete mosaic."[87] The court offered a thorough discussion of the mosaic theory, highlighting factors to consider when determining whether a government action might become a search. One factor to consider is whether an individual would "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."[88] Another factor is whether the government action revealed more than a passerby would normally observe during the regular course of life.[89] Yet another factor to consider is what the mosaic reveals about an individual, focusing on whether the aggregate provided "a highly detailed profile, not simply of where we go, but by easy inference, of our associations – political, religious, amicable and amorous, to name only a few – and of the pattern of our professional and avocational pursuits."[90]

---

[81] Commonwealth v. McCarthy, 484 N.E.3d 493, 494 (Mass. 2020).
[82] *Id.* at 495.
[83] *Id.* at 495–96.
[84] *Id.* at 496.
[85] *Id.*
[86] *Id.*
[87] *Id.* at 504–05.
[88] *Id.* at 504 (internal citations omitted).
[89] *Id.* ("[T]he whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.") (internal citations omitted).
[90] *Id.* at 504–05 (internal citations omitted).

The *McCarthy* court ultimately framed the issue as "whether ALPRs produce a detailed enough picture of an individual's movements so as to infringe upon a reasonable expectation that the Commonwealth will not electronically monitor that person's comings and goings in public over a sustained period of time."[91]

The court began by considering ALPRs generally, noting the ways in which the technology could implicate the Fourth Amendment through the mosaic theory.[92] The analysis boiled down to two primary concerns: the number of ALPR cameras and their locations.[93] Given enough cameras, the court reasoned, the historical location data from an ALPR system would qualify as a Fourth Amendment search because they would allow law enforcement to "reconstruct people's past movements."[94] The placement of cameras further affects the analysis because surveillance of especially sensitive locations such as the home and places of worship reveals more about an individual than a camera on an interstate highway.[95] The court also touched on the notification list, highlighting that, given enough cameras, the police could know someone's precise location any time they decided to drive.[96]

Here, the court emphasized that the record in front of it did not include the entire ALPR system of Massachusetts but was limited to four cameras spread over two bridges.[97] Given the number and location of cameras, the court held

> This limited surveillance does not allow the Commonwealth to monitor the whole of the defendant's public movements, or even his progress on a single journey. . . . Such a limited picture does not divulge "the whole of the defendant's physical movements," or track enough of his comings and goings so as to reveal "the privacies of his life."[98]

The court concluded that four cameras at the ends of two bridges did not meet the necessary threshold, but it did not draw a specific line where ALPR usage would cross into Fourth Amendment search territory.[99]

---

[91] *Id.* at 505.
[92] *Id.* at 506–07.
[93] *See id.* at 506.
[94] *Id.*
[95] *Id.*
[96] *Id.* at 507.
[97] *Id.* at 506.
[98] *Id.* at 508–09 (internal citation omitted).
[99] *Id.* In a concurring opinion, Chief Judge Gants agreed with the court's analysis using the mosaic theory. *Id.* at 512 (Gants, C.J., concurring). He highlighted the issue of the difficulties in determining where to draw the line for when a government action becomes

Judge Bea's concurring opinion in *United States v. Yang*,[100] decided by the Ninth Circuit, similarly concluded that the government's use of ALPR data to locate a suspect's rental car was not a search.[101] Judge Bea emphasized that because the car was only observed once by an ALPR, the database searched by law enforcement did not "reveal[] the whole of Yang's physical movements."[102] However, Judge Bea reviewed information regarding the growing prevalence of ALPRs and, much like the court in *McCarthy*, left open the possibility of ALPR data use constituting a search:

> ALPRs are becoming more and more common and therefore capturing more and more data, which when aggregated, may be able to reveal the whole of one's physical movements.
>
> . . . .
>
> I understand that ALPRs may in time present many of the same issues the Supreme Court highlighted in *Carpenter*. ALPRs can effortlessly, and automatically, create voluminous databases of vehicle location information. If enough data is collected and aggregated, this could have the ability to identify quickly and easily the precise whereabouts and lifestyle habits of those whose vehicle information is recorded. ALPRs also collect information without individualized suspicion, and records can be maintained for years. In retrospective searches, detailed and potentially private information may be exposed, though it is debatable whether license plate location data would ever provide the same "near perfect surveillance" that cell phone location data does.[103]

Similarly, in *Uhunmwangho v. State*, the Ninth Court of Appeals of Texas held that the use of data generated by two ALPRs was not a search.[104] When law enforcement stopped the defendant for speeding, she acted nervously and provided inconsistent information to the officers, prompting a search.[105] During the stop, they ran her license plate number

---

a search and offered his take on potential solutions. *Id.* at 513. More significantly, he emphasized the importance of law enforcement maintaining the factual details for any database search parameters (e.g., duration, number of cameras, etc.) because of their importance to a mosaic theory analysis. *Id.* at 514–15.

[100] United States v. Yang, 958 F.3d 851, 862–63 (9th Cir. 2020). The majority opinion sidestepped the issue of whether the use of ALPR data was a search by deciding the case on standing grounds. *See id.* at 858 ("The Government correctly framed its argument as an issue regarding the defendant's standing to challenge the alleged search in this case.").

[101] *Id* at 863 (Bea, J., concurring).

[102] *Id.* at 862–63 (Bea, J., concurring).

[103] *Id.* at 863 (Bea, J., concurring) (internal citations omitted).

[104] Uhunmwangho v. State, No. 09-19-00119-CR, 2020 WL 1442640, at *1 (Tex. App. Mar. 25, 2020).

[105] *Id.*

through an ALPR database that received data from two ALPRs positioned on a highway. The search yielded one photograph of the defendant's car.[106] While the court focused much of its analysis on the general lack of a reasonable expectation of privacy while driving on public roads, the court ventured into mosaic theory territory. It distinguished this case from *Carpenter* because here, the database search only "retrieved a single photograph," suggesting that the result may have been different had the database provided more data.[107]

D. Pole Cameras

As with GPS, few courts have applied the mosaic theory to pole cameras and other video surveillance directed at homes. The courts that have applied the mosaic theory to pole cameras have drawn a variety of lines to determine what duration of pole camera usage constitutes a search.

In *People v. Tafoya*, the Colorado Court of Appeals held that three-month-long pole camera surveillance of a suspect's house constituted a search.[108] Recognizing that its decision differed from many other courts' holdings, the court held that the video surveillance constituted a search because of its "nature, . . . continuity, and particularly. . .duration."[109] In comparing the *Tafoya* facts to the *Jones* concurrences and to *Carpenter*, the court reasoned that "[v]isual video surveillance spying on what a person is doing in the curtilage of his home behind a privacy fence for months at a time is at least as intrusive as tracking a person's location — a dot on a map — if not more so."[110] In applying the mosaic theory, the court noted the importance of considering the length of the surveillance because otherwise there would be "no temporal cap on how many months or years the police could have continued the video surveillance of Tafoya's property."[111] The court repeatedly emphasized the significance of the pole camera surveillance system's constant monitoring combined with the duration of the surveillance.[112] It explained that it would be impossible for law enforcement or a neighbor to do the same type of monitoring without the use of such technology.[113] Even though the outside of

---

[106] *Id.* at *1, 6.
[107] *Id* at *8.
[108] People v. Tafoya, 2019 COA 176, *1, *cert. granted*, No. 20SC9, 2020 WL 4343762 (Colo. June 27, 2020).
[109] *Id.* at *6.
[110] *Id.* at *8.
[111] *Id.* at *9.
[112] *Id.* (internal citations omitted).
[113] *Id.* at *7, *9.

a house is observable to the public, "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[114]

The court also described the privacy concerns of long-term pole camera surveillance around a house, stating that it "could reveal considerable knowledge of one's comings and goings for professional and religious reasons, not to mention possible receptions of others for these and possibly political purposes."[115] Or put another way, "the use of targeted, long-term video surveillance will necessarily include a mosaic of intimate details of the person's private life and associations."[116]

Similarly, in *Commonwealth v. Mora*, the Supreme Judicial Court of Massachusetts held "that the continuous, long-term pole camera surveillance targeted at the residences of [the two defendants] well may have been a search within the meaning of the Fourth Amendment, a question [the court did] not reach, but certainly was a search under art. 14."[117] In *Mora*, law enforcement used five cameras in total to film one defendant's home for 169 days and another defendant's for 62 days.[118] Much like the *Tafoya* court, the *Mora* court began its analysis by acknowledging that "[m]ost courts to have addressed pole camera surveillance have concluded that it does not infringe on any reasonable expectation of privacy."[119] Interestingly, although the court had already adopted the mosaic theory, it declined to use it in a Fourth Amendment analysis in this case:

> The defendants urge us to follow in the footsteps of these courts, and to apply the "mosaic theory," which we adopted in *Commonwealth v. McCarthy* to conclude that the extended and targeted pole camera surveillance of the defendants violated their reasonable expectations of privacy. Neither we, nor the United States Supreme Court, have considered the constitutional implications of the long-term and targeted video surveillance at issue in this case. Because the status of pole camera surveillance "remains an open question as a matter of Fourth Amendment jurisprudence," we will not "wade into these Fourth Amendment waters. Instead, we decide the issue based on our State Constitution, bearing in mind that

---

[114] *Id.* at *9 (internal quotations omitted).
[115] *Id.* at *8.
[116] *Id.* (internal citations omitted).
[117] Commonwealth v. Mora, 485 Mass. 360, 361 (2020). *See also* Commonwealth v. Cruz-Gonzalez, No. 1977CR00467, 2020 WL 7055431 at *8 (Mass. Super. Nov. 30, 2020) (holding long-term pole camera surveillance directed at residences was a search).
[118] *Mora*, 485 Mass. at 362.
[119] *Id.* at 364.

> art. 14 . . . does, or may, afford more substantive protection to individuals than that which prevails under the Constitution of the United States."[120]

Despite avoiding the constitutional issue, the court still gave a telling mosaic theory analysis that distinguished between cameras surveilling the defendants away from their homes and cameras directed at their homes.[121]

Applying the mosaic theory to the cameras away from the defendants' homes, the court noted that "[s]uch short-term, intermittent, and non-targeted video recording of a person away from his or her own home is little different from being captured by the security cameras that proliferate in public spaces."[122] Because the cameras "did not collect aggregate data about the defendants over an extended period. . . . the cameras similarly did not allow investigators to generate a mosaic of the defendants' private lives that otherwise would have been unknowable."[123]

In contrast, the cameras directed at the defendants' homes provided surveillance that "was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life," thus constituting a search.[124] The court focused on the importance of the home, recognizing that

> even when pole cameras do not see into the home itself, by tracking who comes and goes over long periods of time, investigators are able to infer who is in the home, with whom the residents of the home meet, when, and for how long . . . .
>
> . . . . In such a society, the traditional security of the home would be of little worth, and the associational and expressive freedoms it protects would be in peril. Such invasive and arbitrary government action spurred John Adams to draft art. 14 more than two hundred years ago, and "raises the spectre of the Orwellian state" today.[125]

Even though the public can view a person's entries and exits into their home, here "the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life," resulting in a search.[126] The "combination of duration

---

[120] *Id.* at 365 (internal citations omitted).
[121] *Id.* at 369.
[122] *Id.*
[123] *Id.* at 370.
[124] *Id.* at 373.
[125] *Id.* at 371–72 (internal citations omitted).
[126] *Id.* at 373 (internal citations omitted).

and aggregation in the targeted surveillance here is what implicates a person's reasonable expectation of privacy."[127] Acknowledging that "[a] briefer period of pole camera use, or one that is not targeted at a home, might not implicate the same reasonable expectation of privacy," the court declined to provide a bright-line rule as to what length of time may be appropriate without a warrant under Article 14.[128]

In contrast, in *United States v. Trice*, the Sixth Circuit held that the government did not conduct a search when it used a surveillance camera to record the outside of an apartment door for four to six hours.[129] The court seemingly took the sequential approach when it emphasized that the defendant generally lacked a reasonable expectation of privacy in the common areas and hallway of his apartment building.[130] However, it also tacked on a mosaic theory analysis, highlighting the short time the camera was actually used and the minimal private information it provided. The court concluded that the brief duration of surveillance at issue here did not "provide an intimate window into a person's life" and was therefore not a search.[131]

E. Telephony Metadata

In *United States v. Moalin*, the Ninth Circuit concluded without ruling on the issue that the government's bulk collection of phone records from telecommunications providers (telephony metadata collection program) may have violated the Fourth Amendment.[132] The court, comparing telephony metadata to CSLI, focused on the revealing nature of telephony metadata, especially when considering the duration of the surveillance and the amount of information collected.[133] The surveillance program allowed for 24/7 surveillance over a span of several years.[134] The court observed that this exceeded what a "typical witness" would be able to learn about an individual.[135] Such surveillance "reveal[s] an entire mosaic —a vibrant

---

[127] *Id* (footnote omitted).
[128] *Id.* at 375–76.
[129] United States v. Trice, 966 F.3d 506, 510 (6th Cir. 2020).
[130] *See id.* at 513–14.
[131] *Id.* at 518–19.
[132] United States v. Moalin 973 F.3d 977, 984, 987 (9th Cir. 2020). The Ninth Circuit did not ultimately decide the issue because, even if there was a Fourth Amendment violation, "suppression would not be warranted on the facts of this case. *Id.* at 992–93 (internal citation omitted).
[133] *Id.* at 991–92.
[134] *Id.* at 991.
[135] *Id.* ("Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.") (internal quotations omitted).

and constantly updated picture of the person's life."[136] Unlike "a few days' worth of dialed numbers," society would likely "perceive as private several years' worth of telephony metadata collected on an ongoing, daily basis—as demonstrated by the public outcry following the revelation of the metadata collection program."[137]

The court also discussed the implications of the government's ability to aggregate such data across an "extremely large number of people."[138] The court reasoned that information about others' phone calls could create a more revealing mosaic of the individual at issue.[139] Quoting an amicus brief from the Brennan Center for Justice, the court noted, "it is relatively simple to superimpose our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups and quickly paint a picture that can be startlingly detailed—for example, identifying the strength of relationships and the structure of organizations."[140] For these reasons, the court concluded that "[the defendant] likely had a reasonable expectation of privacy in his telephony metadata—at the very least it is a close question."[141]

F. Aerial Surveillance

In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the Fourth Circuit rejected the Plaintiff's request for an injunction, holding that Baltimore's use of an aerial surveillance program was not a search.[142] The Aerial Investigative Research ("AIR") program was "a carefully limited program of aerial observations of public movements presented as dots," designed to aid the Baltimore Police Department.[143] The court emphasized the limitations of the program.[144] AIR could not identify an individual or specific license plate on its own; it could only track a dot linked to a crime until another surveillance method, such as surveillance cameras on the ground, tied the dot to an individual's identity.[145] The tracking could only begin when a violent crime was reported in a

---

[136] *Id.* (internal quotations omitted).
[137] *Id.* at 992.
[138] *Id.*
[139] *See id.* ("[M]etadata can be combined and analyzed to reveal far more sophisticated information than one or two individuals' phone records convey.").
[140] *Id.* (cleaned up).
[141] *Id.* at 994.
[142] Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 979 F.3d 219, 226 (4th Cir.), *reh'g granted*, 831 F. App'x 662 (4th Cir. 2020).
[143] *Id.* at 223.
[144] *Id.* 223–24.
[145] *Id.*

given area.[146] The surveillance planes only flew for twelve hours during the day.[147] The program deleted any data not related to an arrest after forty-five days.[148]

The court seemed to apply the mosaic theory, determining that the twelve hours the planes were in the air constituted permissible short-term surveillance.[149]

> [S]hort-term surveillance of an individual's public movements is less likely to violate a reasonable expectation of privacy. And under that rule, the AIR program passes muster. As Judge Bennett explained, the built-in limitations of the AIR program mean that it only enables the short-term tracking of public movements. First, the AIR program's cameras are only able to track outdoor movements. They cannot track an individual who enters a building, and analysts cannot tell if the person leaving the building is the same person who entered it. Second, AIR's surveillance planes only fly during twelve daylight hours. Because they do not fly at night, AIR surveillance cannot be used to track individuals from day-to-day.[150]

The court applied similar reasoning to differentiate the aerial surveillance at issue from the CSLI at issue in *Carpenter*. The AIR program could not "track an individual's movement from day to day," but instead could only "track someone's outdoor movements for twelve hours at most."[151] The court found that *Carpenter* only covered data collection that was "detailed, encyclopedic, and effortlessly compiled," concerns not implicated by AIR because of its limitations.[152] It also emphasized that law enforcement uses different technologies for different goals. According to the court, "CSLI is used by law enforcement to learn detailed information about someone it is already monitoring. . . . In contrast, AIR is used to identify suspects and witnesses to crimes; it takes no deep dive into an individual's life and in fact can tell the police very little about an identified person."[153]

Crucially, the court made clear that its decision was narrow, ruling on the specifics of the AIR program.[154] A more extensive aerial surveillance program, one that might implement 24- hour surveillance, could lead

---

[146] *Id.* at 224.
[147] *Id.*
[148] *Id.*
[149] *See id.* at 227.
[150] *Id.* at 227.
[151] *Id.* at 229 (internal citation omitted).
[152] *See id.* at 228 (internal quotations omitted).
[153] *Id.* at 229.
[154] *See id.*

to a different result.[155] This caveat emphasized the court's application of the mosaic theory: a potentially different outcome based on a longer data-gathering period, which creates a more complete picture of an individual's life. Relatedly, the context of this case is interesting; most post-*Carpenter* cases are criminal cases where the defendant is seeking suppression of evidence, so courts focus on the duration of the data the government requested. But here, since the plaintiffs sought a proactive injunction, the court focused its analysis on the length of surveillance over a single day instead of the breadth of the period of data the government was able to access.

In his dissent, Chief Judge Gregory also applied the mosaic theory but reached the opposite conclusion.[156] Interpreting the facts quite differently than the majority, Chief Judge Gregory characterized AIR as "long-term surveillance" that "compiles a 'detailed, encyclopedic' record of 'the whole of' every resident of Baltimore's movements in public."[157] In his mind, this made AIR comparable to the surveillance techniques at issue in *Carpenter* and *Jones*.[158] Chief Judge Gregory stressed AIR's ability to provide up to forty-five days' worth of historical location data.[159] These factors allowed law enforcement to "access [] a category of information otherwise unknowable,"[160] including the "privacies of life," that "reveal[]a person's most intimate associations and activities."[161] Even though AIR could only track outdoor movement which could be readily observed by any passerby, individuals still have a "subjective expectation of privacy in the ***whole*** of these day-to-day movements."[162]

Shedding light on his approach to the mosaic theory specifically, Chief Judge Gregory expanded on why the majority was wrong to rely on the twelve-hour limit placed on the AIR planes to determine that it didn't implicate *Carpenter*.[163] He explained that even though "the AIR program's surveillance planes will fly only during the daylight hours and capture individuals as solitary pixels does not mean that AIR program data

---

[155] *Id.*
[156] *Id.* at 234.
[157] *Id.* at 235–336 (Gregory, C.J., dissenting) (internal citations omitted).
[158] *Id.*
[159] *Id.* at 236.
[160] *Id.* (internal quotations omitted).
[161] *Id.* at 236–37 (internal citations omitted).
[162] *Id.* at 236 (emphasis in original) (internal citation omitted).
[163] *See id.* 237.

cannot be used to track specific individuals over time."[164] Law enforcement can combine the AIR data with other information to form a "comprehensive record of people's past movements."[165] In other words, the rule under *Carpenter* "is that if locational data enables police to deduce a cumulative, retrospective record of a person's physical movements, then the location information obtained was the product of a search."[166] Citing a study provided by the plaintiffs on AIR, Chief Judge Gregory stressed that by analyzing patterns in the forty-five daytimes' worth of data, the government could easily "identify the person behind the pixel based on the routines it follows."[167]

Put plainly in mosaic theory terms, data from the AIR program was a search not because "of what any single photograph may reveal. Rather, [it is because of] the planes photographing the city for twelve hours per day, seven days per week, and creating a retrospective database of everyone's movements across the city."[168] The judge further stated that "[t]he AIR program reveals intimate details about the plaintiffs' lives because it records where they go, not because any single photograph in isolation is especially revealing."[169] Like *Carpenter*, Chief Judge Gregory did not put a lower temporal limit on when aerial surveillance programs would not constitute a search. Thus, his dissent could be interpreted as using the sequential approach to consider all AIR-type programs as searches regardless of the various time limits and durations involved. But this is unlikely. He specifically differentiated general aerial surveillance from AIR and stressed his concern regarding the government's ability to aggregate information obtained by AIR, implicitly invoking the mosaic theory.[170]

---

[164] *Id.* at 238–39 (footnote omitted).
[165] *Id.* at 237–38.
[166] *Id.* at 238 (cleaned up).
[167] *Id.*
[168] *Id.* at 241.
[169] *Id.* at 242.
[170] *Id.* at 238. *See* Phillip Jackson, *Baltimore aerial surveillance program designed to decrease crime ends Saturday. Its future uncertain.*, BALT. SUN (Oct. 30, 2020, 5:24 PM), https://www.baltimoresun.com/news/crime/bs-md-ci-cr-crime-pilot-program-ending-20201030-25pjs53rpbhzpfdvm2r5syvkjq-story.html (stating that the AIR program went on hiatus in early November 2020 and "[a] police spokeswoman did not respond to questions about future plans and how many crimes the air unit may have helped solve."); *see also* Nathaniel Sobel, *EFF Urges Federal Appeals Court to Rehear Case Involving Unconstitutional Baltimore Aerial Surveillance Program*, ELEC. FRONTIER FOUND. (Nov. 30, 2020), https://www.eff.org/deeplinks/2020/11/eff-urges-federal-appeals-court-rehear-case-involving-unconstitutional-baltimore (announcing submission of

II. CASES WHERE COURTS DECLINED TO APPLY THE MOSAIC THEORY

Not all courts have embraced the mosaic theory in light of *Carpenter*. Many continue to apply the sequential approach to technology-based investigatory techniques that ***could*** have implicated the mosaic theory. As the sequential approach is a less fact-specific inquiry in each individual case, I treat the following cases differently than the mosaic theory cases. Instead of offering a case-by-case description, I summarize the courts' conclusions for each investigatory technique and focus on the courts' reasoning in deciding not to apply the mosaic theory.

A. Cell Site Location Information

When courts have considered CSLI and declined to apply the mosaic theory, they have predominantly found that the use of any kind of CSLI constituted a search.[171] In *State v. Muhammad*, the Supreme Court of Washington explicitly rejected the mosaic theory, largely on administrability grounds.[172] In rejecting the government's argument that a single cell phone ping was not a search under *Carpenter*, the court noted:

> First, the argument that an isolated cell phone ping offers limited information and therefore does not implicate the Fourth Amendment appears to advance what federal courts have deemed the "mosaic" theory. . . .
>
> At first glance, the mosaic theory presents an attractive answer to whether a singular cell phone ping constitutes a Fourth Amendment search. But federal courts have recognized the practical problems inherent in this theory when traditional surveillance becomes a search only after some specific period of time elapses. . . . There is no rational point to draw the line; it is arbitrary and unrelated to a reasonable expectation of privacy.
>
> Rather than offering analysis based on a reasonable expectation of privacy, the mosaic theory instead requires a case-by-case, ad hoc determination of whether the length of time of a cell phone ping violated the Fourth Amendment. It offers little guidance to courts or law enforcement and presents the danger that constitutional rights will be arbitrarily and inequitably enforced. [I]f police are to have workable rules, the balancing of the competing interests . . . must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.[173]

---

an amicus brief, joined by other prominent civil rights and privacy rights groups, supporting the plaintiffs' request for a rehearing *en banc*).

[171] *See* Appendix A for a list of relevant cases.

[172] *See* State v. Muhammad, 194 Wash. 2d 577, 593–94 (2019).

[173] *Id.* (internal citations omitted).

Other courts that used the sequential approach for CSLI did not explicitly attack the mosaic theory, but simply focused on the rationale behind *Carpenter.* Courts determined that the length of the surveillance in question or the difference between historical and real-time data was largely irrelevant.[174] For example, in *People v. Simpson*, the Supreme Court of New York, Queens County largely ignored the discussion of the time span of the historical CSLI at issue in *Carpenter* and "f[ou]nd that the express holding of the *Carpenter* court was ***t****hat an individual maintains a legitimate expectation of privacy in his physical movements as captured through the CSLI*."[175] *State v. Snowden* applied similar reasoning. In *Snowden,* the Court of Appeals of Ohio, Second District, Montgomery County interpreted *Carpenter* as standing for the proposition that "[b]efore compelling a wireless carrier to turn over a subscriber's CSLI, the State's obligation is a familiar one – obtain a warrant. This is logically true whether it is one day, two days, three days, or seven days or more of data obtained."[176] The court went on to pithily lay out the difference between the mosaic theory and the sequential approach, explaining, "[w]e should not be preoccupied with what the State learned, but rather the manner in which the government obtained information."[177]

Unlike the other courts that treated historical and real-time CSLI the same, in *Commonwealth v. Almonor*, the Massachusetts Supreme Court, which adopted the mosaic theory for historical CSLI, distinguished it from real-time CSLI.[178] In doing so, the court rejected the government's mosaic theory argument that "the single ping of the defendant's cell phone was too brief to implicate a person's reasonable privacy interest and thus does not constitute a search in the constitutional sense."[179] In describing its reason for differentiating historical and real-time CSLI, the court stated:

> As we stated in *Estabrook*, albeit without elaboration, the six-hour rule applies only to historical "telephone call" CSLI. Historical "telephone call" CSLI is collected and stored by the service provider in the ordinary course of business when the cell phone user voluntarily makes or receives a telephone call. In this context, the

---

[174] As discussed *infra* p. 97, the Massachusetts Supreme Judicial Court represents a significant deviation from the pattern of finding no difference between real-time and historical CSLI.

[175] People v. Simpson, 62 Misc. 3d 374, 380 (N.Y. Sup. Ct. 2018).

[176] State v. Snowden, 140 N.E.3d 1112, 1126 (Ohio Ct. App. 2019).

[177] *Id.* at 1126–27.

[178] Commonwealth v. Almonor, 482 Mass. 35, 36–37 (2019). While the case was decided under Article 14 of the Massachusetts Declaration of Rights, the reasoning is relevant.

[179] *Id*. at 48 (internal quotations omitted).

> six-hour rule is consistent with reasonable societal expectations of privacy. In contrast, there is nothing voluntary or expected about police pinging a cell phone, and the six-hour rule therefore does not apply.[180]

In the court's view, the government's use and acquisition of short-term historical CSLI did not violate any societal expectations of privacy, whereas a single real-time ping crossed the line as a more affirmative step taken by the government to track live movement.[181]

B. GPS Tracking of Vehicles:

In *United States v. Howard*, the District Court for the Middle District of Alabama, Southern Division, took a similar approach to that of the court in *Muhammad* and explicitly declined to apply the mosaic theory, finding that real-time GPS tracking of a borrowed truck was not a search.[182] The court began its analysis by explaining the general confusion present in the case law for Fourth Amendment searches.[183] It noted that the purported solution to the confusion, the mosaic theory, "has puzzled a Supreme Court justice, several circuit judges, three district courts, two state supreme courts, and one of the nation's leading Fourth Amendment scholars."[184] The court made clear that it did not base its decision on the mosaic theory but instead "grounded [it] in the fundamentals of the relevant facts and applicable law."[185]

The court reached its conclusion based on four grounds, three of which clearly applied the sequential approach while one seemed suspiciously similar to the mosaic theory.[186] The court explained there was no *Jones*-type trespass as the borrowed truck's owner permitted the installation of the GPS device.[187] It next distinguished the truck's GPS tracking device from the CSLI in *Carpenter* by noting that the retrospective quality of CSLI was the primary issue, as it differed from "traditional, visual surveillance."[188] Accordingly, the court noted "[b]oth today and at the founding, police could track an identified suspect in real time. They could even

---

[180] *Id.* at 49 (citations omitted).
[181] *See id.*
[182] *See* United States v. Howard, 426 F. Supp. 3d 1247, 1254–56 (M.D. Ala. 2019).
[183] *Id.* at 1252–56.
[184] *Id.* at 1255–56 (footnotes omitted). Unsurprisingly, the leading Fourth Amendment scholar is none other than Professor Kerr.
[185] *Id.* at 1256.
[186] *See id* at 1256–58.
[187] *See id.* at 1256–57.
[188] *Id.* at 1257.

do so without keeping constant eyes on their suspect."[189] Relatedly, the court explained that CSLI tracks individuals anywhere they go with their phone while a vehicle's GPS only tracks individuals when they are driving.[190] Finally, the court cited *stare decisis*, noting *United States v. Knotts*[191] controlled because it "is more factually analogous than *Carpenter*."[192]

Confusingly, the court emphasized that "the surveillance was not for an 'extended period of time.' [The defendant] was monitored during a discreet trip over a twenty-two-hour period with a two-way distance of approximately two-hundred miles."[193] By including this in the analysis, the court begged the question of whether a more extensive surveillance would have turned the use of GPS into a search. If that was the case, it means the court applied the mosaic theory it claimed not to use.[194] Of course, it is possible that the court merely included information about the extent of the surveillance to support its decision based on other grounds and, taking the court at its word, would have applied an identical analysis for surveillance covering any period of time and distance.

Similarly, in *Bailey v. State*, the District Court of Appeals of Florida for the First District held that the government's use of GPS records held by a financing company to track a car was not a search.[195] Per an agreement between the car owner (not the defendant) and the financing company, the car had been equipped with a GPS tracker.[196] The court concluded that *Carpenter* did not apply because of the difference between CSLI and GPS and that *Jones* did not apply because the facts did not involve trespass.[197] Therefore, the court declined to apply the mosaic theory and relied on *Knotts* to find that the defendant had no expectation of privacy in historical GPS records of the car's movements.[198] Nonetheless,

---

[189] *Id.*
[190] *Id.*
[191] United States v. Knotts, 460 U.S. 276, 285 (1983) (finding that the use of a radio transmitter to follow an automobile on public roads was not a search).
[192] United States v. Howard, 426 F. Supp. 3d 1247, 1258 (M.D. Ala. 2019).
[193] *Id.* at 1257.
[194] Professor Matthew Tokson characterizes the court's approach to the mosaic theory as "criticiz[ing] it before applying it." Matthew Tokson, *The "Mosaic Theory" and the Aftermath of Carpenter*, DORF ON LAW (Aug. 03, 2020, 7:30 AM), http://www.dorfonlaw.org/2020/08/the-mosaic-theory-and-aftermath-of.html.
[195] Bailey v. State, No. 1D18-4514, 2020 WL 6706904, at *8 (Fla. Dist. Ct. App. Nov. 16, 2020).
[196] *Id.* at *1.
[197] *Id.* at *5–6.
[198] *Id.* at *7.

the court discussed the mosaic theory at length.

The court began its analysis by looking at *Carpenter*.[199] It emphasized the Supreme Court's focus on the pervasiveness of cell phones and the ability to use historic CSLI to track "the whole of [the defendant's] physical movements."[200] It also underscored the narrow nature of *Carpenter*'*s* holding.[201] Interestingly, in a footnote with no explanation, the court explicitly stated that "*Carpenter* does not address the 'mosaic' theory."[202] The court then addressed *Jones*.[203] While the court ultimately relied on the trespass test in its analysis, it acknowledged the use of the mosaic theory in the lower court opinion and in the two *Jones* concurrences.[204] It described the mosaic theory a few different ways:

> The mosaic theory applies a cumulative understanding of data collection by police and analyzes searches as a collective sequence of steps rather than individual ones. It considers police action to be viewed over time as a collective "mosaic" of surveillance and allows the whole picture to qualify as a protected Fourth Amendment search, even if the individual steps that contribute to the full picture do not, in isolation, reach that constitutional threshold.[205]
>
> Under [the mosaic] approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer-term GPS monitoring in the investigations of most offenses impinges on expectations of privacy.[206]

In a footnote, the court noted that the mosaic theory "contemplates whether the constitutionality of a search may now be based on duration of data acquisition."[207] Based on the court's understanding of the mosaic theory, its statement that *Carpenter* did not adopt the mosaic theory would suggest that the court believed the government's use of historic CSLI is ***always*** a search. The court admitted that *Carpenter* left open the question of short-term CSLI, but if the court believed the outcome would be different depending on the ***duration*** of the CSLI accessed, the Supreme Court

---

[199] *Id.* at *5.
[200] *Id.* (alterations in *Bailey*).
[201] *Id.*
[202] *Id.* at *5 n.6.
[203] *Id.* at *5.
[204] *Id. at* *5–6 ("Likewise, *Jones* does not mandate a conclusion in this case that acquisition of the GPS monitoring constitutes a search. The Supreme Court expressly limited the holding of *Jones* which found only that the installation of the GPS device on the defendant's car constituted a trespass, and therefore, was a search.").
[205] *Id.* at *5.
[206] *Id.*
[207] *Id.* at *5 n.7.

would have been applying the mosaic theory based on the court's own definition.[208] In another footnote, the court quoted the Florida Supreme Court, noting the problems with the mosaic theory.[209] Although the court never explicitly stated this, its hesitancy to apply the mosaic theory suggests that it questioned the value of the doctrine.

In a concurring opinion, Judge Osterhaus suggested that the reasoning in *Carpenter* and the *Jones* concurrences should control, so he would have decided the case under the good-faith exception.[210] Still, he didn't differentiate the duration of the GPS used in the present case from the duration of the data used in *Carpenter* and *Jones*.[211] Thus, it is not clear if he believed the court should have applied the mosaic theory or that the court should always consider the government's use of GPS a search.[212]

C. Pole Cameras

Courts that declined to apply the mosaic theory found that the government's use of pole cameras or similar video surveillance was not a search.[213] *United States v. Moore-Bush* revealed the court's struggles with the mosaic theory. In *Moore-Bush*, the First Circuit reversed the district court, which had found that a search occurred by applying the mosaic theory to footage from pole cameras.[214] The district court began its analysis by determining that in light of *Carpenter*, the holding in *United States v. Bucci*[215] no longer controlled the use of pole cameras. Free of *Bucci*, the court then reasoned that eight months of pole camera surveillance was a

[208] *See id.* at *6 ("Although the Court in *Carpenter* forbid the government from warrantlessly accessing seven days of historical CSLI from a target's wireless carriers, it refused to address whether one's 'reasonable expectation of privacy in the whole of his physical movements' extends to shorter periods of time or to other location tracking devices.).

[209] *Id.* at *5 n.8 ("[T]he mosaic theory has presented problems in practice . . . where traditional surveillance becomes a search only after some specified period of time.") (internal quotations omitted).

[210] *Id.* at *8 (Osterhaus, J., concurring).

[211] *See id.* at *9.

[212] *See id.* at *8–9 ("I cannot see affirming this case under *Knotts*, or with a holding that drivers lack a reasonable expectation of privacy in the GPS records of their vehicle's movements.").

[213] *See* Appendix B for a list of relevant cases.

[214] United States v. Moore-Bush, 963 F.3d 29, 31 (1st Cir. 2020). Since submitting this Note for publication, the First Circuit granted a rehearing en banc granted. United States v. Moore-Bush, 982 F.3d 50 (1st Cir. 2020). The government filed a brief arguing that *Carpenter* didn't adopt the mosaic theory. UNITED STATES OF AMERICA, Appellant, v. Nia MOORE-BUSH, a/k/a Nia Dinzey, Defendant-Appellee. United States of America, Appellant, v. Daphne Moore, Defendant-Appellee., 2021 WL 961022 (C.A.1), *4–6.

[215] United States v. Bucci, 582 F.3d 108, 116–18 (1st Cir. 2009) (finding video surveillance of the front of a home was not a search).

search because

> [i]n the Court's view, three principles from the *Jones* concurrences and *Carpenter* dictate the resolution of this motion. First, as Justice Sotomayor points out in *Jones*, "[a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." Second, as Chief Justice Roberts observes in *Carpenter*, technologies that permit law enforcement officers to access and search vast amounts of passively collected data may "give police access to a category of information otherwise unknowable." Third, as Justice Alito reasons in *Jones*, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[216]

However, the First Circuit disagreed, finding that *Bucci* still applied.[217] It emphasized that *Carpenter* was a narrow decision and "[t]he limitations expressed in the *Carpenter* analyses are not mere dicta," and even if they were dicta, they would still carry considerable force.[218]

The First Circuit considered pole cameras to be "conventional surveillance techniques," that fell outside of *Carpenter*'s scope.[219] Therefore, the principle of *stare decisis* required a reversal because *Bucci* and its precedent was clear on the issue.[220] The court in *Bucci* applied the sequential approach, finding that eight months of pole camera surveillance in front of the defendant's house was not a search.[221] The defendant lacked a reasonable expectation of privacy in the front of his house because it was exposed to the public.[222]

This focus on public exposure was present in all the cases that declined to apply the mosaic theory. For instance, in *United States v. Kubiasiak*, the District Court for the Eastern District of Wisconsin declined to

---

[216] United States v. Moore-Bush, 381 F. Supp. 3d 139, 147–48 (D. Mass. 2019), *as amended* (June 4, 2019), *rev'd and remanded*, 963 F.3d 29 (1st Cir. 2020) (internal citations omitted).

[217] *Moore-Bush*, 963 F.3d at 32.

[218] *Id.* at 39–40.

[219] *Id.* at 40 ("*Carpenter's* limitations unquestionably apply here. Pole cameras are conventional, not new, technology. They are the exact kind of "conventional surveillance technique[ ]" the Court carefully said it was not calling into question.") (footnote and internal citations omitted).

[220] *Id.* at 42.

[221] United States v. Bucci, 582 F.3d 108, 116–17 (1st Cir. 2009).

[222] *Id.*

apply the mosaic theory to a camera set up on a neighbor's property.[223] "The camera . . . was in a fixed location, and recorded only what the neighbor, or a police officer standing in the neighbor's house, could have seen. The surveillance did not present the kind of aggregate view of intimate details of the defendant's every movement that concerned the concurrence in *Jones*, or the majority in *Carpenter*."[224] The magistrate judge explicitly rejected the mosaic theory in *Kubiasiak*, noting "[p]erhaps in the future, the court of appeals or the Supreme Court will give guidance on what role an aggregate record of activities exposed to the public captured by video surveillance plays in the expectation of privacy analysis. Today, however, no such guidance or authority exists to support [the defendant's] mosaic or aggregate theory."[225] Similarly, in *United States v. Tirado*, the United States District Court for the Eastern District of Wisconsin found *Carpenter* and the mosaic theory did not apply to pole camera surveillance because it was a conventional surveillance technique that captures "only matters exposed to the public," and doesn't "provide[] the same aggregate account of a person's life, revealing his 'political, professional, religious, and sexual associations.'"[226]

III. TAKEAWAYS

I begin this Part by exploring technology-specific takeaways. I do not address aerial surveillance or telephony metadata in this section because there is only one case for each investigative technique, so drawing conclusions related to these technologies would be premature. However, I incorporate these technologies in my subsequent discussion of generally applicable mosaic theory takeaways. There, I look at the broader issues these cases invoke and reflect on the meaning of the lower courts' treatment of the mosaic theory since *Carpenter*.

A. Cell Site Location Information

The two main questions that courts ask when deciding CSLI cases after *Carpenter* are: did the Supreme Court adopt the mosaic theory? If so, what length of time can the government use CSLI before it constitutes

---

[223] United States v. Kubasiak, No. 18-CR-120-PP, 2018 WL 4846761, at *7 (E.D. Wis. Oct. 5, 2018).
[224] *Id.*
[225] United States v. Kubasiak, No. 18-CR-120, 2018 WL 6164346, at *3 (E.D. Wis. Aug. 23, 2018).
[226] United States v. Tirado, No. 16-CR-168, 2018 WL 3995901, at *2 n.2 (E.D. Wis. Aug. 21, 2018) (internal citations omitted).

a search? Many courts have omitted duration analysis and focused entirely on the inherently revealing nature of CSLI itself. In doing so, those courts have afforded CSLI a high degree of protection, much higher than the protection offered by *Carpenter*. Relatedly, it is difficult to square the non-mosaic approach to CSLI with the plain language of *Carpenter*, which made clear that it was a narrow decision that did not touch upon real-time or short-term CSLI. The courts that rejected the mosaic theory assume, based on the Supreme Court's general approach to CSLI, that the Court's concern over seven days of historical CSLI extends to any amount of CSLI and the mention of duration was merely incidental to the facts of *Carpenter*.

The courts that closely followed *Carpenter* by differentiating between long and short-term CSLI and applying the mosaic theory, confronted a line drawing problem. For example, one court[227] found that five days of CSLI was close enough to the seven days that *Carpenter* established as a search, but another court[228] found that two days did not sufficiently establish a search. A bit of an outlier, the Massachusetts Supreme Judicial Court drew the line at six hours for historical CSLI.[229] Generally, courts do not appear to draw a major distinction between historical and real-time CSLI. But since the real-time CSLI cases only use hours of data, no court has considered it a search under the mosaic theory.[230] It is also unlikely that a court could find that any singular tower dump would trigger a search under the mosaic theory. A tower dump provides significantly less information about an individual than two days of historical CSLI or a few hours of real-time CSLI, neither of which were found to constitute a search.[231] Hypothetically, the use of multiple tower dumps to track an individual phone number over a significant period of time could rise to the level of a search for some courts. However, this fact pattern is unlikely because the government typically has other means of tracking a specific number.

Although the Supreme Court decided *Carpenter* itself on facts involving CSLI, courts using the mosaic theory grant less protection for data

---

[227] State v. Gibbs, No. 2017-001846, 2020 WL 4814266 at *1, *4 (S.C. Ct. App. Aug. 19, 2020).
[228] People v. Edwards, 63 Misc. 3d 827, 828, 831 (N.Y. Sup. Ct. 2019).
[229] Commonwealth v. Wilkerson, 156 N.E.3d 754, 766 (2020).
[230] People v. Tham Bui, No. H044430, 2019 WL 1325260 at *21 (Cal. Ct. App. Mar. 25, 2019); Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App. 2019).
[231] *See* United States v. Walker, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *1, *5 (E.D.N.C. July 20, 2020).

acquired by this technology than courts that do not adopt the mosaic theory. *Carpenter* made clear the dangers related to law enforcement's use of CSLI, but the mosaic theory offers the government an out depending on the specific amount of CSLI it has accessed. Under the sequential approach, the government must always obtain a warrant for any amount of CSLI. By contrast, jurisdictions that use the mosaic theory allow the government to acquire short-term CSLI without a warrant.

B. GPS Tracking of Vehicles

The two main questions that courts ask when deciding if GPS location data constitutes a search are: Do *Carpenter* and the mosaic theory cover GPS? If they do, how long can the government track a car before it constitutes a search? As to the first question, courts are split. Two cases discussed here explicitly applied *Carpenter* and performed a mosaic theory analysis.[232] The courts in the other two cases explicitly held that *Carpenter* and the mosaic theory did not apply. [233] One stated outright that neither *Carpenter* nor the holding in *Jones* adopted the mosaic theory.[234]

It is not clear how a court that does not apply the mosaic theory would analyze a long-term GPS tracking case that does not involve government trespass. On one hand, it does not seem likely that a court could treat GPS like CSLI because it would render the trespass test entirely irrelevant. On the other, it is strange to suggest that no length of GPS tracking could ever constitute a search, since multiple years of GPS tracking data would be at least as revealing as the seven days of CSLI in *Carpenter*. Although the court in *Howard* did factor in the short-term nature of the government's use of GPS, this was not dispositive since the court claimed to apply the sequential approach, which does not consider duration.[235] *Howard* does provide one way to meaningfully differentiate GPS trackers attached to vehicles from CSLI: cell-phones track an individual's every move, whereas cars only follow an individual's movements when driving.[236] The court in *Bailey* seemed to have no issue with long-term GPS monitoring at all. Perhaps there is no wrinkle and courts are comfortable with limitless GPS tracking on a vehicle if there is no government trespass.

---

[232] United States v. Diggs, 385 F. Supp. 3d 648, 651 (N.D. Ill. 2019); Kinslow v. State, 129 N.E.3d 810, *1–2 (Ind. Ct. App. 2019).
[233] United States v. Howard, 426 F. Supp. 3d 1247, 1254–56 (M.D. Ala. 2019); Bailey v. State, No. 1D18-4514, 2020 WL 6706904, at *2 (Fla. Dist. Ct. App. Nov. 16, 2020).
[234] *Bailey*, No. 1D18-4514, 2020 WL 6706904, at *5 n.6.
[235] See *Howard*, 426 F. Supp. 3d at 1256–57.
[236] *Id.* at 1257.

In that case, unlike CSLI, the mosaic theory offers individuals more protection for GPS location data that the government did not acquire via trespass than the sequential approach does.

As to the line drawing problem, the lack of cases makes it difficult to reach any conclusions. Unsurprisingly, at least in comparison to the duration of CSLI that constitutes a search, one court that applied the mosaic theory found that the use of historical, long-term (one month) GPS is a search. It is unsurprising (except for perhaps in Massachusetts) that another court found that the use of six hours of real-time GPS data was not a search. Presumably, courts would need to draw similar lines for GPS tracking, as they have begun to draw for CSLI.

C. Automatic License Plate Readers

While the number of ALPR cases is limited, the main question that courts grapple with is how to apply the mosaic theory to ALPRs. Thus far, accessing ALPR databases does not meet the threshold of a search. Courts are of the opinion that ALPR databases do not provide as revealing a picture as CSLI did in *Carpenter*, although courts seem to agree that they one day could. This demonstrates the importance of fully developing the record as to how many cameras feed into the database system and how many hits exist for the license plate in question. After GPS, this technology has the potential to provide the most similar kind of tracking to the CSLI discussed in *Carpenter*. However, a court's willingness to find it a search depends on the density of the ALPRs in a given area and how the ALPR database is set up. If courts applied the sequential approach to cases involving ALPRs, they probably would not consider their usage a search. But if ALPRs continue to proliferate, there is no reason that courts should treat the technology differently than CSLI.

D. Pole Cameras

The use of pole cameras and video surveillance directed at homes presents similar questions to the use of GPS: Do *Carpenter* and the mosaic theory apply? If they do, what amount of surveillance constitutes a search? Courts are split on the first question. The majority of courts have leaned towards not applying the mosaic theory because the cameras only capture information available to the public and that information does not reveal the same private details as CSLI. The First Circuit in *Moore-Bush* clarified that *Carpenter* did not apply to pole cameras because they are a conventional surveillance technique.[237] All of the courts that did not apply

[237] United States v. Moore-Bush, 963 F.3d 29, 40 (1st Cir. 2020).

the mosaic theory found that the government's use of pole cameras was not a search.

Other than the district court finding that was overruled by the First Circuit, only two other courts applied the mosaic theory to decide whether the use of pole cameras constituted a search. The low number of cases makes it difficult to determine the line for an acceptable collection period of footage from the cameras. In *Tafoya*, the court found that three months-worth of footage from pole cameras was a search, while the Sixth Circuit in *Trice* found that the four to six hours of footage from a surveillance camera outside of an apartment door was not a search.[238] Although I categorize *Trice* as a mosaic theory case based on the duration factors the court considered in its reasoning, I hesitate to suggest that it clearly split with the First Circuit. For one, pole cameras are not identical to the surveillance camera used in *Trice*, though the two are similar. Second, the Sixth Circuit did not find the duration of the surveillance to be dispositive.[239] It spent the majority of the opinion explaining why the defendant generally lacked a reasonable expectation of privacy in the common areas and hallway of his apartment building.[240] Still, the Sixth Circuit discussed duration and used language from *Carpenter* and *Jones* in that discussion, which differed from the First Circuit's approach.[241]

As with GPS, applying the mosaic theory to pole cameras and video surveillance provides more Fourth Amendment protection than does applying the sequential approach. All of the courts that applied the sequential approach to pole cameras concluded that their use was never a search, regardless of duration. The mosaic theory provides courts a way, given a long enough period of surveillance, to find that the use of pole cameras constitutes a search.

E. Big Picture

The mosaic theory is messy. Based on how the lower courts have handled it so far, there are two general questions: Should the mosaic theory apply? If so, how should it be applied? Embedded in the first question are two sub-questions: Did *Carpenter* adopt the mosaic theory? If so, which investigative techniques does *Carpenter* cover?

Addressing the first sub-question, courts are split. Courts that did not apply the mosaic theory to CSLI suggested that the Supreme Court did

---

[238] People v. Tafoya, 2019 COA 176, *1, *cert. granted*, No. 20SC9, 2020 WL 4343762 (Colo. June 27, 2020); United States v. Trice, 966 F.3d 506, 510 (6th Cir. 2020).
[239] Trice, 966 F.3d at 513–14.
[240] *See id.*
[241] *See id.* at 518–19.

not adopt the mosaic theory. In *Bailey*, the court explicitly said as much.[242] In those jurisdictions, it is unlikely that advocates could successfully make mosaic theory arguments for any investigative technique. As mentioned above, that cuts both ways in terms of Fourth Amendment protection. With CSLI, the mosaic theory offers less Fourth Amendment protection than the sequential approach. For technology like GPS and pole cameras, the mosaic theory offers greater protection.

Moving on to the second sub-question: courts that believe *Carpenter* adopted the mosaic theory must determine which technologies it covers. CSLI is obviously covered as it was the focus of *Carpenter*. Courts that applied the mosaic theory to other technologies focused on what the information could reveal about an individual, given enough of it. Courts that did not apply the mosaic theory to those same investigative techniques rationalized their approach in two related ways. First, courts disagreed with the premise that the particular technique in question could reveal sensitive information in which individuals have a legitimate privacy interest, such as entry and exit to their home. Second, courts pointed to the narrow language in *Carpenter* and put investigative techniques other than CSLI under the "conventional surveillance technique" umbrella, which the plain language of *Carpenter* excludes.

Courts most strongly diverged on the issue of whether the mosaic theory applies to pole cameras. Some courts embraced the mosaic theory wholeheartedly while others stated that pole cameras are specifically excluded from *Carpenter*.[243] Beyond using the narrow nature of *Carpenter*, many courts have also focused on an underlying tension within the mosaic theory to avoid applying it to technology such as pole cameras: If there is no reasonable expectation of privacy in any given individual data point, how can the aggregate of such data points create that expectation?[244]

There is just as much of a mess, if not more, when looking at the second question: how to actually apply the mosaic theory. Once a court decides that *Carpenter* and the mosaic theory apply to a given investigational technique, it is faced with several issues. The most obvious is determining where it should draw the line as to when an investigative technique becomes a search. Even for CSLI, presumably the most straightforward surveillance technique to analyze given that it was the

---

[242] Bailey v. State, No. 1D18-4514, 2020 WL 6706904, at *5 n.6 (Fla. Dist. Ct. App. Nov. 16, 2020).

[243] *Compare Tafoya*, 2019 COA 176, at *1; Commonwealth v. Mora, 485 Mass. 360, 361 (2020) *with* United States v. Moore-Bush, 963 F.3d 29, 40 (1st Cir. 2020).

[244] This can be thought of as the "mathematical problem." Gray & Citron, *supra* note 3, at 398–99 ("[t]he sum of an infinite number of zero-value parts is also zero").

very subject of *Carpenter*, courts are all over the place. Extrapolating from *Carpenter*'s seven-day threshold, courts have tried to draw meaningful lines at five days of data, two days of data, tower dump data, and real-time tracking. Whether those lines are actually meaningful is not obvious. For the clearest example of this confusion, one court[245] was confident that the use of two days of CSLI was clearly not a search under *Carpenter,* while another court[246] found that anything more than six hours was a search under *Carpenter*. In jurisdictions that have not yet heard a post-*Carpenter* CSLI case, this leaves judges, lawyers, and law enforcement to guess when accessing CSLI would constitute a search.[247] The mess only grows when looking at surveillance techniques other than CSLI.

When courts decide to apply the mosaic theory in non-CSLI cases, the line drawing problem compounds. How are courts supposed to compare the number of hits in an ALPR database to the duration of accessed CSLI? So far, courts have largely tried to draw the line based on how much the data revealed about an individual's personal life and "whether the government learned more than a stranger could have observed."[248] Though the verbiage varies, courts discuss terms such as the "privacies of life," "intimate details," "intimate window," and "intimate associations and activities."[249] Courts have also framed the issue as whether the information would be otherwise unknowable apart from the mosaic assembled

---

[245] People v. Edwards, 63 Misc. 3d 827, 831–32 (N.Y. Sup. Ct. 2019).

[246] Commonwealth v. Wilkerson, 156 N.E.3d 754, 766 (2020).

[247] This result was predictable. As Professor Kerr stated quite frankly in discussing when accessing historical CSLI may or may not be a search, "[w]e don't know." Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision; *see also* Kerr, *supra* note 5, at 39 ("The police need to know the rules to follow them, and they can't know them and can't follow them under the mosaic approach.").

[248] *See* Kerr, *supra* note 7, at 330 (describing the different flavors of the mosaic theory). *See, e.g.*, United States v. Walker, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *1, *5 (E.D.N.C. July 20, 2020) (considering whether the government action "chronicl[ed] that individual's private life for days); Kinslow v. State, 129 N.E.3d 810, at *9 n.6 (Ind. Ct. App. 2019) (concluding use of GPS "d[id] not provide an intimate window into a person's life); Commonwealth v. McCarthy, 484 N.E.3d 493, 509 (Mass. 2020) (concluding ALPR data did not reveal "the privacies of [the defendant's] life"); *Mora*, 485 Mass. at 373 (concluding home pole camera surveillance "was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life); *Edwards*, 63 Misc. 3d at 832 ("Anyone who was passing through that lobby or walking on the street nearby on that early November evening could have seen the very same thing."); People v. Tham Bui, No. H044430, 2019 WL 1325260 at *21 (Cal. Ct. App. Mar. 25, 2019) (concluding defendant "had no reasonable expectation of privacy in his real time location or movements in a vehicle on public streets").

[249] *See, e.g.*, *Walker*, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *1, 5; *Kinslow*, 129

by the government.[250] Some courts have also used a probabilistic analysis, asking whether the government could learn more than an average individual might expect.[251] While the exact approach deviates and results in varying outcomes, the general approach is largely consistent.

Still, it is not clear where a court should draw those lines. In anticipating the confusion, Paul Rosenzweig bluntly explained, "the Supreme Court's decision in *Carpenter v. United States* is not law. Anyone who says they can read the majority opinion and predict with any degree of confidence how the Court will deal with any number of future technologies—be they biometrics, facial recognition, DNA or real-time cell-site location information (CSLI)—is, frankly, just making it up."[252] This uncertainty will inevitably need to work its way through the appellate system and, indeed, the process has already begun.[253]

The mess gets messier when it isn't even clear what the "how much is too much" measures. For most of the investigative techniques, it is a pretty straightforward question of duration, e.g., a certain number of hours or days for CSLI, GPS, and pole cameras. Technology like ALPRs makes the analysis trickier because the question not only involves duration, but also the number of hits received or the overall number of ALPRs in a given area. The most complicated example of applying this second question comes from the AIR program in Baltimore, where two time periods were at issue.[254] The majority focused on the amount of hours per day that the AIR planes gathered data, while the dissent found it relevant that law enforcement could access up to forty-five days' worth of that data.[255] The complication is at least partially explained by the nature of

---

N.E.3d at *9 n.6; *McCarthy*, 484 Mass. at 509*; Mora*, 485 Mass. at 373; *Edwards*, 63 Misc. 3d at 832; *Tham Bui*, No. H044430, 2019 WL 1325260, at *21.

[250] *See, e.g.*, United States v. Diggs, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019); *Mora*, 485 Mass. at 373; United States v. Moore-Bush, 381 F. Supp. 3d 139, 147–48 (D. Mass. 2019).

[251] *See, e.g.*, United States v. Moalin 973 F.3d 977, 992 (9th Cir. 2020).

[252] Paul Rosenzweig, *Carpenter v. United States and the Law of the Chancellor's Foot*, Lawfare (June 27, 2018, 7:41 AM), https://www.lawfareblog.com/carpenter-v-united-states-and-law-chancellors-foot.

[253] *See*, *e.g.*, Commonwealth v. Pacheco, 237 A.3d 396, 397 (Pa. 2020) (granting an appeal to address how *Carpenter* applies to 108 days of real time CSLI).

[254] Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 979 F.3d 219, 224 (4th Cir. 2020).

[255] *Id.* at 229 ("Whereas CSLI could be used to reliably track an individual's movement from day to day, AIR can only be used to track someone's outdoor movements for twelve hours at most."); *id.* at 239 ("The police would have access to 45 daytimes' worth of retroactive locational data to follow any given 'pixel' as it moved through time and space. By analyzing patterns, it is possible—and often relatively easy—to identify the person behind the pixel based on the routines it follows.") (Gregory, C.J., dissenting).

the case. It was civil rather than criminal, and the plaintiffs challenged the program as a whole, as opposed to the government's access of specific data over a specific time period.[256] That case also addressed whether aggregating information across different investigational techniques should be factored into the "how much is too much" analysis.[257] The majority ultimately concluded that *Carpenter* prohibited the cross-technique approach when traditional surveillance techniques were used, but the dissent vehemently disagreed.[258]

Another question that courts have left open is whether it matters what actions law enforcement takes to gather the data. For most of these technologies, law enforcement simply accesses a database, e.g., CSLI, ALPRs, and sometimes GPS. Other times, law enforcement collects the data itself using methods like pole cameras and "pinging" phones or using cell-site simulators, AIR, and GPS the government placed. This has not yet been a major issue, but a couple courts have suggested that more affirmative acts by law enforcement deserve increased scrutiny.[259]

Another complicating factor with the mosaic theory is that it is often impossible to determine whether a government action is a search until after it has already taken place. Much of the courts' analyses focus on what the government learned, not what the government did. The clearest example is in the ALPR context.[260] The database may have no photos of a given license plate, it may have just a few, or it could potentially have hundreds.[261] Law enforcement cannot know whether there are enough

---

[256] *Id.* at 222.

[257] *Id.* at 227 ("In response, plaintiffs object that the police may be able to use preexisting surveillance tools, like security cameras and license plate readers, in conjunction with AIR photographs to track individuals from day to day. But plaintiffs do not challenge these existing tools—only the AIR program in particular. And for good reason. The Supreme Court specifically stated that traditional surveillance tools, specifically security cameras, remain lawful in light of *Carpenter*, 138 S. Ct. at 2220, and we are not at liberty to revisit that conclusion."); *see id.* at 239–40 ("That plaintiffs do not independently challenge the legality of surveillance cameras and license plate readers does not mean that this Court must ignore their availability to the police and integration in the AIR program when applying *Carpenter*.") (Gregory, C.J., dissenting).

[258] *Id.* at 227; *id.* at 239–40 (Gregory, C.J., dissenting).

[259] *See* Commonwealth v. Almonor, 482 Mass. 35, 49 (2019); State v. Sylvestre, 254 So. 3d 986, 991 (Fla. Dist. Ct. App. 2018) ("If a warrant is required for the government to obtain historical cell-site information voluntarily maintained and in the possession of a third party, we can discern no reason why a warrant would not be required for the more invasive use of a cell-site simulator.") (internal citations omitted).

[260] *See, e.g.*, Commonwealth v. McCarthy, 484 N.E.3d 493, 494 (Mass. 2020).

[261] *See* Jessica Gutierrez-Alm, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*,

photos to constitute a search until it checks the database.[262] Law enforcement cannot know which rules apply until it has already taken the potentially regulated action. Chief Judge Dillard of the Court of Appeals of Georgia addressed this issue directly, noting:

> [L]aw enforcement will find it increasingly tricky to navigate the crossroads of ever-advancing technology and personal privacy as they relate to Fourth Amendment prohibitions. And this difficulty is only exacerbated by the fact that the decisions of the Supreme Court of the United States establish that warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing. "But as the Supreme Court emphasized once again in *Carpenter v. United States*, there remains a tried and true means of safely traversing these crossroads when law enforcement's specific obligations under the Fourth Amendment are in doubt—get a warrant. This default position seems especially wise in light of the "equilibrium-adjustment" the Supreme Court of the United States recently made in *Carpenter*. And while obtaining a warrant may not always lend itself to expediency, our republic's Fourth Amendment jurisprudence has "historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency."[263]

Of course, as is so often the case, "would that it 'twere so simple."[264] At least one court has suggested that if the government obtains a warrant that a court later finds invalid, the government may forfeit its argument that its investigatory action was not actually a search under *Carpenter* and the mosaic theory.[265]

The mosaic theory does not necessarily provide individuals more Fourth Amendment protection. Just as the mosaic theory gives people one more way to claim that a governmental action *is* a search, it also gives the

---

38 HAMLINE L. REV. 127, 154 (2015) (discussing the surveillance capabilities of ALPRs).

[262] *See* Kerr, *supra* note 5, at 39 ("The police need to know the rules to follow them, and they can't know them and can't follow them under the mosaic approach.").

[263] *Mobley v. State*, 346 Ga. App. 641, 651, 816 S.E.2d 769, 777 (2018) (Dillard, C.J., concurring) (footnotes omitted), *cert. granted* (Mar. 4, 2019), rev'd, 307 Ga. 59, 834 S.E.2d 785 (2019), *and vacated*, 353 Ga. App. 680, 839 S.E.2d 199 (2020).

[264] Movieclips, *Hail, Caesar! - Would That It Were So Simple Scene (2/10)*, YouTube (Jan. 27, 2017), https://www.youtube.com/watch?v=G629a_3MkkI.

[265] *See Matter of Search of Info. Stored at Premises Controlled by Google*, No. 20 M 392, 2020 WL 4931052, at *4 (N.D. Ill. Aug. 24, 2020) ("By having opted for a search warrant application in lieu of taking a chance that a warrantless seizure of the information to be yielded by the proposed geofences would not be upheld, and by not having developed further the argument for the Fourth Amendment's inapplicability, the government has forfeited the argument.").

government one more way to claim that its action *is not* a search. This has occurred most obviously in the case of CSLI,[266] but it is not hard to imagine it applying to any number of surveillance techniques. If ALPR databases continue to proliferate, courts that do not adopt the mosaic theory may well be inclined to treat them exactly like CSLI and create a bright line rule where access always constitutes a search. A court that adopts the mosaic theory can make that determination after the fact. If the database contained only a few hits, it could decide that the government's action was not a search. Defendants, beware.

Finally, it is telling that some courts have explicitly stated their confusion and uncertainty regarding the mosaic theory and the current state of Fourth Amendment doctrine. In some cases, this has led state courts to ignore any Fourth Amendment question and only use the mosaic theory to decide the issue on state constitutional grounds.[267] Other courts use the mess created by the mosaic theory to avoid applying it at all.[268] Problems arise with both approaches because technology-based investigative techniques that implicate the mosaic theory are only going to become more prevalent. The decision to apply or not apply the mosaic theory can prove dispositive in many situations and lead to opposite outcomes.

CONCLUSION

Ask any law student taking Criminal Procedure—understanding the Supreme Court's Fourth Amendment decisions is hard.[269] The mosaic theory has added an entirely new layer of confusion to an already jumbled topic. At least under the sequential approach, the Court provided a clear answer for a particular investigative technique. Using a thermal-imaging device to look into a house constitutes a search,[270] but going through somebody's trash on the sidewalk does not.[271] The Court drew clear lines

---

[266] Orin Kerr (@OrinKerr), TWITTER (July 22, 2020, 4:26 PM), https://twitter.com/orinkerr/status/1286080270345449473 ("If you adopt the mosaic theory, a tower dump shouldn't be a search: You're just learning one small fact about a person in isolation. If you reject the mosaic theory, it should be a search: It is collecting CSLI, period.")

[267] Commonwealth v. Mora, 485 Mass. 360, 361 (2020); Commonwealth v. Almonor, 482 Mass. 35, 36–37 (2019).

[268] State v. Muhammad, 194 Wash. 2d 577, 593–94 (2019); United States v. Howard, 426 F. Supp. 3d 1247, 1255–56 (M.D. Ala. 2019).

[269] Orin S. Kerr, *A Theory of Law*, 16 GREEN BAG 2D 111 (2012).

[270] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[271] California v. Greenwood, 486 U.S. 35, 37 (1988). Though, going forward it's not hard to imagine a mosaic theory garbage case where the government searched through multiple weeks-worth of garbage. That is another problem with the mosaic theory; even for cases where the Court has drawn a clear line and determined a certain investigative technique

for law enforcement to respect, courts to uphold, and lawyers to argue.

With the mosaic theory, however, almost every case will need an entirely new analysis to determine whether the particular aggregate of information obtained revealed too much about the defendant. Two years after *Carpenter*, so much mystery remains regarding how, or even if, a court should apply the mosaic theory, and this demonstrates the need for clarity. Either an explicit rejection of the doctrine or a clear framework for applying it in a consistent and cohesive manner would greatly reduce the confusion currently burdening the lower courts. Taking an example from Massachusetts, perhaps the most workable solution is a variety of bright-line rules for every investigative technique. Each bright-line rule has the potential to be under- or over-inclusive, but such rules would provide much needed clarity while still maintaining some of the mosaic theory's flexibility. While it is unreasonable to expect the Supreme Court to provide bright-line rules for every technology-based investigative technique, it is critically important that the Court provide lower courts with some guidance.

The Supreme Court's simplest solution would be an explicit rebuke of the mosaic theory. The Court could clarify that *Carpenter* applies to any and all CSLI. By eliminating any question of whether *Carpenter* applied the mosaic theory, the Court would direct lower courts to stick to the sequential approach, the traditional model for Fourth Amendment analysis. The question of which investigative techniques qualify for the mosaic theory would disappear, as would the mosaic theory's inherent line-drawing problem. Lower courts could continue to rely on well-established Fourth Amendment jurisprudence and there would be no need to wade into uncharted waters.

However, eliminating the mosaic theory would create a gap for certain investigative techniques. For technology like ALPRs, protection for any amount of usage might be overly burdensome for law enforcement, while unlimited usage carries significant privacy concerns. This tension is what made the mosaic theory appealing in the first place. Fortunately, there is a solution, but it exists outside of the scope of the judiciary.

The legislature can and should regulate emerging technologies that pose significant privacy concerns. As pointed out by Justice Alito, "[l]egislation is much preferable to the development of an entirely new body of Fourth Amendment law for many reasons, including the enormous

---

is not a search, many of those techniques would need to be revisited to ask the "how much" question.

complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."[272] The legislature can respond to the ever-evolving technological landscape by holding hearings and consulting experts.[273] If a law proves to be problematic, the legislature can change or eliminate it directly, unlike the judiciary's lengthy appellate process.[274] Indeed, this process is already occurring. Returning to the example of ALPRs, California state legislators have recognized the privacy concerns and are acting.[275]

Eliminating the mosaic theory from Fourth Amendment doctrine and leaving the legislature to address technology issues in this context is the most prudent step. Importantly, the Court could continue to address technology and the Fourth Amendment when necessary. For particularly invasive technologies, perhaps such as CSLI, the Court would be free to continue to apply the sequential approach and guarantee Fourth Amendment protection for any amount of usage.

In a vastly expanding technological landscape, these cases are sure to continue appearing. With the door at least open to the mosaic theory, lawyers will continue to argue that it should apply in various circumstances. The Fourth Circuit panel in *Leaders of a Beautiful Struggle* split on how to approach the mosaic theory and, at the time of writing this Note, the case is awaiting a rehearing *en banc*.[276] Similarly, the First Circuit granted a rehearing *en banc* for *Moore-Bush*.[277] Recently, law enforcement in Mississippi announced a pilot program where participating residents can provide live stream access of their personal security cameras, including Amazon Ring cameras, directly to law enforcement.[278] This could resemble a scenario where almost every home in an area has a pole camera monitoring its neighbors. In other words, it would make a perfect case for the mosaic theory. If courts, law enforcement, and lawyers are

---

[272] Carpenter v. United States, 138 S. Ct. 2206, 2361 (Alito, J., dissenting).
[273] Kerr, *supra* note 7, at 350.
[274] *See id.* at 350.
[275] Kari Paul, *California legislation targets police use of license plate readers*, The Guardian (Jan. 12, 2021, 6:00 PM), https://www.theguardian.com/us-news/2021/jan/12/california-police-automated-license-plate-readers.
[276] *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 831 F. App'x 662 (4th Cir. 2020).
[277] United States v. Moore-Bush, 963 F.3d 29, 50 (1st Cir. 2020) (1st Cir. 2020).
[278] Matthew Guariglia, *Police Will Pilot a Program to Live-Stream Amazon Ring Cameras*, ELECTRONIC FRONTIER FOUNDATION (Nov. 03, 2020), https://www.eff.org/deeplinks/2020/11/police-will-pilot-program-live-stream-amazon-ring-cameras.

expected to grapple with these ever growing and ever prevalent technology-based investigative techniques, the Supreme Court needs to clean up the mosaic theory mess.

APPENDIX A

Commonwealth v. Almonor, 482 Mass. 35, 47–48 n.9, 120 N.E.3d 1183, 1196 (2019)	Supreme Judicial Court of Massachusetts, Plymouth	Real-time CSLI "ping" is a search under art. 14.
Commonwealth v. Pacheco, 2020 PA Super 14, 227 A.3d 358, 370*, appeal granted in part*, 237 A.3d 396 (Pa. 2020)	Superior Court of Pennsylvania	No difference between real-time and historical CSLI. Using real-time CSLI is a search.
People v. Harris, 62 Misc. 3d 1076, 1080, 92 N.Y.S.3d 863 (N.Y. Sup. Ct. 2019)	New York Supreme Court, Queens County	Use of CSLI is a search.
People v. Simpson, 62 Misc. 3d 374, 379-80, 88 N.Y.S.3d 763 (N.Y. Sup. Ct. 2018)	New York Supreme Court, Queens County	Use of CSLI is a search.
Reed v. Commonwealth, No. 2018-CA-001574-MR, 2020 WL 594084, at *4 (Ky. Ct. App. Feb. 7, 2020), *review granted* (Sept. 16, 2020), *not to be published* (Sept. 16, 2020)	Court of Appeals of Kentucky	Real-time CSLI "ping" is a search.
State v. Brown, 331 Conn. 258, 272, 202 A.3d 1003, 1011 (2019)	Supreme Court of Connecticut	Use of historical CSLI is a search.
State v. Muhammad, 194 Wash. 2d 577, 585, 451 P.3d 1060, 1068 (2019)	Supreme Court of Washington	Use of CSLI is a search.

State v. Burke, 2019-Ohio-1951, ¶ 27, *appeal not allowed*, 2019-Ohio-3731, ¶ 27, 157 Ohio St. 3d 1406, 131 N.E.3d 75	Court of Appeals of Ohio, Eleventh District, Trumbull County	Use of historical CSLI is a search.
State v. Snowden, 2019-Ohio-3006, ¶ 33, 140 N.E.3d 1112, 1125-26, appeal not allowed, 2019-Ohio-4600, ¶ 33, 157 Ohio St. 3d 1485, 134 N.E.3d 205	Court of Appeals of Ohio, Second District, Montgomery County	Use of historical CSLI is a search.
State v. Sylvestre, 254 So. 3d 986, 991 (Fla. Dist. Ct. App. 2018)	District Court of Appeal of Florida, Fourth District.	Use of a cell-site simulator is a search.

APPENDIX B

United States v. Bronner, No. 3:19-CR-109-J-34JRK, 2020 WL 3491965, at *23 (M.D. Fla. May 18, 2020), report and recommendation adopted, No. 3:19-CR-109-J-34JRK, 2020 WL 3490192 (M.D. Fla. June 26, 2020)	United States District Court, M.D. Florida	Use of pole camera not a search.
United States v. Edmonds, 438 F. Supp. 3d 689, 693–94 (S.D.W. Va. 2020)	United States District Court, S.D. West Virginia, Charleston Divison	Use of pole camera not a search.
United States v. Fanning, No. 1:18-CR-362-AT-CMS, 2019 WL 6462830, at *4 (N.D. Ga. May 28, 2019), report	United States District	Use of pole camera not a search.

and recommendation adopted, No. 1:18-CR-0362-AT-1, 2019 WL 3812423 (N.D. Ga. Aug. 13, 2019)	Court, N.D. Georgia, Atlanta Division	
United States v. Kay, No. 17-CR-16, 2018 WL 3995902, at *3 (E.D. Wis. Aug. 21, 2018)	United States District Court, E.D. Wisconsin	Use of pole camera not a search.
United States v. Kelly, 385 F. Supp. 3d 721, 726–27 (E.D. Wis. 2019)	United States District Court, E.D. Wisconsin	Use of stationary video surveillance of the exterior of apartment building and hallway outside of apartment not a search.
United States v. Kubasiak, No. 18-CR-120-PP, 2018 WL 4846761, at *7 (E.D. Wis. Oct. 5, 2018)	United States District Court, E.D. Wisconsin	Use of cameras installed at neighbor's home not a search.
United States v. Moore-Bush, 963 F.3d 29, 31 (1st Cir. 2020)	United States Court of Appeals, First Circuit	Use of pole camera not a search.
United States v. Thomas Ukoshovbera A. Gbenedio, No. 1:17-CR-430-TWT-JSA, 2019 WL 2177943, at *4 (N.D. Ga. Mar. 29, 2019), report and recommendation adopted sub nom. United States v. Gbenedio, No. 1:17-CR-430-TWT, 2019 WL 2173994 (N.D. Ga. May 17, 2019)	United States District Court, N.D. Georgia, Atlanta Division	Use of pole camera not a search.

United States v. Tirado, No. 16-CR-168, 2018 WL 3995901, at *2 (E.D. Wis. Aug. 21, 2018)	United States District, E.D. Wisconsin	Use of pole camera not a search.
United States v. Tuggle, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3 (C.D. Ill. July 31, 2018)	United States District Court, C.D. Illinois	Use of a pole camera not a search.*

*The court left open the possibility of potentially applying the mosaic theory in the future. *See United States v. Tuggle*, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3 (C.D. Ill. July 31, 2018) (Discussing eighteen months of pole camera surveillance and finding "[a]t some point the length of monitoring may constitute a search. Here, the facts and case law from other circuits do not support a finding that the extended surveillance at issue here constitute that search."