BRENNAN CENTER FOR JUSTICE

The Fourth Amendment in the Digital Age

How *Carpenter* Can Shape Privacy Protections for New Technologies

By Laura Hecht-Felella PUBLISHED MARCH 18, 2021

Brennan Center for Justice at New York University School of Law

Table of Contents

Introduction

The Fourth Amendment stands for the principle that the government generally may not search its people or seize their belongings without appropriate process and oversight. Today, we are at a jurisprudential inflection point as courts grapple with when and how the Fourth Amendment should apply to the data generated by technologies like cell phones, smart cars, and wearable devices. These technologies — which we rely on for enhanced communication, transportation, and entertainment — create detailed records about our private lives, potentially revealing not only where we have been but also our political viewpoints, consumer preferences, people with whom we have interacted, and more. The resulting trove of information is immensely valuable to law enforcement for use in investigations and prosecutions, and much of it is currently available without a warrant.

This paper describes how the U.S. Supreme Court's 2018 decision in *Carpenter v. United States* has the potential to usher in a new era of Fourth Amendment law. In *Carpenter*, the Court considered how the Fourth Amendment applies to location data generated when cell phones connect to nearby cell towers.[1] The Court ultimately held that when the government demanded seven days of location information from defendant Timothy Carpenter's cell phone provider without a warrant, it violated the Fourth Amendment. The decision sits at the intersection of two lines of cases: those that examine location tracking technologies, like beepers or the Global Positioning System (GPS), and those that discuss what expectation of privacy is reasonable for information disclosed to third parties, like banks or phone companies. In reaching its conclusion that a warrant was required, the Court upended existing precedent, ruling for the first time that location information maintained by a third party was protected by the Fourth Amendment.

In exploring the Court's decision in *Carpenter* and its application to data from a variety of technologies — such as GPS, automated license plate readers (ALPRs), and wearables — this paper argues that it is incumbent on courts to preserve the balance of power between the people and the government as enshrined in the Fourth Amendment, which was intended to "place obstacles in the way of a too permeating police surveillance."[2] Moreover, in determining the scope of the Constitution's protections for data generated by digital technologies, courts should weigh the five factors considered in *Carpenter*: the intimacy and comprehensiveness of the data, the expense of obtaining it, the retrospective window that it offers to law enforcement, and whether it was truly shared voluntarily with a third party. Section I is an overview of Fourth Amendment jurisprudence. Section II discusses the *Carpenter* decision and its takeaways. Section III applies *Carpenter* to various surveillance technologies and looks ahead at how Fourth Amendment jurisprudence might continue to develop in the digital age.

Overview of Fourth Amendment Jurisprudence

While *Carpenter* in many ways signaled a departure from the Court's reliance on traditional models like the third-party doctrine, the decision is still firmly rooted in precedent. Thus, it is important to begin by situating *Carpenter* historically within the landscape of relevant Fourth Amendment jurisprudence.

The Fourth Amendment safeguards the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by generally requiring that the government first obtain authorization from a neutral judge or magistrate in the form of a warrant.[3] The framers intended the Fourth Amendment to curtail indiscriminate searches and seizures, which the colonists had been subjected to under British rule.[4] Writs of assistance had bestowed on British officers blanket authority to conduct searches of any place, at any time, without notice or reasonable suspicion.[5] The British government attempted to use the writs to stifle free speech and suppress political revolution. Given this history, the Court has repeatedly recognized the interconnectedness of various civil liberties, like freedom of expression and assembly, and the protections against government intrusion enshrined in the Fourth Amendment.[6]

Reasonable Expectation of Privacy Test

Historically, the Supreme Court interpreted the Fourth Amendment in light of its origins as the embodiment of the early English common law principle that "every man's home is his castle."[7] Early decisions conceptualized Fourth Amendment protections as extending exclusively to the seizure of "tangible material effects" or an "actual physical invasion" into the areas enumerated by the amendment (persons, houses, papers, and effects).[8] The theory that the Fourth Amendment protected only against physical intrusion of private spaces, called the trespass doctrine, guided the Court's Fourth Amendment jurisprudence for several decades until its 1967 decision in *Katz v. United States*.

The Court seemingly abandoned the trespass doctrine in *Katz*, in which it considered whether the government's use of an electronic listening device attached to the outside of a public phone booth implicated the Fourth Amendment. The Court conceded that there had been no trespass but still concluded that a search had occurred, reasoning that "the Fourth Amendment protects people and not simply areas."[9]

The Court's holding that the Fourth Amendment's reach "cannot turn upon the presence or absence of a physical intrusion" was revolutionary.[10] For the first time, Fourth Amendment protections were divorced from the physical trespass requirement. Rather, as described in Justice John Marshall Harlan's concurrence, which set out what has become known as the *Katz* test, the Constitution protects against government intrusion when a person has exhibited an actual (subjective) expectation of privacy and their expectation of privacy is one that society is objectively prepared to recognize as reasonable.[11] *Katz* is the foundation of modern Fourth Amendment jurisprudence. It extends the sphere of the Fourth Amendment's protections to law enforcement surveillance that encroaches on privacy, even without a physical intrusion.

Third-Party Doctrine

After unveiling the two-pronged reasonable expectation of privacy test in *Katz*, the Court went on to distinguish information voluntarily turned over to third parties. In *United States v. Miller* (1976) and *Smith v. Maryland* (1979), the Court codified the third-party doctrine, which stands for the principle that individuals have no legitimate expectation of privacy in information that they voluntarily share with third parties, regardless of

whether they intended for the government to have access to the data.[12] Thus, while the government would need a warrant to obtain an individual's personal papers from their home, law enforcement could obtain the same papers from a third party with whom they have been shared — even for a limited purpose — with little to no legal process, at least as a constitutional matter.[13]

In *Miller*, the Court held that defendant Mitch Miller had no legitimate expectation of privacy in his financial records, including copies of checks and deposit slips maintained by his bank, because he had "voluntarily conveyed" this information to a third party. It was irrelevant that Miller had shared the records with his bank for the limited and specific purpose of doing business; the fact that they were in a bank teller's hands meant that the government could access them without a warrant.[14]

In *Smith*, the Court similarly held that law enforcement's use of a pen register, a device installed by a telephone company at its offices to monitor the telephone numbers dialed on defendant Michael Smith's home phone, was not a search requiring a warrant. The Court reasoned that when Smith used his phone, he voluntarily assumed the risk that the phone company might relay the numbers he had called to the police.[15]

The Court conceptualized voluntariness broadly in these decisions, but Justice Thurgood Marshall's dissent in *Smith* gave voice to an argument that has been echoed by critics: disclosure to a third-party bank or phone carrier is not truly voluntary, given that banks and phones are necessary components of modern society.[16] The third-party doctrine has begun to lose force in recent years and was significantly undermined in *Carpenter*. It has not yet, however, been conclusively abandoned or overturned.

Public Versus Private Spaces

Two decisions from the 1980s revealed the Court's divergent approaches under the *Katz* model to government surveillance in public versus private spaces. In *United States v. Knotts* (1983) and *United States v. Karo* (1984), the Court considered the constitutionality of using a surreptitiously planted beeper device to monitor a suspect's movements.

The Court determined in *Knotts* that a warrant was not required to monitor "a person traveling in an automobile on public thoroughfare" using a concealed beeper as a tracking device. The Court reasoned that the government could have obtained the same information relayed by the beeper by physically following defendant Leroy Knotts on public roads.[17] Thus, Knotts had "no reasonable expectation of privacy in his movements from one place to another."[18]

However, the Court reached a different conclusion in *Karo*, in which federal investigators used a beeper to track a container of ether, allegedly intended to produce cocaine, as it moved between private residences and commercial storage lockers. The Court distinguished the use of beeper monitoring in private residences from *Knotts*, finding that the warrantless use of a beeper to monitor activity in a private home — a location not open to visual surveillance — violated the Fourth Amendment.[19]

Knotts and *Karo* underscored the heightened constitutional implications of using a surveillance device that elicits information from within a home. While the decisions highlighted the Court's willingness to find a decreased expectation of privacy in a person's public movements, the Court explicitly reserved the question of whether "different constitutional principles may be applicable" if "twenty-four-hour surveillance of any citizen of this country [were] possible."[20] Needless to say, this scenario is no longer a mere possibility but a reality.

Impact of Technology

In several decisions after *Knotts* and *Karo*, the Court grappled with the impact of technological advances on an individual's objective reasonable expectation of privacy. Although no comprehensive doctrine emerged from these cases, various aspects of their reasoning are reflected in the *Carpenter* decision.

In *Florida v. Riley* (1989), the Court upheld the warrantless aerial observation of the interior of defendant Michael Riley's residential greenhouse using a helicopter, reasoning that since "private and commercial flight by helicopter is routine," Riley could not have reasonably expected that his greenhouse would be protected from aerial observation.[21]

A little more than a decade later, in *Kyllo v. United States* (2001), the Court held that where "the Government uses a device that is not in general public use" — in this case a thermal imager — "to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[22] In distinguishing technologies on the basis of their public prevalence, the Court in *Kyllo* attempted to "take the long view" so that its rulings might "take account of more sophisticated systems that are already in use or in development."[23] The Court's decision in *Carpenter* builds on the principle articulated in *Kyllo* that the Fourth Amendment must evolve as technology advances.[24]

The complexities inherent in applying the Fourth Amendment to modern technologies were evidenced again in *Riley v. California* (2014), where the Court held that police are generally required to obtain a warrant before searching digital information on an arrestee's cell phone.[25] The Court noted that cell phones have immense storage capacity, facilitating the storage of vast amounts of sensitive data that would not typically be carried around in hard-copy form. The Court observed that cell phones are now "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy," and that "a significant majority of American adults now own such phones."[26] The Court's later decision in *Carpenter* echoed this recognition of the cell phone's pervasiveness in modern society.[27]

Revising the Trespass Doctrine

The Court's divided 2012 decision in *United States v. Jones* revealed fault lines in its Fourth Amendment analysis. The question before the Court was whether the warrantless installation and use of a GPS device to track the movements of a suspect's vehicle over the course of a month constituted a search under the Fourth Amendment. The majority opinion, written by Justice Antonin Scalia, revived the trespass doctrine, finding that the physical installation of a GPS onto a car — an "effect" in Fourth Amendment parlance — in order to obtain information about defendant Antoine Jones's physical movements constituted a search.[28] In his opinion for the majority, Justice Scalia explained that "the *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test."[29] In two concurring opinions, five justices argued that the monitoring of an individual's location for a lengthy period of time constituted a search under the Fourth Amendment, but neither of those opinions garnered a majority to supplant Justice Scalia's reasoning for the Court.[30] The split decision, in which some justices advocated for the abandonment of the trespass doctrine entirely, further complicated the already complex Fourth Amendment analysis that developed in the wake of *Katz*.

As technology has transformed our society, many of the elements considered by the Court under *Katz* and its progeny — including whether a technology is in general public use and whether the information sought by the government was relayed to a third party — have become increasingly tenuous measures of whether an

individual has a reasonable expectation of privacy in the data sought by the government. Indeed, even at the time that *Kyllo* was decided, four dissenting justices criticized the Court's focus on whether the technology in question was in general public use, noting that "it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[31] Likewise, Justice Sonia Sotomayor opined in her concurrence in *Jones* that the third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[32] The Court finally confronted these critiques squarely — though not exhaustively — in *Carpenter*.

Carpenter v. United States: A New Approach

The Supreme Court's decision in *Carpenter v. United States* begins a new chapter in Fourth Amendment jurisprudence. As described below, the facts the Court considered seemed to fall squarely within the existing third-party doctrine framework developed in *Smith* and *Miller*, but the Court reached a radically different outcome. While the Court explicitly narrowed its holding to the facts before it, the decision illustrates the justices' reluctance to uncritically extend existing precedents like the third-party doctrine and the Court's readiness to reconsider what constitutes a reasonable expectation of privacy in the digital age. The *Carpenter* decision is likely to profoundly affect future cases involving digital technologies.

The *Carpenter* Decision

In *Carpenter*, the Court held that a warrant was required for the police to obtain seven days or more of historical cell-site location information (CSLI) records. CSLI records are generated when cell phones connect to nearby cell towers, which occurs at the start and end of calls, during the transmission of text messages and routine data connections, and several times a minute when a cell phone is turned on, even when it is not in use.[33] Wireless carriers currently maintain CSLI data, which can be used to determine a cell phone's approximate location, for up to five years.[34]

Based on CSLI evidence, defendant Timothy Carpenter had been charged with aiding and abetting a series of robberies. The government had sought 152 days of Carpenter's CSLI records from MetroPCS and seven days of CSLI from Sprint pursuant to the Stored Communications Act, under which the government can require the disclosure of certain telecommunications records upon showing "reasonable grounds" to believe that the records are "relevant and material to an ongoing criminal investigation."[35] Ultimately, the government obtained 12,898 location points tracking Carpenter's movements across 127 days — averaging about 101 data points per day. Before trial, Carpenter's attorneys moved to suppress the government's cell-site evidence on Fourth Amendment grounds, arguing that the FBI needed a warrant based on probable cause to obtain the records. The district court denied the motion to suppress, and the U.S. Court of Appeals for the Sixth Circuit affirmed. Carpenter ultimately appealed to the Supreme Court, which reversed and held that acquisition of Carpenter's cell-site records was a Fourth Amendment search.[36]

Although the Court declined to explain how its holding might be applied to data or technologies other than historical CSLI,[37] the *Carpenter* decision is nevertheless transformative. Rather than focusing exclusively on the threat posed by technologies that are not yet in public use, as it had in the past, the Court recognized the risk to privacy posed by technologies that are already commonplace, like cell phones. The Court noted that if there were no Fourth Amendment constraints on obtaining CSLI, "[o]nly the few without cell phones could escape this tireless and absolute surveillance."[38] This is a clear departure from the Court's reasoning in *Kyllo*, in which the justices relied on the fact that the technology in question was not in general public use.

Additionally, for the first time, the Supreme Court made it clear that the third-party doctrine is not absolute. The Court did not overturn *Smith* or *Miller*, but in his opinion for the majority, Chief Justice John Roberts recognized that the bright-line rule from these decisions is ill-suited to the digital age.[39] Given that most of us routinely reveal or disclose private information as a function of using a variety of increasingly ubiquitous personal technologies, it is no longer tenable to conclude categorically that individuals forfeit any reasonable expectation of privacy in information disclosed to third parties. Rather, the Court considered whether Carpenter had "truly shared" his CSLI voluntarily, "as one normally understands the term."[40]

In dissenting opinions, four justices highlighted the difficulties in applying the majority's new conception of voluntariness, particularly given the similarities between CSLI and the bank records at issue in *Miller*. For example, Justices Anthony Kennedy and Samuel Alito argued in their dissents that Carpenter had no Fourth Amendment privacy interest in his CSLI since it was possessed, owned, and controlled by a third party — namely, his cell phone provider.[41] Justices Clarence Thomas and Neil Gorsuch went further in asserting that the unworkability of the *Carpenter* decision exemplified broader shortcomings in Fourth Amendment doctrine and calling the *Katz* legacy into question.[42]

The *Katz-Carpenter* Test

The Court's decision in *Carpenter* lays the foundation for a new, five-factor *Katz-Carpenter* test for use in determining whether a warrant is required when the government seeks to obtain data from digital technologies. Although the Court declined to express a view on tools other than historical CSLI, the majority recognized that individuals routinely reveal private information to third parties as a by-product of using a variety of modern technologies. Thus, in making an objective reasonableness determination under *Katz*, the law must seek to secure "the privacies of life" against "arbitrary power" and uphold the framers' central aim to "place obstacles in the way of a too permeating police surveillance."[43] Unfortunately, as Justice Gorsuch underscored in his dissenting opinion, the Court did not explain "how far to carry either principle or how to weigh them against the legitimate needs of law enforcement."[44]

Instead, with *Carpenter*'s gloss on the objective prong of *Katz*'s reasonable expectation of privacy test, determining whether a warrant is required for the government to obtain data from modern technologies requires balancing the several elements the Court considered. As Justice Kennedy recognized in his dissent, the five factors most relevant to the majority's opinion are comprehensiveness, intimacy, expense, retrospectivity, and voluntariness.[45] This paper argues that together these five factors comprise the *Katz-Carpenter* test. Each factor is described in more detail below.

Comprehensiveness

A technology implicates comprehensiveness if it can give the government "near perfect surveillance" and create a record that is "detailed, encyclopedic, and effortlessly compiled."[46] As the *Carpenter* majority grappled with the breadth of the surveillance that CSLI makes possible, it made clear that it found the comprehensiveness of the information sought by the government relevant in determining whether a Fourth Amendment search had occurred. Despite previously differentiating in *Knotts* and *Karo* between a reasonable expectation of privacy in public versus private spaces — for instance, in a home versus on public roads — the *Carpenter* Court, pointing to the concurrences in *Jones*, observed that "individuals have a reasonable expectation of privacy in the whole of their physical movements."[47] Incorporated into this analysis was the duration of the surveillance. While the Court determined that seven days of CSLI data was enough to constitute a Fourth Amendment search, it declined to rule on whether the government could obtain data from a more limited period without a warrant.[48]

Intimacy

A technology provides an intimate window into a person's life when it potentially reveals personal information such as "familial, political, professional, religious, and sexual associations."[49] The *Carpenter* Court recognized that for many Americans, CSLI records hold the "privacies of life."[50] A cell phone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[51] Writing for the majority, Chief Justice Roberts explained that unlike bank

records or a pen register, time-stamped location data creates a "detailed chronicle of a person's physical presence compiled every day, every moment."[52] Accordingly, the Court's reasoning in *Carpenter* suggests that a person is more likely to retain a reasonable expectation of privacy in third-party records if the information contained in them is particularly intimate or sensitive and revealing.

Expense

Expense is implicated when a technology makes surveillance "easy, cheap, and efficient as compared to traditional investigative tools."[53] In other words, it acts as a force multiplier, allowing the government to conduct surveillance that resource limitations might have otherwise made impossible. Quoting *Jones*, the *Carpenter* Court noted that "society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement [of an individual] for a very long period."[54] But in the context of CSLI, for example, this expectation is threatened by the fact that "[w]ith just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense."[55]

Retrospectivity

Retrospectivity comes into play when a technology or data set creates an infallible record that allows the government to effectively travel back in time. The Court's *Carpenter* analysis considered two elements with regard to this factor. First, the Court noted that CSLI data's retrospective quality gives police access to a category of information that is otherwise unknowable — in other words, CSLI functions like a time machine of sorts — allowing law enforcement agents to go back in time prior to the first moment of suspicion and investigate anyone they wish.[56] Thus, the technology "runs against everyone," since the government does not need to know in advance whether or when to follow a particular individual. Second, the Court highlighted that CSLI records are free from the "frailties of recollection," and "[u]nlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."[57] Because wireless carriers continuously collect, store, and retain CSLI data about every customer, the government can trace anyone's past whereabouts subject only to carriers' retention policies.

Voluntariness

Lastly, without overturning *Smith* and *Miller*, the Court recognized that data generated by technologies that are integral to modern-day life could not be said to be voluntarily shared when the production of this information is "inescapable and automatic."[58] The Court noted that a cell phone logs CSLI records by "dint of its operation, without any affirmative act on the part of the user beyond powering up."[59] Additionally, cell phones are so "indispensable to participation in modern society" that it is difficult to avoid their use.[60] The Court compared CSLI to an ankle monitor, noting that cell phones are almost akin to a "feature of human anatomy" because they travel with us wherever we go.[61]

▪ ▪ ▪

Carpenter limited the scope of the third-party doctrine and greatly expanded the Fourth Amendment's potential reach. However, its narrow holding also left unresolved how the Fourth Amendment might be applied to other technologies. The five-factor *Katz-Carpenter* test distilled above is intended to bridge that gap. While the Court did not provide guidance on how to prioritize each of these five factors, it did suggest that no one consideration is dispositive in determining whether a warrant is required. Rather, courts must take a holistic approach, as the majority did in *Carpenter*, with the aim of evaluating whether any given technology threatens to expand the government's ability to engage in too-permeating police surveillance.[62]

Prominent legal scholars have espoused other possible interpretations that place particular emphasis on some of these factors or instead entirely omit them. We briefly describe some of these theories below and explain why we believe that our theory most fully accounts for the Court's opinion in *Carpenter* and offers guidance regarding the treatment of other technologies under the Fourth Amendment.

Other Interpretations of *Carpenter*

While some legal scholars have emphasized the narrowness of the *Carpenter* decision, others have maintained that it is an inflection point in Fourth Amendment jurisprudence that will broaden constitutional protections.[63] Most analyses begin with the recognition that *Carpenter* attempts to reconcile the Fourth Amendment with our modern, digital age reality.[64] However, commentators diverge in their explanations of what led the Court to conclude that collecting seven days of CSLI data constituted a search requiring a warrant and of how courts should apply the ruling going forward.

For example, Professor Paul Ohm suggests that a three-factor test emerges from the majority opinion. When the government seeks to access large, private databases containing nonpublic information about individuals, judges should ask whether the information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection.[65]

Professor Orin Kerr identifies three different requirements needed to trigger Fourth Amendment protections for records that contain metadata like location information rather than content: (1) the records exist because of digital age surveillance methods; (2) they are not the product of a user's meaningful voluntary choice because they are necessarily created when a person uses core digital age technologies; and (3) they tend to reveal the privacies of life beyond the legitimate interests of criminal investigations.[66]

Professors Susan Freiwald and Stephen Wm. Smith, the latter a former magistrate judge, distinguish five factors as central to the Court's inquiry: whether the surveillance technique was (1) hidden, (2) continuous, (3) indiscriminate, and (4) intrusive, along with (5) the expense and effort required to compile the data.[67] These five particulars overlap significantly with the factors we identify as comprising the *Katz-Carpenter* test, but they include as additional elements that the data be hidden and indiscriminate. Freiwald and Smith argue that "hidden surveillance requires procedural hurdles to keep it in check because it lacks the safeguards that exposure provides to more public forms of surveillance."[68] Moreover, indiscriminate surveillance gives rise to government fishing expeditions through databases akin to general writs of assistance.[69] The *Katz-Carpenter* test advanced in this paper discusses indiscriminate surveillance in the context of retrospectivity in asking if the technology runs against everyone. However, we believe that *Carpenter* has potential implications even for technologies that do not meet Freiwald and Smith's definition of "hidden."

These three illustrative theories share the foundational belief that *Carpenter* has the potential to reshape how the Fourth Amendment applies to the records generated by new technologies, notwithstanding the Court's assertion of the narrowness of its holding. The *Katz-Carpenter* test advanced in this paper is built on the same core principle and overlaps with several of these theories when it comes to relevant factors. For instance, the intimate nature of the information sought by the government is highlighted in all three approaches. However, in focusing on the five factors that Justice Kennedy underscored in his dissent as particularly relevant, our *Katz-Carpenter* test broadens *Carpenter*'s potential applicability in hopes of evaluating its potential impact on the records generated by modern technologies ranging from smart cars to wearables.

Applying the *Katz-Carpenter* Test to Other Data

As the Court recognized in *Carpenter*, new technologies do not always "fit neatly under existing precedents."[70] This section explores how the *Katz-Carpenter* test articulated above might apply to a variety of technologies. While the resolution of specific cases will of course be fact-dependent, this section demonstrates how the *Katz-Carpenter* model pushes courts to adopt greater Fourth Amendment protections for the records created by digital technologies.

This section begins with a discussion of cell phone and smart car location information and then moves on to review surveillance technologies used by law enforcement. While the latter do not implicate the third-party doctrine, the *Carpenter* approach is nevertheless instructive in terms of the objectively reasonable expectation of privacy that someone might have in the data generated by these technologies. Finally, it examines how the Fourth Amendment might apply to law enforcement access to data from commercial technologies that collect personal data incidental to their use: body-worn technologies, smart doorbells, and web browsers.

Location Information from Cell Phones and Smart Cars

The teachings of *Carpenter* translate most readily to government collection of location information held by a third party. Examples of this include real-time cell phone location information, GPS data from smart cars, and reverse location searches.

Real-Time Cell Phone Location Information

The *Carpenter* Court reserved decision on real-time tracking of cell phones.[71] However, there can be little question that such surveillance poses many of the same privacy concerns as historical CSLI and will constitute a Fourth Amendment search under the *Katz-Carpenter* analysis, requiring a warrant based on probable cause.

Cell phones generate location information in many ways, most commonly in the form of CSLI or GPS data.[72] As discussed above, CSLI is location data created when cell phones connect to nearby cell towers, which happens not only when they are used to make calls, message, and access data, but also simply when they are turned on.[73] Real-time CSLI data can be obtained either through the contemporaneous monitoring of CSLI records or by pinging a suspect's phone. Contemporaneous monitoring occurs when a wireless provider tracks a cell phone's location using the CSLI records generated automatically as the phone connects to nearby cell towers and then conveys that data in real time to the police. "Pinging" is when a wireless carrier sends a signal to a cell phone, compelling it to automatically respond and thereby reveal its location in relation to the nearest cell towers.[74]

Phones with GPS chips also continuously generate location information as they position themselves relative to nearby satellites.[75] Today, almost all cell phones are equipped with embedded GPS chips as a result of a Federal Communications Commission (FCC) order that strengthened location accuracy requirements for cell phones in order to improve 911 services.[76] Most GPS chips are accurate to within about 16 feet, depending on factors like urban density.[77] In comparison, the accuracy range for the CSLI in *Carpenter* was between approximately 660 feet and 4 square miles.[78]

Cell phone location information can be collected and retained by a variety of parties, including cell phone providers (such as AT&T or Verizon) and phone manufacturers and operating systems (such as Apple and Google).[79] Some of the most extensive and detailed repositories of GPS data are created by third-party cell

phone applications, which use GPS to provide users with a variety of services ranging from locating a rideshare to delivering weather or news.[80] Cell phone location data is frequently sold to data brokers, which compile consumers' personal information and resell or share that information with others, including law enforcement.[81]

When an individual's location is unknown, ascertaining their whereabouts using contemporaneous cell phone location information might reveal their presence inside a home or other constitutionally protected space. Given the impossibility of accurately predicting the nature of an individual's location, *Kyllo* and *Karo* indicate that a warrant should be required for real-time tracking of cell phones.[82] In fact, even before *Carpenter* was decided, several courts had determined that law enforcement must acquire a warrant to lawfully obtain real-time cell phone location data since there is no way to know in advance whether the phone is physically located within a constitutionally protected place.[83] Cases addressing real-time location tracking in the wake of *Carpenter* have generally reached the same outcome.[84] Nevertheless, because the *Carpenter* Court declined to extend its holding to real-time monitoring or address the applicability of *Karo* or *Kyllo*, we analyze below the use of real-time CSLI and GPS data under the *Katz-Carpenter* test. Our analysis reaffirms the conclusion that a warrant should be required.

In any given case, the comprehensiveness of real-time phone tracking will depend in part on the duration of the surveillance. However, real-time location monitoring, like historical CSLI, implicates comprehensiveness because it facilitates the creation of a record that is detailed and effortlessly compiled while allowing law enforcement to track every movement a person makes. These conditions give the government access to near-perfect surveillance.

Real-time GPS and CSLI monitoring also expose the same intimate location data as historical CSLI. While the sensitivity of the information revealed by such surveillance may depend on its duration, even a single data point can be extremely revealing.[85] Moreover, as the Court recognized in *Carpenter*, sustained surveillance of a person's movements can reveal an extraordinary amount, including their associations, attendance at public or private gatherings, where they pray, where they work, if they attended a political protest or rally, and even with whom they spend their nights.[86] Because the intimacy of the information revealed by real-time surveillance cannot be known in advance, it should be uniformly protected with a warrant requirement.

Cell phone tracking is inexpensive and efficient compared to traditional investigative tools. As the Court recognized in *Carpenter*, GPS data makes it possible for law enforcement to effectively monitor exponentially more people than conventional methods and to do so at a far lower cost.[87] Similarly, CSLI pinging and contemporaneous monitoring are cheap and easy relative to other forms of police surveillance.[88] For example, many wireless providers have created websites allowing law enforcement agents to request and obtain real-time location data without leaving their desks; this can cost as little as $13 per phone, according to a 2019 report.[89] In comparison, a 2014 analysis indicated that more traditional methods of location tracking, such as physically tailing a suspect, cost law enforcement approximately $275 per hour. Although the latter data is several years older, it seems unlikely that the cost of physical surveillance would have decreased significantly.[90]

Retrospectivity is one meaningful difference between historical CSLI and real-time cell phone location monitoring in any form. By its very nature, real-time GPS and CSLI allow the government to monitor someone's movements as they occur. They do not run against everyone in the same way as historical CSLI unless the information is collected indiscriminately or stockpiled. Rather, the police need to know in advance whether they want to follow a particular individual.

Regarding voluntariness, as the Court recognized in *Carpenter*, cell phones are such an indispensable part of modern society that it is nearly impossible to avoid their use. Like historical CSLI, real-time CSLI exploits an unavoidable feature of cell phones — namely, that they automatically connect to nearby cell towers and in doing so transmit time-stamped location information. Cell phone users can no more protect themselves from real-time pinging or contemporaneous tracking than they can guard against historical CSLI monitoring. Absent powering off a cell phone, there is no way to avoid collection of real-time CSLI information. Thus, the generation of real-time CSLI data is inescapable and automatic.

This aspect of the voluntariness analysis is more nuanced with respect to real-time GPS monitoring. Cell phones with embedded GPS chips similarly generate location data automatically when they are turned on, but most smartphones now allow users to deactivate location services and to control whether specific applications have access to their location data.[91] However, reports have shown that these permission systems are often either ineffective or vulnerable to work-arounds.[92] In addition, even if users can successfully deactivate a cell phone's location services, they likely could not disable the E911 location tracking systems mandated by the FCC, which law enforcement have exploited in the past to conduct real-time GPS monitoring.[93] In most cases, like real-time CSLI, real-time GPS data is inescapably and automatically generated.

As the foregoing discussion demonstrates, the Fourth Amendment privacy concerns posed by real-time cell phone location tracking are largely analogous to those posed by historical CSLI. Such surveillance upends traditional expectations of privacy by removing historical constraints on police surveillance, including resource and capability limitations. In the hands of law enforcement, the information generated by real-time tracking has the potential to replicate and exacerbate the disproportionate surveillance of communities already subject to overpolicing, including noncitizens, people of color, Muslim Americans, and LGBTQ+ individuals. Through GPS surveillance and CSLI monitoring, law enforcement can comprehensively and inexpensively monitor the movements of nearly every American at any point in time.[94] Because the intimacy of the information revealed — including whether it will expose data from inside a home or another constitutionally protected space — cannot be determined in advance, all real-time location information should be equally protected as a constitutional matter. The fact that real-time tracking does not always implicate retrospectivity should not serve to remove this data from the Fourth Amendment's protection.

Real-time GPS and CSLI monitoring clearly expand the government's ability to engage in too-permeating police surveillance by allowing police to obtain information that would otherwise be unknowable. Whether such surveillance will reveal information from inside constitutionally protected spaces like the home is impossible to predict in advance. Thus, both the *Karo* and *Kyllo* decisions and the *Katz-Carpenter* analysis indicate that law enforcement should be required to obtain a warrant before accessing this data.

Smart Car GPS Data

Although the Court's decisions in *Knotts* and *Karo* suggested that individuals have a reduced expectation of privacy on public roads, they left open the question of how the Fourth Amendment might apply if "twenty-four-hour surveillance of any citizen of this country [were] possible."[95] Under the *Jones* concurrences and the *Katz-Carpenter* analysis, it is likely that monitoring of GPS data from smart cars constitutes a Fourth Amendment search requiring a warrant based on probable cause.

Like most cell phones, many modern vehicles are equipped with embedded GPS technologies that generate location information while facilitating a variety of functions ranging from navigation assistance to weather alerts to security.[96] Car manufacturers and their affiliates may collect and retain this location information — and share it with law enforcement, either in response to a government inquiry or in other contexts.[97]

In *Jones* and *Carpenter*, the Court laid the groundwork for finding that surveillance of GPS data from smart cars gives rise to Fourth Amendment concerns. While the majority decision in *Jones* centered on the trespassory installation of a GPS in a car, the five concurring justices argued that it was the sustained monitoring of an individual's location that constituted a search under the Fourth Amendment.[98] In the context of smart cars, where data is collected by third-party companies, *Carpenter* reinforces the reasoning of the *Jones* concurrences.

GPS tracking of smart cars touches on each of the five elements that the Court considered in *Carpenter*. First, as Justice Sotomayor noted in her concurrence in *Jones* and the Court reaffirmed in *Carpenter*, GPS monitoring is cheap compared to conventional surveillance techniques.[99] Thus, it evades an ordinary check on abusive law enforcement practices, limited resources, and acts as a force multiplier, permitting the government to surveil exponentially more people than would otherwise be possible.

Regarding comprehensiveness, GPS monitoring of smart cars enables tracking of the totality of someone's movements on public and private roadways, creating a detailed record that gives the government access to near-perfect surveillance. While *Carpenter* suggested that the monitoring of GPS data from phones is more problematic than from cars because people "regularly leave their vehicles," the Court did recognize that a GPS device tracks every movement a person makes in their vehicle.[100] For the majority of Americans whose vehicles are their primary mode of transportation, tracking their cars' location is analogous to tracking the whole of their public movements.[101]

Duration was an additional aspect of the Court's comprehensiveness analysis. In *Jones*, four concurring justices opined that "longer-term" government monitoring of GPS data presented Fourth Amendment concerns at some point "before the 4-week mark."[102] Although a consensus has yet to emerge as to what constitutes longer-term GPS monitoring, it is reasonable to infer from *Jones* that the outermost threshold is less than four weeks and from *Carpenter* that it might be seven days.[103]

With regard to intimacy, GPS data from smart cars may not always be as revealing as from cell phones because people do leave their cars. However, whether in a phone or a car, GPS location data can reveal whether someone visited an immigration attorney, a political campaign's headquarters, a religious site, or a fertility doctor, for example. Because the degree of intimacy is impossible to know in advance, GPS data from cars should be protected to the same extent as cell phones.

GPS devices in smart cars satisfy both aspects of the Court's voluntariness analysis as well: indispensability to participation in modern society and automatic collection. First, for many Americans, using a car is necessary to participate in society. Throughout much of the United States, a majority of Americans rely on driving — not only to commute to work but for all aspects of their lives. In fact, 87 percent of Americans use personal vehicles daily for shopping, errands, social visits, and recreational activities.[104]

Second, the generation of location data from vehicles with embedded GPS chips is unavoidable. Because GPS systems in vehicles can record data both when a car is started and periodically as it is driven, the only sure way to avoid leaving behind a trail of location data is to avoid using the car altogether.[105] Even then, some GPS systems collect data when a car is parked and turned off.[106] Moreover, similar to historical CSLI, GPS data from vehicles is usually collected without affirmative action on the part of the user.[107] Disabling an embedded GPS device in a car is difficult. The BBC profiled one car owner's attempts to disable the embedded GPS system in

his Volkswagen Golf and found that even after the owner — a security expert — physically disconnected the system's antenna, the car remained online due to 3G chips embedded in the dashboard.[108]

Lastly, GPS chips in smart cars also implicate retrospectivity. Like CSLI, they continuously generate data that can be recorded and retained, which means that law enforcement can trace a given individual's past whereabouts subject only to the retention policies of car manufacturers or their affiliates. Because the devices create a record that can be reviewed and analyzed at a later date, they run against everyone by creating an infallible record that allows the government to recreate almost anyone's past movements.

Under the *Katz-Carpenter* analysis, as informed by *Jones*, longer-term monitoring of GPS data from smart cars clearly constitutes a Fourth Amendment search requiring a warrant based on probable cause. Although shorter-term monitoring may be less comprehensive, it does not necessarily fall outside the ambit of the Fourth Amendment. The *Carpenter* Court indicated that no single factor is dispositive. Shorter-term monitoring similarly implicates intimacy, expense, retrospectivity, and voluntariness — suggesting that a warrant should still be required. Regardless of the duration of the surveillance, GPS technology in smart cars acts as a force multiplier, upending the traditional balance preserved by the Fourth Amendment by giving the government access to information that would otherwise be unknowable due to resource limitations or other constraints.

Reverse Location Searches: Tower Dumps and Geofence Searches

Reverse location searches are requests made by law enforcement for information on all the devices within a set area during a specific time period. The *Carpenter* Court reserved the question of whether its holding might be extended to tower dumps, a type of reverse location search that occurs when law enforcement requests the CSLI data connected to specific cell towers at a particular time.

Geofence searches are another, more insidious example of reverse location searches. They occur when law enforcement seeks GPS and other location information from devices within or near a designated area from companies like Google. Because tower dumps pull user data from one or a handful of identified towers, and each tower can handle only so many users, there is effectively a known upper limit on the geographic scope and number of people searched. By contrast, when Google receives a geofence request, the company searches all the users in its entire location history database. In follow-up requests, Google may then provide contextual location coordinates beyond the geofence area, such as showing where certain users moved before or after the original timeframe.[109] Reverse location searches can occur in other contexts as well — for example, when police seek to identify all the devices that connected to a particular Wi-Fi network.

Over the last several years, tower dumps and geofence searches have become increasingly popular with law enforcement.[110] Cell phone providers and technology companies reported thousands of such requests in 2019.[111] They are often supported only by a court order requiring a lower standard of suspicion than a warrant.[112] Whereas Apple has said that it cannot conduct reverse location searches because it does not maintain location records pertaining to its devices, Google stores geolocation records from Android phones and applications like Gmail, YouTube, and Google Maps in its Sensorvault database.[113] Google reported a 1,500 percent increase in geofence requests from 2017 to 2018 and a 500 percent increase from 2018 to 2019.[114] These types of searches are extremely cheap, costing law enforcement as little as $245 to retrieve data potentially on thousands of devices.[115]

Despite their popularity, reverse location searches remain of dubious efficacy. For example, after struggling to identify a suspect in a 2019 murder investigation in Phoenix, police requested location information from Google on all devices recorded as being near the crime scene while the crime was in progress. In part based on

data from Google's Sensorvault database, the police arrested Jorge Molina, whose Google account had registered his location as being near the crime scene. In fact, Molina was innocent; he had been home (along with his cell phone) when the crime occurred. It turned out that Molina's stepfather was the likely perpetrator of the crime. Molina had previously logged onto his Google accounts on his stepfather's phone, inaccurately linking his account to the device that Google reported was at the scene of the crime when it occurred. The collateral consequences of Molina's arrest based on faulty information from the reverse location search were colossal. After being arrested at work, Molina lost his job. His car was impounded for the investigation and then repossessed.[116] This case illustrates the risks of government overreliance on new technological tools for fighting crime.

The *Katz-Carpenter* model provides guidance on whether a warrant should be required, but a warrant alone may not solve the constitutionality issues presented by reverse location searches. The Fourth Amendment requires that warrants be based on probable cause and state with particularity the property to be searched or seized.[117] In some cases, law enforcement has obtained warrants for reverse location searches, called geofence warrants.[118] These warrants are by nature not specific or particularized. More traditional searches, like the one at issue in *Carpenter*, involve law enforcement asking for information about a specific device belonging to a specific suspect, whereas reverse location searches are designed to reveal geolocation data from hundreds to thousands of devices at once, with the understanding that the majority of those devices are owned and operated by people not suspected of any wrongdoing.[119] This essentially permits the government to work backward in identifying a suspect by requesting information on anyone within a set area during a given period of time.

Courts must consider the similarities between the dragnet surveillance facilitated by reverse location searches and the framers' concerns about general warrants. As Justice Gorsuch opined in his dissent in *Carpenter*: "Why isn't a tower dump the *paradigmatic* example of 'too permeating police surveillance' and a dangerous tool of 'arbitrary' authority — the touchstones of the majority's modified *Katz* analysis? On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?"[120]

Indiscriminate surveillance of the kind facilitated by reverse location searches threatens key tenets of an open democracy by chilling free speech and freedom of association and intruding on the right to privacy. Dragnet surveillance has historically been used, as the colonists experienced, to suppress dissent or opposition to the government. In their current iteration, reverse location searches share many of the same characteristics as the general writs reviled by the framers. They reveal intimate information not only about an individual suspect but also about the tens of thousands of other unsuspecting (and unsuspected) people nearby. For example, during a 2010 investigation, the FBI received information about more than 150,000 cell phone users in Denver when it used tower dumps to obtain information about four rural robbery locations.[121] This is akin to the government's searching through every single house in a neighborhood in order to uncover evidence of a crime. The Constitution — specifically the Fourth Amendment — protects against this type of mass surveillance.

The constitutionality of geofence warrants is currently being litigated in several cases, including *United States v. Chatrie*.[122] If these warrants are deemed unconstitutional, the government will have to cease issuing these requests entirely, unless it is possible for law enforcement to narrow the searches in a way that would allow them to establish particularity or probable cause — for example, by identifying a specific individual to be targeted and configuring the technology to minimize data collection by automatically filtering or discarding information not pertaining to that individual.

Most lower court decisions addressing reverse location searches since *Carpenter* have focused on whether to suppress evidence from warrantless tower dumps that occurred prior to the date of the *Carpenter* decision.[123]

However, two lower court decisions do give some indication of how courts have approached this issue in the wake of *Carpenter*. In both opinions, the courts discussed several of the *Katz-Carpenter* factors rather than resolving the cases on the basis of the Fourth Amendment's prohibition on dragnet surveillance.

In *United States v. Adkinson* (2019), the U.S. Court of Appeals for the Seventh Circuit upheld the FBI's warrantless acquisition of tower dump evidence during a robbery investigation. The court distinguished *Carpenter* on the basis of comprehensiveness and voluntariness: the FBI's search in *Adkinson* identified phones at one location at one period in time rather than over a period of days, and T-Mobile's terms of service with the defendant allowed it to disclose information to law enforcement in some contexts.[124] The Superior Court of Pennsylvania reached a similar conclusion in *Commonwealth v. Dunkins* (2020), upholding a reverse location search of a college's Wi-Fi network. The court noted that whereas "CSLI tracks an individual's movements at all times of the day regardless of where he travels, the Wi-Fi data in this case is only collected when an individual logs onto the campus wireless network and is present on . . . campus."[125] The court also found it persuasive that the defendant had voluntarily consented to the university's internet use policy when he signed onto the campus Wi-Fi network.[126]

Both the *Adkinson* and *Dunkins* decisions artificially narrowed *Carpenter*. In evaluating whether, as a whole, CSLI monitoring would upset the balance struck by the Fourth Amendment in facilitating too-permeating police surveillance, the *Carpenter* Court considered not only comprehensiveness and voluntariness but also expense, retrospectivity, and intimacy. If these other courts had considered these points, they likely would have reached a different conclusion.

Reverse location searches clearly implicate several elements of the *Katz-Carpenter* test. When it comes to expense, reverse location searches are far cheaper than traditional investigative tools.[127] Retrospectivity comes into play because they result in the procurement of historical geolocation data and encompass not just the suspected perpetrator's personal information but that of anyone within the identified catchment area (and often beyond) without any justification, notice, or remedy. The degree of intimate data revealed by a reverse location search is impossible to know in advance, but *Carpenter* recognized that monitoring someone's movements might expose their familial, political, professional, religious, and sexual associations.[128] Moreover, since reverse location searches rely on cell phone location information, they might pull data pertaining to someone's movements within a constitutionally protected space such as their home, implicating *Karo*.

Finally, the voluntariness analysis in *Adkinson* and *Dunkins* conflicts with *Carpenter*'s recognition that ubiquitous, modern technologies like Wi-Fi and cell phones are necessary for participation in modern society. Just as one cannot avoid the automatic conveyance of location data while using a cell phone, consenting to wireless carriers' standardized terms of service or using a Wi-Fi network as a college student is unavoidable. *Adkinson*'s and *Dunkins*'s conceptions of voluntariness misguidedly empower service providers to define the scope of an individual's constitutional rights through their terms of service.

As courts continue to consider how *Carpenter* applies to reverse location searches, they should engage fully with the breadth of the Court's decision and not take its reservation of decision on tower dumps as a determination that the Fourth Amendment does not apply. These searches threaten to tip the balance of government power because they facilitate dragnet surveillance, indicating that even a warrant cannot cure their constitutional defects and highlighting that the *Carpenter* decision itself is not a complete solution to the incongruities of modern Fourth Amendment jurisprudence.

Law Enforcement Surveillance Technologies

This section applies the *Katz-Carpenter* analysis to surveillance technologies used directly by law enforcement, including cell-site simulators, automated license plate readers, and drones. Since these technologies are either built or purchased by the government for its own use, they do not implicate the third-party doctrine or voluntariness. Nevertheless, to the extent that *Carpenter* provides guidance as to what should be considered an objectively reasonable expectation of privacy in the digital age, the remaining four factors that the *Carpenter* Court considered — intimacy, comprehensiveness, expense, and retrospectivity — are relevant to whether the Fourth Amendment requires law enforcement to obtain a warrant prior to using these technologies.

Cell-Site Simulators

A warrant should be required when law enforcement seeks to deploy cell-site simulators given the potential of this technology to greatly expand the government's surveillance power. The *Katz-Carpenter* factors should be viewed holistically, with an eye toward whether the technology upends the balance of power between the people and the government. Although cell-site simulators may implicate expense and comprehensiveness to a lesser extent than historical CSLI, many courts have required a warrant for their use. However, as with reverse location searches, to the extent that cell-site simulators are used to conduct dragnet surveillance, a warrant alone cannot cure the Fourth Amendment concerns.

Cell-site simulators imitate cell towers, appearing to nearby mobile phones as a preferred cell tower based on signal strength and prompting them to connect. Law enforcement generally uses them to identify all the cell phones within a given area in real time or to pinpoint the location of targeted suspects' phones.[129] Cell-site simulators are also known as Stingrays, triggerfishes, Digital Receiver Technology (DRT) boxes, and international mobile subscriber identity (IMSI) catchers.[130] The specific capabilities of a given cell-site simulator depend on the model; beyond collecting identifying information from nearby cell phones, some can identify an exact phone number, precisely locate a specific phone, or block cell service for all mobile phones within a particular area.[131]

Like many of the technologies discussed in this paper, the true prevalence of cell-site simulators is unknown. At least 75 law enforcement agencies in 27 states and the District of Columbia own cell-site simulators, but these numbers do not account for the fact that many agencies purchase and use the technology in secret.[132]

After a 2015 congressional investigation on cell-site simulators, several federal agencies updated their policies to require their agents to obtain warrants before deploying the devices.[133] The investigating committee's report recommended that Congress pass legislation to establish a clear, nationwide framework for when and how the technology can be used, but no federal law was ever passed. Under the Wiretap Act, law enforcement must obtain a warrant to use cell-site simulators to intercept the contents of a communication.[134] In other contexts, federal law is less clear. In this void, at least five states have passed legislation requiring a warrant for the use of cell-site simulators.[135]

Even before *Carpenter* was decided, several courts had required police to obtain warrants before using cell-site simulators.[136] For example, in *People v. Gordon* (2017), the Southern District of New York held that using a cell-site simulator constituted a search under the Fourth Amendment and thus required a search warrant, noting the sensitivity of the information collected by the devices, their accuracy in pinpointing cell phones' locations, and the fact that they can act as an instrument of eavesdropping if they collect information on call or text content.[137]

Other courts have reached similar conclusions post-*Carpenter*. For example, a Florida district court observed in *State v. Sylvestre* (2018) that use of a cell-site simulator would be even more invasive than the collection of CSLI — especially if phones were in private residences or in other private locations like "doctor's offices, political headquarters, and other potentially revealing locales."[138] However, courts have been reluctant to require a warrant for the use of cell-site simulators when the device was used to identify a phone number as opposed to an individual's location. For instance, in 2019 a Missouri district court determined that the limited use of a cell-site simulator to identify a defendant's cell phone rather than to track his location did not violate the Fourth Amendment.[139]

Cell-site simulators raise many of the same Fourth Amendment concerns under the *Katz-Carpenter* analysis as CSLI collection. Particularly when used to obtain information about devices within a specific area (as opposed to identifying an individual phone number), cell-site simulators implicate retrospectivity in several ways. First, they run against everyone: in addition to information about a given suspect, they sweep up data on bystanders not suspected of criminal wrongdoing, which can be retained by law enforcement for future use. Moreover, to the extent that they can stockpile data, they permit the government to travel back in time to survey individuals' movements or identify phone numbers even before the moment of suspicion.

Known instances of cell-site simulators being used at political rallies and protests, as well as to track suspects through the surveillance of a friend's or relative's home, evidence how this technology can also provide an intimate window into someone's life, revealing political or familial associations.[140] As computer scientist and legal scholar Jonathan Mayer testified to the House Committee on Science, Space, and Technology, "cell-site simulators can be particularly valuable when law enforcement officers are tracking a suspect indoors," which, recalling *Knotts* and *Karo*, calls into question the Fourth Amendment's heightened protections for traditionally private spaces like the home.[141]

Cell-site simulators differ most markedly from CSLI in terms of their comprehensiveness and expense. With respect to comprehensiveness, cell-site simulators can create a detailed and encyclopedic record of all the devices within a specific area, but they are limited in duration and scope. They log an individual device's presence within a given locality rather than the totality of its movements.

As to expense, cell-site simulators vary substantially in cost, ranging from tens of thousands to hundreds of thousands of dollars.[142] Many local police departments obtain funding for them through federal grants from the Department of Homeland Security, lessening the substantial budget impact.[143] Regardless of their upfront cost or who provides the funding, however, the fact remains that once purchased, cell-site simulators make surveillance remarkably efficient compared to traditional investigative tools. Law enforcement can collect information on tens of thousands of people at a time using a cell-site simulator, a breadth that would be all but impossible even with a large number of police officers engaging in manual surveillance.

Cell-site simulators illustrate how the factors in the *Katz-Carpenter* model should be viewed holistically, bearing in mind whether and how a technology affects the balance of power between the people and the government. Although expense and comprehensiveness may not be implicated to the same extent as with historical CSLI, many courts have nonetheless required a warrant for their use. As a Washington, DC, federal appeals court noted:

> Allowing the government to deploy such a powerful tool without judicial oversight would surely shrink the realm of guaranteed privacy far below that which existed when the Fourth Amendment was adopted. It would also place an individual in the difficult position either of

> accepting the risk that at any moment his or her cell phone could be converted into a tracking device or of forgoing necessary use of the cell phone.[144]

The Supreme Court resolved this same quandary in *Carpenter* by imposing a warrant requirement. It follows that under the *Katz-Carpenter* test, a warrant should be required for cell-site simulators as well, at least for their use in identifying the locations or movements of a given individual's device.

A warrant cannot resolve Fourth Amendment concerns when cell-site simulators are used for general, dragnet surveillance to collect the location data of a number of individuals. As with reverse location searches, there is no way for a warrant in such situations to meet the particularity requirement. Such a use should be banned entirely.

Automated License Plate Readers

Although automated license plate readers satisfy each of the *Katz-Carpenter* factors, most courts have declined to impose a warrant requirement for their use. This trend will likely change as ALPR systems become more sophisticated and pervasive.

ALPRs are high-speed camera systems, typically mounted on stationary poles or attached to police vehicles, that automatically scan or "read" the license plate of each vehicle that passes by. While the specific capabilities of ALPR systems vary, some can record up to 1,800 plates a minute.[145] In addition to providing real-time information to law enforcement agencies about each vehicle scanned, ALPR systems can also upload plate numbers, along with the location, date, and time of the scan, to a central, searchable database, generating a repository of historical records.[146] Sometimes additional information is recorded, including the make and model of the vehicle, photos of the outside of the vehicle including bumper stickers or other distinguishing details, or photos of the driver and passengers.[147]

ALPR data can be used for a variety of purposes — assessing tolls on roads or bridges, locating a particular vehicle in real time, determining where a vehicle has been in the past, or identifying vehicles known to be stolen or connected with outstanding warrants.[148] Low-income communities and communities of color, which have historically been subjected to overpolicing, are often disproportionally subjected to ALPR surveillance.[149] In some cities, law enforcement officers are known to "grid" certain neighborhoods, meaning they drive up and down every street using mobile ALPRs to indiscriminately record information on each vehicle for use in future investigations.[150]

Law enforcement agencies frequently share ALPR databases.[151] Some ALPRs are also owned and operated by private individuals or businesses, who may choose to share the data collected with law enforcement or use it for other purposes, such as landlord-tenant issues or private investigations.[152] Immigration and Customs Enforcement, a component of the Department of Homeland Security, routinely accesses a database of more than 6 billion ALPR records amassed by private businesses and local law enforcement agencies.[153]

ALPR systems are exceptionally commonplace. According to one report, in 2016 and 2017, 173 law enforcement agencies collectively scanned 2.5 billion license plates.[154] At least 16 states have statutes regulating the use of ALPRs.[155] Jurisdictions vary in terms of retention policies for ALPR data. For instance, New Jersey permits ALPR data to be retained for five years, whereas Maine requires that data be deleted after 21 days.[156]

Courts have been reluctant to curtail the installation of ALPRs and have regularly held that law enforcement can, without any suspicion of criminal activity, perform at least an initial check of a given license plate against a

database.[157] However, ALPR systems potentially raise constitutional concerns at several points throughout their use, including at the time of installation, during data collection, while comparing an individual license plate against a database, and during data analysis or monitoring.[158]

The use of ALPR systems clearly touches on the *Katz-Carpenter* factors. First, even though they track license plates, which are by design displayed prominently and publicly on all vehicles, ALPRs can reveal intimate information about a given individual. For example, ALPRs were infamously used by the New York City Police Department to identify Muslim worshippers at mosques in the surrounding metropolitan area.[159] ALPR systems have also been used to track all the cars entering or leaving a town and could be used to identify vehicles at a protest.[160] Although ALPR systems generally do not record as many individual data points as a GPS, the information that they do collect can be just as revealing.[161] Even discrete or short-term monitoring of ALPR data can reveal personal, possibly intimate information, like trips to a psychiatrist or criminal defense attorney. In one instance, reporters were able to identify the block where a city council member lived after less than a minute of research using ALPR data from the Oakland Police Department.[162]

Moreover, the records that networked ALPR cameras generate can be comprehensive. As the concurring justices explained in *Jones*, monitoring a car's movements can impinge on reasonable expectations of privacy, regardless of whether those movements were disclosed to the public at large.[163] Even less sophisticated networks of ALPR cameras can create a detailed record of a vehicle and its driver's movements, potentially revealing habits and patterns ranging from someone's commute to work to where they stop for breakfast in the morning to whom they visit in the evening. For example, investigative reporting on one private ALPR system revealed that searches of license plates from vehicles in large cities might reveal granular details about the vehicle's movements on highways, smaller streets, and specific neighborhoods, as well as addresses where the vehicle was identified. The ALPR system mapped this information, creating an accessible and detailed record of the vehicle's past location history (which also touches on retrospectivity).[164] The data from ALPR systems encompassing greater numbers of cameras will be even more comprehensive; law enforcement systems are likely among the more expansive and sophisticated.

ALPRs make it easy and inexpensive for the government to accumulate and analyze vast amounts of data. *Carpenter* requires courts to look ahead, toward where technology is evolving.[165] As ALPRs become more commonplace, law enforcement will conceivably be able to survey all vehicles on a public road at very little cost.[166] This capacity would fundamentally upend the traditional balance struck by the Fourth Amendment in limiting excessively pervasive government surveillance. As Justice Sotomayor observed in her *Jones* concurrence, "society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual's car for a very long period."[167]

ALPR data implicates the retrospectivity element of the *Katz-Carpenter* analysis in two ways. First, ALPR systems run against everyone because they collect information indiscriminately about every vehicle that passes by, regardless of suspicion of criminal activity. Second, as mentioned above, the information collected by ALPR devices is stored in databases that can be accessed later by law enforcement, meaning that the police do not need to know in advance if they want to follow an individual. The latter concern might be addressed by limitations on the retention of data collected by ALPRs, but the former is unavoidable. By design, ALPRs are intended to surveil and collect data about the general public, sweeping up millions of innocent people in their dragnet surveillance. In fact, audits of ALPR systems in Northern California, New York, and North Carolina revealed that more than 99 percent of data collected pertained to people not suspected of wrongdoing. As with

reverse location searches and cell-site simulators, to the extent that ALPRs are used to conduct dragnet surveillance, a warrant will not remediate the constitutional concerns posed by the technology.

Notwithstanding the relevance of the *Katz-Carpenter* framework to ALPRs, most courts that have addressed them so far have declined to impose limitations on their use. Prior to *Carpenter*, several courts had upheld their use by law enforcement.[168] Of those courts to address ALPR surveillance in the wake of the decision, most have either sidestepped the issue or declined to extend *Carpenter*'s reasoning given the limited scope of the ALPR search at issue.[169]

Still, ALPRs clearly raise many of the same concerns that the Court considered in *Carpenter*. This is exemplified by a concurring opinion in the Ninth Circuit Court of Appeals case *United States v. Yang*, in which Judge Carlos Bea observed:

> 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.[170]

As ALPRs become ever more ubiquitous, it will become increasingly difficult for courts to distinguish ALPRs from GPS or CSLI monitoring, especially when ALPRs are used to surveil individuals' movements over a longer period using either historical or real-time data. Although courts have not yet required a warrant for ALPR monitoring, this will likely change in the future as ALPR systems become more commonplace, in turn giving rise to more comprehensive and deeply revealing databases.

Surveillance Drones

Drones clearly implicate the *Katz-Carpenter* factors, suggesting that a warrant should be required for their use. However, prior Supreme Court precedent upholding other forms of warrantless aerial surveillance muddles the application of *Carpenter* to this technology.

A drone is an unmanned aircraft that is piloted either remotely or autonomously, guided by a remote control or via integrated computer sensors.[171] There are hundreds of different drone models and they vary widely in size, intended use, and functionality. Some resemble airplanes, while others fly using spinning rotors, like a helicopter.[172] Drones may be as large as a Boeing 737 jetliner or as minute as the Pentagon's "Nano Hummingbird," which weighs less than a AA battery.[173]

Smaller, multirotor commercial drones are popular with both recreational users and domestic law enforcement.[174] Whereas larger military drones can cost $150 million each, commercial drones are much less expensive; common models used by law enforcement agencies start at $700.[175] They are often equipped with sophisticated surveillance features, such as high-definition cameras, live-feed video, infrared cameras, heat sensors, powerful zoom capabilities, GPS, time-stamping, and obstacle sensors.[176] A number of commercial drones also have autopilot capabilities that allow users to continually film one target.[177] Some drones allow operators to track targets over 65 square miles.[178] Others contain license plate readers.[179]

Government-owned drones are used by law enforcement in every state.[180] Law enforcement agencies acquire them through donations, federal grants, seizure, or the regular budgeting process.[181] Drones have been deployed to surveil crime scenes, assist in hostage situations, and aid in search-and-rescue operations, among other tasks.[182] The technology also allows for large-scale surveillance — particularly of big events like protests.

Like reverse location searches, warrantless drone surveillance makes possible pervasive, dragnet surveillance that threatens civil liberties. Drone surveillance by nature runs against everyone within a broad geographical area. Indeed, mass warrantless drone surveillance became commonplace across the United States during the 2020 protests following the killings of George Floyd and Breonna Taylor, with the plausible effect of suppressing or intimidating protestors exercising their First Amendment rights.[183] Whether drone data can be restricted to a particular target — thereby avoiding the issue of general warrants — is unclear.

A series of U.S. Supreme Court cases upholding airplane and helicopter surveillance have made Fourth Amendment challenges to drone surveillance difficult. In *California v. Ciraolo* (1986), the Court held that aerial observations of a backyard from publicly navigable airspace did not constitute a search under the Fourth Amendment.[184] Similarly, in *Florida v. Riley* (1989), the Court found that the use of a helicopter flown at 400 feet to see inside a suspect's greenhouse did not violate his reasonable expectation of privacy. Since the helicopter was in publicly navigable airways and flying according to regulations, the Court reasoned that "any member of the public" could have flown in that location.[185] Finally, in *Dow Chemical Co. v. United States* (1986), the Court held that warrantless use of aerial mapping cameras did not violate the Fourth Amendment for analogous reasons.[186]

However, modern drone surveillance is markedly different than the targeted aerial surveillance at issue in these cases from the 1980s. No longer are police flying once or twice over a suspect's backyard looking for evidence of a specific crime. Rather, modern drone programs — like one recently piloted by the Baltimore Police Department in conjunction with a private company — allow for continuous monitoring of entire cities and specific individuals all at once.[187] A panel of the U.S. Court of Appeals for the Fourth Circuit recently upheld the Baltimore program, citing *Ciraolo*, *Riley*, and *Dow*.[188] The decision distinguished *Carpenter* on the basis of supposed technical differences between drones and historical CSLI relating to the duration of surveillance, ease of use, and ability to identify individuals.[189] These arguments were significantly undermined by an external audit and the chief justice's dissenting opinion.[190] The Fourth Circuit has agreed to rehear the case en banc, indicating that it may be looking to reverse the original decision.[191]

Drones certainly touch on the *Katz-Carpenter* factors. They can easily provide an intimate window into a person's life given their ability to record video and track a target in real time.[192] Their extensive use at protests speaks to their capacity to expose a person's political associations. Drone surveillance might also reveal an individual's professional, religious, or sexual associations — particularly if used to capture footage of office buildings, religious areas, or LGBTQ+ bars, for example. Some law enforcement drones even have infrared cameras with the ability to capture images through walls, posing additional privacy risks to traditionally private spaces like the home and implicating *Karo*.[193]

Though it depends on how they are deployed, drones can also create detailed records that allow for the comprehensive tracking of someone's movements. Drones are frequently used to monitor or track suspects and can be used to facilitate the prolonged virtual observation of a target or building.[194]

Drone technology also has become cheap and efficient to use. Modern commercial drones cost only hundreds to a few thousand dollars.[195] While they may entail costs for maintenance and personnel training, as unmanned surveillance devices they are less difficult to use and less costly than traditional tracking methods.[196] In fact, a recent Department of Justice report revealed that most agencies found the use of drones to be cost-effective in the long run, especially compared to other aerial surveillance options like helicopters.[197]

Lastly, drones also implicate retrospectivity. They record video footage, images, and sensor data about everyone within their purview that can be accessed and analyzed after the fact. This means they both run against everyone and permit the government to travel virtually back in time.

Drones highlight the inherent complications in applying *Carpenter* to technologies addressed by the Court at a time when the tools available were less sophisticated than they are today. Decisions like *Ciraolo*, *Riley*, and *Dow* that upheld warrantless aerial surveillance in other contexts may make it difficult for lower courts to conclude that a warrant should be required for drone surveillance. That being said, those three aerial surveillance cases were each decided more than 30 years ago, when drone technology was not yet as advanced as it is today.

Moreover, the legislative landscape has changed: at least 18 states now require law enforcement to obtain a search warrant to use drones for surveillance or to conduct a search in various circumstances.[198] To the extent that *Carpenter* exemplifies the Court's reluctance to uncritically extend existing precedents, the Court might reach a different conclusion should it review a drone case today. Drones clearly implicate the *Katz-Carpenter* factors, suggesting that a warrant should be required for their use.

Data from Other Technologies

In an increasingly digital world, we rely on commercial technologies to assist us with a variety of tasks, from tracking our heart rates to monitoring who comes to our door. These technologies enable third parties to collect and store many kinds of sensitive information. This section discusses *Carpenter*'s application to the data generated by commercial technologies, including wearables like Fitbit and Apple Watch and smart doorbells such as Ring.

Body-Worn Technologies

If the *Carpenter* decision sits at the intersection of two lines of Fourth Amendment cases — those addressing location and the third-party doctrine — then cases on body-worn technologies are at the intersection of three. To wit, they complicate the Fourth Amendment analysis further because they center on particularly sensitive types of data: information from inside the home and health information. These were granted heightened constitutional protections by the Court in *Karo* and in *Ferguson v. City of Charleston* (2001).[199] Whereas in *Karo* the Court reaffirmed protections for information originating inside the home, in *Ferguson* the Court declined to extend the third-party doctrine to diagnostic medical tests. Both cases suggest that a warrant should be required for police to access information from body-worn technologies, also called wearables or activity trackers. *Carpenter* buttresses this conclusion, even though data from wearables is typically held by third-party companies.

Wearables are often advertised as tools for staying fit, monitoring health, providing navigation assistance, or improving communication. In the course of providing these services, wearables continuously collect information on a variety of data points ranging from a user's heart rate to distance traveled and location. This

process generates a detailed record of a user's location history in addition to other personal data, including medical information and a history of physical activity. This information is often stored locally before being transmitted to a cloud server.[200]

Body-worn technologies touch on each of the five *Katz-Carpenter* factors. With respect to intimacy and comprehensiveness, the sensitive data generated by body-worn technologies implicates many of the same concerns that CSLI did in *Carpenter*. For example, the integrated GPS in Fitbit and Apple Watch devices records a user's location by the minute. These devices also collect other deeply personal information, including medical metrics like heart rate, temperature, movement history, and sleep stages.[201] This trove of information not only creates a comprehensive picture of someone's physical location at any given point in time but also allows inferences to be drawn about someone's health, affiliations, emotions, and activities. For instance, an elevated heart rate and temperature might indicate stress or nervousness; in other contexts, temperature data might reveal sensitive information about a user's reproductive status. Moreover, some devices also collect information regarding the user's proximity to other tracked individuals. Combined with demographic information, this data can provide intimate details about individual interactions and give rise to near-perfect surveillance.[202]

Like cell-site location information, wearables also touch on retrospectivity, though the analysis will depend on the retention policies of the party from which the records are being sought. Most body-worn technologies generate a detailed record of data about users that can be stored for long periods of time and accessed retroactively. For instance, Apple Watch content backs up automatically to a user's companion iPhone or iCloud account.[203] Fitbit records are stored indefinitely on company servers.[204] These caches enable law enforcement agents to go back in time and collect information from before the first moment of suspicion, providing access to data that would likely otherwise be unknowable. Additionally, body-worn technologies make surveillance inexpensive and efficient compared to traditional investigative techniques.[205]

In the future, wearables might become as commonplace as cell phones, but for now their use is certainly voluntary. An Apple Watch is arguably not like a cell phone or car because it is not such a pervasive and insistent part of daily life that its use is difficult to avoid. However, in determining that CSLI was not truly shared voluntarily, the *Carpenter* Court considered not only the indispensability of cell phones to participation in modern life but also that they generated location information automatically. As discussed above, many body-worn technologies similarly generate and retain information automatically.

Law enforcement has accessed data from body-worn technologies during criminal investigations in several documented instances. However, often this data was derived from devices belonging to the victim rather than the alleged defendant and was used to determine the victim's location or, based on a device's heart rate tracker, the time of death.[206] As such, there has been little litigation on whether a warrant is required for the government to obtain data from wearables. Even so, in several of the most prominent investigations involving data from wearables, the police did obtain a warrant to access the data.[207] *Carpenter*'s reasoning underscores the appropriateness of a warrant: data collected by body-worn technologies is sensitive and comprehensive, and these tools create a retrospective record that is relatively easy and inexpensive for the government to access.

Smart Doorbells

It is less clear how smart doorbells like Amazon's Ring or Google's Nest Hello fit into the *Katz-Carpenter* analysis. This is because smart doorbells generally capture information from outside rather than inside the home, and they hew closely to more traditional surveillance tools like security cameras. In addition, they record

information about a specific area rather than the whole of a person's movements, and they may implicate the Court's prior cases on curtilage since they capture footage of the area immediately surrounding a home.

Smart doorbells are connected to the internet and are designed to be affixed to an outside door. They activate when they detect motion nearby or when someone presses the doorbell. The device then notifies the user. In some models, built-in speakers allow the user to respond to a visitor in real time. Ring and Nest Hello are two commonly used smart doorbells. For a monthly fee, Ring users can sign up for video recording and photo capture capabilities.[208] Users are also automatically enrolled in a free application called Neighbors, which allows them to submit footage to law enforcement or upload it online; it also provides information to users about crimes in their area.[209] The Nest Hello can record and store video footage, and Google's cloud service can even use facial-recognition software to learn to identify visitors.[210]

While the Court has previously recognized that people have a legitimate expectation of privacy in the area immediately surrounding their home, traditionally called the curtilage, the Court has typically afforded greater constitutional protections against physical intrusions compared to surveillance not involving a trespass.[211] To the extent that *Carpenter* demonstrates the Court's willingness to revisit the harms of nonphysical surveillance, technologies like smart doorbells may push the Court to consider extending Fourth Amendment protections further.

Of all the technologies discussed herein, smart doorbells are the most different from CSLI in their comprehensiveness. By design, they record movements within a set geographical area rather than tracking the totality of a person's movements. They will not reveal to the government someone's entire location history. However, they do provide near-perfect surveillance of an individual's comings and goings from wherever they are affixed through the creation of detailed and encyclopedic records. Moreover, when viewed in conjunction with other nearby devices, the data generated by smart doorbells may provide police with comprehensive information about a given neighborhood or locality.[212]

Smart doorbells equipped with recording features clearly implicate retrospectivity. They effectively allow the government to look back in time by generating records free of the frailties of human memory that are commonly retained by providers for sustained periods of time. Ring users, for example, can select data plans that provide 60 days or more of recorded video storage. A user can share videos via a share link or by posting to the Neighbors app, and the videos may remain online indefinitely.[213] Furthermore, because smart doorbells can also record information about passersby's comings and goings, they have the potential to run against everyone — effectively blanketing certain neighborhoods with surveillance cameras. The greater the housing density, the more likely it is that a neighborhood resident will be caught on film, whether by their own camera or a neighbor's.

When it comes to expense, smart doorbells make surveillance easy and efficient by allowing the government to access and even conduct surveillance continuously for long periods at almost no cost. For instance, Ring's Neighbors Public Safety Service portal is free for law enforcement; it allows agencies to see community posts from the neighborhoods they police and to request footage from users.[214] In some cases, smart doorbell owners can choose to give law enforcement permission to access video footage from their doorbell cameras in real time.[215]

Depending on how they are used, smart doorbells can also give the government an intimate window into the privacies of someone's life. A smart doorbell might offer a complete picture of its user's comings and goings from one of their most private spaces — their home — as well as information about their associations.[216]

Moreover, a smart doorbell affixed somewhere like an abortion clinic, methadone clinic, or religious site (or a building nearby) could facilitate the monitoring of the general public's visits to sensitive locations. Smart doorbells can also be used to track First Amendment–protected activity, as exemplified by reports that the Los Angeles Police Department (LAPD) requested that Ring users submit footage of Black Lives Matter protestors. The LAPD is one of at least 2,000 public safety agencies with a formal partnership with Ring.[217]

The issue of voluntariness is complicated by the fact that smart doorbells must be installed proactively by users. Courts considering the application of the *Katz-Carpenter* analysis to smart doorbells will have to weigh these two considerations: the voluntary adoption of the technology relative to the potential for passive data sharing. In cases where smart doorbells are used to track the movements of individuals other than the owner, voluntariness is vitiated entirely; members of the public have no control over whether their public movements might be captured by a device affixed to a private home and then shared with law enforcement.

The broad principles that the Court articulated in *Carpenter* around protecting the privacies of life against arbitrary power and upholding the framers' central aim to constrain a too-permeating police surveillance are certainly relevant to a Fourth Amendment analysis of smart doorbells.[218] However, it is less clear how helpful the *Katz-Carpenter* test will be in evaluating whether a warrant should be required for the police to access the data generated by this particular technology. The answer will depend on how much weight courts give the factors of comprehensiveness, retrospectivity, and intimacy and on the identity of the subject of the investigation — whether it is the owner, who voluntarily installed the camera, or another individual, who did not.

Internet Browsing History

In his dissent in *Carpenter*, Justice Kennedy raised the question of whether the Court's holding should be applied to information like web browsing histories.[219] The likely answer is yes.

A user's internet browsing history is a detailed record of recently visited web pages, including information such as page title and time of visit. A variety of entities collect browsing histories, including internet service providers (ISPs), search engines, and web browsers like Google Chrome and Apple's Safari.[220] In addition, most websites can track users through the placement of cookies, which record information about user visits and activities.[221]

Of all the technologies discussed in this paper, perhaps none implicates intimacy as readily as search histories. People type into their preferred search engine questions about everything from politics to medical concerns. Internet browsing histories can reveal someone's sexual orientations, reading habits, and more or run the risk of misleading the observer about an individual who is searching on behalf of another. As Professor Paul Ohm explained in testimony before Congress:

> The list of websites an individual visits, available to a [broadband internet access service] provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.[222]

Besides their general breadth, web browsing histories when aggregated can facilitate the drawing of inferences that might not otherwise have been apparent, such as changes in a user's mental health or an evolution in their political viewpoint.

In addition to intimacy, search histories also implicate the other factors that the Court considered in *Carpenter*. Because many companies retain data on user browsing histories for long periods of time, it is possible for law enforcement to access and analyze historical data, creating the same kind of retrospective time machines about which the *Carpenter* majority warned.[223] For example, Google — which processed more than 12.4 billion search queries in the United States in October 2020 alone — stores records of user search histories and only recently announced that it would allow users to set a time limit on retention of their data.[224]

It is also relatively inexpensive and efficient for law enforcement to access web browsing histories through tools like keyword warrants, which are requests for information on every person who searched for a specific term.[225] Like reverse location searches, keyword warrants are of dubious constitutionality. Police do not need particularized suspicion of a given individual or place to be searched to obtain one; rather, these general warrants are essentially a form of indiscriminate mass surveillance, the very harm the framers intended the Fourth Amendment to address. The potential civil rights harms of arresting or targeting someone for investigation based on something they searched online are immense.

Regarding comprehensiveness, web browsing histories are also detailed, encyclopedic, and effortlessly compiled with respect to the types of data described by Professor Ohm above. However, the analysis is more nuanced when it comes to location data specifically. Though search histories and IP addresses can be used to gain insight into someone's location — such as when Google received a keyword warrant requesting information on all users who had searched the address of a particular residence in an arson investigation — they generally provide a less complete record of someone's movements than historical CSLI.[226]

Internet browsing data is not truly shared voluntarily as the term is normally understood. Like cell phones, the internet is so indispensable to participation in modern society that it is difficult to avoid its use.[227] Moreover, the collection of data incidental to internet searches is automatic and inescapable. Even when individuals use more privacy-protective search engines, like DuckDuckGo, all internet traffic still passes through their ISPs, which can record browsing histories, including the domain names of websites visited.[228]

Most cases to address law enforcement's access to internet browsing history involve the search of a physical device already in the government's possession. For example, in *United States v. Okparaeke* (2018), the Southern District of New York held that the internet browsing history on the defendant's cell phone, which was already in police custody, fell within the scope of the search warrant that police had obtained for any electronically stored information on the device.[229] The court denied the defendant's motion for reconsideration and to suppress evidence. While judges have signed orders for keyword warrants, the constitutionality of these relatively new types of searches has yet to be fully litigated.

Whereas the third-party doctrine may in the past have dealt a fatal blow to Fourth Amendment protections for internet browsing histories, *Carpenter* changes that. The deeply revealing nature of search histories, their retrospective qualities, their efficiency and low cost to law enforcement, and the fact that the internet is indispensable to modern life all suggest that the nature of this data is clearly enough to overcome third-party doctrine privacy considerations — and enough to necessitate a warrant for police to access this information.

Conclusion

As technological advances have fundamentally changed what society views as private and how we store information, it has become exponentially easier and cheaper for the government to obtain vast amounts of data about each of us. Given this context, *Carpenter* should be read broadly as reimagining what a reasonable expectation of privacy in the digital age is.

In finding that individuals may retain a reasonable expectation of privacy in information shared with third parties and in their public movements, *Carpenter* revises the Fourth Amendment analysis for all modern technologies and the records they generate, not just cell-site location information. As the above analysis indicates, the five-factor *Katz-Carpenter* framework suggests that in the wake of *Carpenter*, a warrant should be required to access a range of data, such as that collected by GPS, ALPRs, and body-worn technologies.

It remains to be seen how *Carpenter* will shape the future of Fourth Amendment jurisprudence. As the Court noted, however, the Fourth Amendment enshrines a central aim of the framers — to preserve the balance of power between the people and the government.[230] Modern-day technologies facilitate surveillance so permeating that it would be unrecognizable to the founding fathers. As courts grapple with these issues, they must recognize the power of technology to profoundly destabilize the balance of power between people and government and the Fourth Amendment's vital role in preventing government encroachment.

About the Author

Laura Hecht-Felella is the George A. Katz Fellow with the Brennan Center's Liberty and National Security Program. She focuses on issues related to civil rights and technology, as well as content moderation and online speech. Prior to joining the Brennan Center, Laura was an attorney at Brooklyn Legal Services, where she represented low-income New Yorkers in litigation seeking to prevent displacement and preserve affordable housing. Previously, she worked on reproductive justice issues at National Advocates for Pregnant Women. She is a graduate of the Macaulay Honors College of the City University of New York and New York University School of Law.

Acknowledgments

The Brennan Center gratefully acknowledges The Bauman Foundation, CS Fund/Warsh-Mott Legacy, Herb Block Foundation, Media Democracy Fund, and Open Society Foundations for their generous support of our work.

Many people assisted with the development of this paper. The author would like to express her gratitude to the Brennan Center's Rachel Levinson-Waldman and Liza Goitein for their guidance, insightful comments, and careful revisions, as well as Kaylana Mueller-Hsia and Sahil Singhvi for their attention to detail in fact-checking the report. The author is also grateful to Laura Reed and Lisa Femia for their research assistance. She greatly appreciates the guidance and support of Michael Waldman and John Kowal. She also thanks Orin Kerr, Paul Ohm, Barry Friedman, Nate Wessler, Michael Price, and Jumana Musa for their invaluable review of a draft of this report and for their thoughtful feedback and subject matter expertise. The Brennan Center's communications team, especially Alden Wallace, Yuliya Bas, Matt Harwood, Jeanne Park, and Zachary Laub, provided critical support in readying this research for publication and ensuring the report's successful launch.

Endnotes

[1] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[2] *Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
[3] U.S. Const. amend. IV. In most instances, failure to comply with the warrant requirement can only be excused by exigent circumstances or other exceptions that do not apply to the scenarios described in this paper.
[4] Boyd v. United States, 116 U.S. 616, 625–26 (1886) (noting that this experience was "fresh in the memories of those who achieved our independence and established our form of government.").
[5] United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990); and *Boyd*, 116 U.S. at 625.
[6] Stanford v. Texas, 379 U.S. 476, 484 (1965) (quoting Marcus v. Search Warrant, 367 U.S. 717, 729 (1961)) (noting that the Bill of Rights was "fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression.").
[7] Ker v. California, 374 U.S. 23, 47 (1963).
[8] Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Berger v. New York, 388 U.S. 41 (1967), *and overruled in part by* Katz v. United States, 389 U.S. 347 (1967).
[9] *Katz*, 389 U.S. at 351–53 (1967) ("The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").
[10] *Katz*, 389 U.S. at 353.
[11] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[12] Smith v. Maryland, 442 U.S. 735, 744 (1979); and United States v. Miller, 425 U.S. 435, 442–44 (1976).
[13] Given the limitations in constitutional law, Congress has enacted several regulations to protect data privacy. These include the Children's Online Privacy Protection Act (1998), the Health Insurance Portability and Accountability Act (1996), and the Electronic Communications Privacy Act (1986). However, there is no comprehensive statutory scheme with respect to how third parties must protect data. See, e.g., Stephen P. Mulligan and Chris D. Linebaugh, *Data Protection and Privacy Law: An Introduction*, Congressional Research Service, May 9, 2019, https://crsreports.congress.gov/product/pdf/IF/IF11207.
[14] In *Miller*, the Treasury Department's Alcohol, Tobacco, and Firearms Bureau used a subpoena to obtain the defendant's records from two banks where he maintained accounts. *Miller*, 425 U.S. at 437.
[15] *Smith*, 442 U.S. at 744–46.
[16] *Smith*, 442 U.S. at 749–50 (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice. . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.").
[17] United States v. Knotts, 460 U.S. 276 (1983).
[18] *Knotts*, 460 U.S. at 281–83.
[19] United States v. Karo, 468 U.S. 705, 716 (1984).
[20] *Knotts*, 460 U.S. at 283.
[21] Florida v. Riley, 488 U.S. 445 (1989).
[22] Kyllo v. United States, 533 U.S. 27, 40 (2001).
[23] *Kyllo*, 533 U.S. at 36.
[24] *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34).
[25] Generally, warrantless searches of an arrestee's person and his or her immediate physical possessions are permitted under an exception to the Fourth Amendment. This exception is premised on the "heightened government interests at stake in a volatile arrest situation," as well as "an arrestee's reduced privacy interests upon being taken into police custody." Riley v. California, 573 U.S. 373, 391 (2014).
[26] *Riley*, 573 U.S. at 385, 393.
[27] *Carpenter*, 138 S. Ct. at 2210 ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." (quoting *Riley*, 573 U.S. at 385)).
[28] United States v. Jones, 565 U.S. 400 (2012).
[29] *Jones*, 565 U.S. at 401.
[30] *Jones*, 565 U.S. at 413 (Sotomayor, J., concurring); and *Jones*, 565 U.S. at 418 (Alito, J., concurring).
[31] *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).
[32] *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).
[33] *Carpenter*, 138 S. Ct. at 2211–12.
[34] *Carpenter*, 138 S. Ct. at 2218 (noting that "[w]hile carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections").
[35] Stored Communications Act of 1986, 18 U.S.C. § 2703(d).
[36] *Carpenter*, 138 S. Ct. at 2211–12.
[37] *Carpenter*, 138 S. Ct. at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.").
[38] *Carpenter*, 138 S. Ct. at 2218.
[39] *Carpenter*, 138 S. Ct. at 2217 ("We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").
[40] *Carpenter*, 138 S. Ct. at 2220.

[41] *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting) ("Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process."); and *Carpenter*, 138 S. Ct. at 2257 (Alito, J., dissenting) ("Carpenter did not create the cell-site records. Nor did he have possession of them; at all relevant times, they were kept by the providers. Once Carpenter subscribed to his provider's service, he had no right to prevent the company from creating or keeping the information in its records.").
[42] *Carpenter*, 138 S. Ct. at 2236 (Thomas, J., dissenting) ("The more fundamental problem with the Court's opinion, however, is its use of the 'reasonable expectation of privacy' test, which was first articulated by Justice Harlan in *Katz v. United States*, 389 U.S. 347, 360–61, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967) (concurring opinion). The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law."). See also *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) ("I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only Katz-squared. Returning there, I worry, promises more trouble than help. Instead, I would look to a more traditional Fourth Amendment approach.").
[43] *Carpenter*, 138 S. Ct. at 2214 (first quoting *Boyd*, 116 U.S. at 630; then quoting *Di Re*, 332 U.S. at 595).
[44] *Carpenter*, 138 S. Ct. at 2266 (Gorsuch, J., dissenting).
[45] In his dissent in *Carpenter*, Justice Kennedy identified intimacy, comprehensiveness, expense, retrospectivity, and voluntariness as the relevant components of the majority's multifactor analysis in determining whether a Fourth Amendment search has occurred. *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting). Even prior to *Carpenter*, several of these factors were already emerging as particularly relevant to the Court's application of the Fourth Amendment to digital age public surveillance technologies. See, e.g., Rachel Levinson-Waldman, "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public," *Emory Law Journal* 66 (2017): 530 ("Existing case law, seen through a new lens, provides the blueprint for a workable, comprehensive mechanism for applying the Fourth Amendment to digital age public surveillance technologies. This approach aggregates factors courts have already identified as relevant to their Fourth Amendment analysis, but in an ad hoc manner, and transforms them into a more rigorous, replicable approach. These factors are (1) the duration of the surveillance; (2) the lowering of structural barriers to pervasive surveillance, reflected in the greatly reduced cost of tracking; (3) the recording of an individual's or group's movements; (4) the elicitation of information from within a protected space such as a home; and, as appropriate, (5) whether the technology undermines core constitutional rights and (6) whether surveillance technologies are piggy-backed on each other.").
[46] *Carpenter*, 138 S. Ct. at 2218, 2216.
[47] *Carpenter*, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring)).
[48] *Carpenter*, 138 S. Ct. at 2217n3 ("[W]e 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 purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").
[49] *Carpenter*, 138 S. Ct. at 2217.
[50] *Carpenter*, 138 S. Ct. at 2214 (quoting *Boyd*, 116 U.S. at 630).
[51] *Carpenter*, 138 S. Ct. at 2218.
[52] *Carpenter*, 138 S. Ct. at 2220.
[53] *Carpenter*, 138 S. Ct. at 2218.
[54] *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).
[55] *Carpenter*, 138 S. Ct. at 2218.
[56] Paul Ohm, "The Many Revolutions of *Carpenter*," *Harvard Journal of Law & Technology* 32 (2019): 367 (noting that the metaphor of police access to historical data as time travel was first proposed by legal scholar Stephen Henderson).
[57] *Carpenter*, 138 S. Ct. at 2218, 2219.
[58] *Carpenter*, 138 S. Ct. at 2223.
[59] *Carpenter*, 138 S. Ct. at 2220.
[60] *Carpenter*, 138 S. Ct. at 2220 (citing *Riley*, 573 U.S. at 385).
[61] *Carpenter*, 138 S. Ct. at 2218 (citing *Riley*, 573 U.S. at 385).
[62] This approach echoes Orin Kerr's theory of equilibrium-adjustment, which posits that the Supreme Court adjusts the scope of protection in response to new facts in order to restore the status quo level of protection. Orin S. Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," *Harvard Law Review* 125 (2011): 476.
[63] Compare Barry Friedman, "The Worrisome Future of Policing Technology," *New York Times*, June 22, 2018, https://www.nytimes.com/2018/06/22/opinion/the-worrisome-future-of-policing-technology.html ("The growing use of technology by law enforcement agencies to monitor or target people — particularly people and communities of color — is expanding at head-spinning speed, and nothing the courts do is going to stop that . . . [the chief justice's] opinion didn't overturn the rule that says that any time the government wants information on you that you've provided to a third party, the government can get it, even though in the digital age most of your information is now in the hands of third parties . . . ") with Ohm, "Many Revolutions of *Carpenter*," 358 ("*Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more."); and Orin S. Kerr, "Implementing *Carpenter*," in *The Digital Fourth Amendment* (Oxford: Oxford University Press, forthcoming), 1, https://papers.ssrn.com/abstract_id=3301257 ("More importantly for us, by presenting the facts as they did, the Court laid the groundwork for the similar treatment of digital technologies present and future that genuinely raise the concerns the Justices expressed in *Carpenter*.").

[64] See, e.g., Kerr, "Implementing *Carpenter*," 1 ("The Court was trying to do what this book argues they should: Adjust Fourth Amendment rules for the digital age to restore the earlier balance of government power. The Justices feared that the digital age alters the fundamental balance of the Fourth Amendment because so many private records are now easily accessible to the government outside of places or things. The Court countered that change by introducing Fourth Amendment protection for at least some of those records to restore the prior balance. It was pure equilibrium-adjustment."); Ohm, "Many Revolutions of *Carpenter*," 358 ("The Supreme Court's opinion in *Carpenter v. United States* has been heralded by many as a milestone for the protection of privacy in an age of rapidly changing technology."); and Susan Freiwald and Stephen Wm. Smith, "The *Carpenter* Chronicle: A Near-Perfect Surveillance," *Harvard Law Review* 132 (2018): 206 ("One lesson of *Carpenter* is that courts must not be reluctant to confront the challenges of twenty-first-century technology.").
[65] By "deeply revealing," Ohm explains that he refers to information that is either sensitive, meaning that it can be used to harm an individual or group, or intimate, meaning that it reveals something important and not widely known. Regarding the second factor, "depth" refers to the detail and precision of the information; "breadth" refers to how frequently it is collected and for how long it is stored; and "comprehensive reach" refers to the number of people tracked in the database. Finally, data collection is inescapable if it relates to services — like cell phones — that are necessary to participate in society; records are generated automatically when there is no meaningful opportunity to opt out. Ohm, "Many Revolutions of *Carpenter*," 370–78 (also noting the similarities of this test to the work of Susan Freiwald).
[66] Kerr notes that in his view, the traditional Fourth Amendment rule is that contents of communications are protected, but non-content metadata is not. He argues that, after *Carpenter*, non-content Internet records should be protected under the Fourth Amendment when three requirements are met: the records exist because of the digital age, they are created without meaningful voluntary choice, and they tend to reveal the privacies of life. Kerr, "Implementing *Carpenter*," 16–25.
[67] Freiwald and Smith, "*Carpenter* Chronicle," 219–21.
[68] Freiwald and Smith, "*Carpenter* Chronicle," 219.
[69] Freiwald and Smith, "*Carpenter* Chronicle," 220.
[70] *Carpenter*, 138 S. Ct. at 2214.
[71] *Carpenter*, 138 S. Ct. at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI . . . .").
[72] The location of a cell phone might also be inferred in other ways, for example from the use of Bluetooth or Wi-Fi. See, e.g., Dieter Holger, "How 'Free' Wi-Fi Hotspots Can Track Your Location Even When You Aren't Connected," *PCWorld*, November 1, 2018, https://www.pcworld.com/article/3315197/free-wi-fi-hotspots-can-track-your-location-even-when-you-arent-connected.html; and Bennett Cyphers and Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, Electronic Frontier Foundation, December 2, 2019, 19, https://www.eff.org/wp/behind-the-one-way-mirror.
[73] *Carpenter*, 138 S. Ct. at 2211–12.
[74] Stephanie Lacambra, *Cell Site Location Information: A Guide for Criminal Defense Attorneys*, Electronic Frontier Foundation, March 28, 2019, 1, https://www.eff.org/files/2019/03/28/csli_one-pager.pdf. We note that pinging would be a search under Fourth Amendment trespassory theory independent of *Carpenter* to the extent that it results in law enforcement commandeering a cell phone, causing the device to generate and relay data that it would not otherwise.
[75] Alexandra Witze, "GPS Is Doing More Than You Thought," *Scientific American*, October 30, 2019, https://www.scientificamerican.com/article/gps-is-doing-more-than-you-thought; and "What Is a GPS? How Does It Work?," Library of Congress, accessed January 20, 2021, https://www.loc.gov/everyday-mysteries/item/what-is-gps-how-does-it-work.
[76] See "Interconnected VoIP Service; Wireless E911 Location Accuracy Requirements; E911 Requirements for IP-Enabled Service Providers," 76 Fed. Reg. 188 (Sept. 28, 2011) (codified at 47 C.F.R. § 20.18 (2019)) (requiring wireless service providers to have E911 technology available in order to assist with emergency response), https://www.govinfo.gov/content/pkg/FR-2011-09-28/pdf/2011-24865.pdf.
[77] Jacob Kastrenakes, "GPS Will Be Accurate within One Foot in Some Phones Next Year," *Verge*, September 25, 2017, https://www.theverge.com/circuitbreaker/2017/9/25/16362296/gps-accuracy-improving-one-foot-broadcom.
[78] *Carpenter*, 138 S. Ct. at 2218.
[79] Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, Brennan Center for Justice, December 20, 2018, https://www.brennancenter.org/our-work/research-reports/cellphones-law-enforcement-and-right-privacy.
[80] "The Problem with Mobile Phones," Electronic Frontier Foundation, October 30, 2018, https://ssd.eff.org/en/module/problem-mobile-phones. Examples of cell phone applications that collect and store GPS data include dating, social media, fitness, and local news and weather service apps. See, e.g., "Safety Tips," Grindr, accessed January 20, 2021, https://help.grindr.com/hc/en-us/articles/217955357-Safety-Tips; "How Do I Turn Location Services On or Off for Facebook?" Facebook, accessed January 20, 2021, https://www.facebook.com/help/275925085769221; and "Map Your Run with New Nike+ GPS App," Nike, September 7, 2010, https://news.nike.com/news/map-your-run-with-new-nike-gps-app.
[81] See, e.g., Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," *New York Times*, January 25, 2011, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Byron Tau, "House Investigating Company Selling Phone Location Data to Government Agencies," *Wall Street Journal*, June 24, 2020, https://www.wsj.com/articles/house-investigating-company-selling-phone-location-data-to-government-agencies-11593026382; and Edith Ramirez et al., *Data Brokers: A Call for Transparency and Accountability*, Federal Trade Commission, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[82] We note that there is generally an emergency exception to the warrant requirement to the extent that concerns about emergencies arise.

[83] In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 539 (D. Md. 2011) (finding a "reasonable expectation of privacy both in [subject's] location as revealed by real-time [CSLI] and in his movement where his location is subject to continuous tracking over an extended period of time."). See also Tracey v. State, 152 So. 3d 504, 525–26 (Fla. 2014) ("[W]e hold that regardless of [the defendant] Tracey's location on public roads, the use of his cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required."); and Commonwealth v. Augustine, 4 N.E.3d 846, 864–66 (Mass. 2014) (in finding that a warrant was required for the police to obtain historical CSLI, noting that the "distinction between privacy interests in public and private spaces makes CSLI especially problematic, because cellular telephones give off signals from within both spaces, and when the government seeks to obtain CSLI from a cellular service provider, it has no way of knowing in advance whether the CSLI will have originated from a private or public location.").
[84] However, at least one lower court distinguished *Carpenter* based on the limited duration of the surveillance. Compare Sims v. State, 569 S.W.3d 634, 645–46 (Tex. Crim. App. 2019) (recognizing that *Carpenter* applies to real-time location information but determining that pinging a suspect's phone five times within three hours was too short a time frame to raise an expectation of privacy) with State v. Snowden, 140 N.E.3d 1112, 1127–28 (Ohio Ct. App. 2019); and State v. Muhammad, 451 P.3d 1060, 596–99 (Wash. 2019). As indicated in *Snowden* and *Muhammad*, many courts have declined to suppress real-time location information obtained without a warrant under the exigent circumstances doctrine. The exigent circumstances doctrine is an exception to the Fourth Amendment, which applies when obtaining a warrant would endanger police officers or other individuals or would result in concealment or destruction of evidence.
[85] See, e.g., Brief of Technology Experts as *Amici Curiae* in Support of Petitioner at 29, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) ("[B]ecause of the increasing precision of CSLI . . . even a single data point has the potential to reveal highly sensitive information about a person's associations, habits, beliefs, medical conditions, and vices.").
[86] *Carpenter*, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring)).
[87] *Carpenter*, 138 S. Ct. at 2218.
[88] See Brief of Technology Experts at 26, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) ("In addition to being relatively cheap to obtain and store, CSLI data is uniquely easy to analyze in bulk compared to previous forms of surveillance data, such as wiretaps. Chiefly, this is because CSLI is structured data. That is, the information is stored in a predictable and standardized format that computers can be easily programmed to read, interpret, and even analyze, all without the need for human involvement.").
[89] Brief of Technology Experts at 11–12, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) ("As law enforcement's appetite for CSLI has grown, the phone companies have created automated self-service websites through which government personnel can request and receive location data" from their own offices.); and Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone," *Vice*, January 8, 2019, https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.
[90] Kevin S. Bankston and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*," *Yale Law Journal* 123 (2014): 350.
[91] See, e.g., Apple, *Location Services Privacy Overview: Learn How Location Services Protects Your Privacy*, November 2019, 3–4, https://www.apple.com/privacy/docs/Location_Services_White_Paper_Nov_2019.pdf; and Google, "Manage Your Android Device's Location Settings," Google Account Help, accessed January 21, 2021, https://support.google.com/accounts/answer/3467281?hl=en. There may also be additional nuances to the voluntariness analysis in specific cases involving GPS, depending on factors like an app's privacy policies or available settings.
[92] Sean Hollister, "Thousands of Android Apps Can Track Your Phone — Even If You Deny Permissions," *Verge*, July 8, 2019, https://www.theverge.com/2019/7/8/20686514/android-covert-channel-permissions-data-collection-imei-ssid-location; Zack Whittaker, "Apple Says Its Ultra Wideband Technology Is Why Newer iPhones Appear to Share Location Data, Even When the Setting Is Disabled," *TechCrunch*, December 5, 2019, https://tcrn.ch/2PeyPRG; Marrian Zhou and Richard Nieva, "Google Is Probably Tracking Your Location, Even If You Turn It Off, Says Report," *CNET*, August 13, 2018, https://www.cnet.com/news/google-is-probably-tracking-your-location-even-if-you-turn-it-off-says-report; and Rob Pegoraro, "Apple and Google Remind You about Location Privacy, but Don't Forget Your Wireless Carrier," *USA Today*, November 23, 2019, https://www.usatoday.com/story/tech/columnist/2019/11/23/location-data-how-much-do-wireless-carriers-keep/4257759002.
[93] The FCC's wireless Enhanced 911 (E911) rules require wireless carriers to provide information on the location of 911 callers. "911 and E911 Services," Federal Communications Commission, last modified December 23, 2020, https://www.fcc.gov/general/9-1-1-and-e9-1-1-services; and United States v. Wallace, 885 F.3d 315 (5th Cir. 2018), *denying en banc rev.* (Dennis, J. and Graves, J. dissenting) ("Defendant William Wallace contends that the Government violated the Fourth Amendment by ordering his service provider to activate his phone's 'Enhanced 911' capability and to relay his GPS coordinates in real time, including while he was in his home."). See also Apple, "About Privacy and Location Services in iOS and iPadOS," accessed February 26, 2021, https://support.apple.com/en-us/HT203033 ("For safety purposes, your iPhone's location information may be used when you place an emergency call to aid response efforts regardless of whether you enable Location Services."); and Google, "Manage Your Android Device's Location Settings" ("If [Android Emergency Location Service] is off, your mobile carrier may still send the device's location during an emergency call or text.").
[94] Pew Research Center, "Mobile Fact Sheet," June 12, 2019, https://www.pewresearch.org/internet/fact-sheet/mobile (noting that the "vast majority of Americans — 96% — now own a cellphone of some kind").
[95] *Knotts*, 460 U.S. at 283.
[96] See, e.g., Eric A. Taub, "Car Navigation Systems Plot a Course Forward against Phone Apps," *New York Times*, February 1, 2018, https://www.nytimes.com/2018/02/01/business/car-navigation-systems-apps.html.

[97] Car manufacturers and their affiliates may detail their policies on the collection, retention, and sharing of GPS location information in their terms of service. See, e.g., Toyota, "Connected Vehicle Services Privacy and Protection Notice," accessed January 25, 2021, https://www.toyota.com/privacyvts/images/doc/privacy-portal.pdf ("Your GPS Navigation is equipped with a traffic feature that automatically collects and transmits, through GPS technology, your Location Data, travel direction and speed. . . . It is not tied to your VIN or Personal Information. . . . We may also share your Location Data . . . with . . . Law enforcement . . . ."); General Motors, "OnStar Privacy Statement," last modified January 2020, https://www.onstar.com/us/en/privacy_statement ("We may collect the following information through your use of the products and services, including when you operate or travel in a vehicle that has active products or services, and otherwise with your consent. . . . Information about the use of your vehicle, including operational and safety related information: such as GPS location. . . . [W]e may share your information . . . [a]s required or permitted by law . . ."); and Mazda, "Connectivity Privacy Policy," last modified May 1, 2020, https://www.mazdausa.com/site/privacy-connectedservices ("All of our Connected Vehicles . . . collect and transmit certain Default Data from the Connected Vehicle, . . . 'Default Data' includes the following: 'Location Data': geo-location coordinates of your Connected Vehicle's latitude and longitude each time you turn off your Connected Vehicle. . . . Additionally, we may share the Default Data as follows: with law enforcement, courts, administrative bodies, or governments ('Enforcement Entities') as may be required by applicable law . . . ."). However, oftentimes the length and complexity of these terms of service make them inaccessible to users. Keith Wagstaff, "You'd Need 76 Work Days to Read All Your Privacy Policies Each Year," *Time*, March 6, 2012, https://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year.

[98] *Jones*, 565 U.S. at 413 (Sotomayor, J., concurring), 418 (Alito, J., concurring).

[99] *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring); and *Carpenter*, 138 S. Ct. at 2217–18 ("And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.").

[100] *Carpenter*, 138 S. Ct. at 2218 ("Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone [is] — almost a 'feature of human anatomy' . . . "); and at 2215 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

[101] Additional factors may affect the completeness of the GPS data generated by smart cars, such as the volume of trips someone takes and how close to their destination they choose to park. Center for Sustainable Systems, "Personal Transportation Factsheet," University of Michigan, October 2020, http://css.umich.edu/factsheets/personal-transportation-factsheet ("In the U.S., the predominant mode of travel is by automobile and light truck.").

[102] *Jones*, 565 U.S. at 430 (Alito, J. concurring).

[103] Compare United States v. Diggs, 385 F. Supp. 3d 648, 652–55 (N.D. Ill. 2019), *reconsideration denied*, No. 18 CR 185, 2020 WL 208826 (N.D. Ill. Jan. 14, 2020) (relying on *Carpenter* and the *Jones* concurrences to find that the government's warrantless acquisition from a third party of more than a month of historical location data from a vehicle's built-in GPS system was an unreasonable search) with United States v. Howard, 426 F. Supp. 3d 1247, 1257 (M.D. Ala. 2019) (concluding that no warrant was necessary to obtain 22 hours' worth of data from a built-in GPS system).

[104] Bureau of Transportation Statistics, "National Household Travel Survey Daily Travel Quick Facts," United States Department of Transportation, May 31, 2017, https://www.bts.gov/statistical-products/surveys/national-household-travel-survey-daily-travel-quick-facts.

[105] Jim Edwards, "Ford Exec: 'We Know Everyone Who Breaks the Law' Thanks to Our GPS in Your Car," *Business Insider*, January 8, 2014, https://www.businessinsider.com/ford-exec-gps-2014-1; and Ford, "Ford US Privacy Policy, Including Vehicle Connectivity Privacy," last modified September 14, 2020, https://www.ford.com/help/privacy/ ("Location and Global Positioning System (GPS) (if equipped): Some vehicles contain global positioning system (GPS) capability or, in some instances, may utilize the GPS in connected wireless devices. GPS may be used to determine the vehicle's physical location, travel direction, and speed, and to record this information over time to provide location-based services."). See also Fiat, "Uconnect® Access Privacy Policy," last modified July 1, 2014, https://www.driveuconnect.com/privacy-policy.html; Toyota, "Connected Vehicle Services Privacy"; General Motors, "OnStar Privacy Statement"; and Mazda, "Connectivity Privacy Policy."

[106] See Mazda, "Connectivity Privacy Policy"; and Fiat, "Uconnect® Access Privacy Policy" ("In addition to the information that you directly provide, Sprint may collect information from you or your vehicle (with Information You Give, all called 'Collected Data') which may include but not limited to . . . location information . . . as may be required by law or regulations. Some of this data may be transmitted even after your ignition is off.").

[107] See, e.g., Toyota, "Connected Vehicle Services Privacy" ("Your GPS Navigation is equipped with a traffic feature that automatically collects and transmits, through GPS technology, your Location Data, travel direction and speed to support HD traffic and weather information available in your Vehicle."); General Motors, "OnStar Privacy Statement" ("We may collect the following information through your use of the products and services. . . . Information about the use of your vehicle, including operational and safety related information: such as GPS location . . . "); and Mazda, "Connectivity Privacy Policy" ("We automatically collect certain default data from the connected vehicle on an ongoing basis. Only we can deactivate the TCU and disable our collection of all default data. Note that the sale, transfer, or lease termination of a connected vehicle will not disable automatic default data collection. . . . 'Default Data' includes . . . 'Location Data': geo-location coordinates of your Connected Vehicle's latitude and longitude each time you turn off your Connected Vehicle ('Ignition-Off') . . . ").

[108] Erin Biba, "How Connected Car Tech Is Eroding Personal Privacy," BBC, August 9, 2016, http://www.bbc.com/autos/story/20160809-your-car-is-not-your-friend.

[109] Brief of *Amicus Curiae* Google LLC In Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant, United States v. Chatrie, No. 3:19-cr-130, 12–13 (E.D. Va. Dec. 23, 2019), https://assets.documentcloud.org/documents/6747427/2.pdf.

[110] Mana Azarmi, "Location Data: The More They Know," Center for Democracy & Technology, November 27, 2017, https://cdt.org/insights/location-data-the-more-they-know/ ("Verizon sounded the alarm in its recent transparency report about the growing use of cell tower dumps: 'This tool is being used much more frequently by law enforcement. We previously reported that in 2013 we received approximately 3,200 warrants or orders for cell tower dumps; we received 14,630 warrants or orders for cell tower dumps in 2016.'").

[111] Sprint, *Sprint Corporation Transparency Report*, July 2019, 2, https://newsroom.sprint.com/csr//content/1214/files/Transparency%20Report%20July%202019.pdf ("For court orders that are based on a finding that the records sought are 'relevant and material' to an ongoing criminal investigation, Sprint may produce any records that are requested, including incoming and outgoing telephone numbers, but not the content of communications (i.e., non-content records), or historical records showing the locations of the cell towers used during a phone call or when sending or receiving a text message. . . . For court orders based on a finding of 'probable cause,' meaning a likelihood that the request will provide evidence of a crime, Sprint may produce historical records showing the locations of cell towers used during a phone call or when sending a text message, and location information for a device in real time. In addition, court orders may compel Sprint to identify the telephone numbers for all calls that use a specific cell tower to connect to Sprint's network during a specific period of time."); and Google, "Global Requests for User Information," Google Transparency Report, last modified December 2019, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period. See also T-Mobile, *T-Mobile US, Inc. Transparency Report for 2018*, 6, https://www.t-mobile.com/content/t-mobile/corporate/news/media-library/details/document.html/content/dam/t-mobile/corporate/media-library/public/documents/TransparencyReport2018.pdf?a=b (reporting 6,184 requests for tower dumps in 2018).
[112] Azarmi, "Location Data"; and Brian Owsley, "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance," *University of Pennsylvania Journal of Constitutional Law* 16 (2013): 2.
[113] Compare Apple, *Legal Process Guidelines*, accessed January 21, 2021, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf ("Device location services information is stored on each individual device and Apple cannot retrieve this information from any specific device.") with Jennifer Valentino-DeVries, "Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works." *New York Times*, April 13, 2019, https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html.
[114] Brief of *Amicus Curiae* Google LLC, *Chatrie*, No. 3:19-cr-130 at 13–14.
[115] Gabriel J. X. Dance and Jennifer Valentino-DeVries, "Have a Search Warrant for Data? Google Wants You to Pay," *New York Times*, January 24, 2020, https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html.
[116] Meg O'Connor, "Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder," *Phoenix New Times*, January 16, 2020, https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374; and Jennifer Valentino-DeVries, "Tracking Phones, Google Is a Dragnet for the Police," *New York Times*, April 13, 2019, https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.
[117] U.S. Const. amend. IV.
[118] Brief of Google LLC, *Chatrie*, No. 3:19-cr-130 at 11 ("Typically, U.S. law-enforcement authorities use legal process (whether in the form of a search warrant, court order, or subpoena) to compel Google to disclose content or records of electronic communications associated with specifically identified Google users or accounts.").
[119] See Valentino-DeVries, "Google's Sensorvault"; George Joseph and WNYC Staff, "Manhattan DA Got Innocent People's Google Phone Data through a 'Reverse Location' Search Warrant," *Gothamist*, August 12, 2019, https://gothamist.com/news/manhattan-da-got-innocent-peoples-google-phone-data-through-a-reverse-location-search-warrant; Katie Haas, "Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions," American Civil Liberties Union, March 27, 2014, https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique; and Aaron Mak, "Close Enough," *Slate*, February 19, 2019, https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html.
[120] *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J. dissenting).
[121] Nate Anderson, "How 'Cell Tower Dumps' Caught the High Country Bandits — and Why It Matters," *Ars Technica*, August 29, 2013, https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters.
[122] *Chatrie*, No. 3:19-cr-130.
[123] Generally, courts have been hesitant to suppress evidence from warrantless tower dumps for two reasons. The first is the good-faith exclusionary rule, which states that if law enforcement officers had a reasonable, good faith belief that they were acting according to legal authority, illegally seized evidence should still be admissible. Second, courts have noted that the Supreme Court specifically reserved the question of whether its holding in *Carpenter* would apply to tower dumps. See, e.g., People v. Root, No. 346164, 2020 WL 1816009, at *6 (Mich. Ct. App. April 9, 2020) ("In this case, we likewise find that the police acted in good faith when obtaining information regarding defendant's cell phone as part of the 'tower dump.' Here, when police in 2009 obtained information from a 'tower dump' of certain cell phone towers at the times relevant to Kelly's disappearance, they did so with a court order under the Stored Communications Act, which was not considered to be improper conduct under existing precedent. Indeed, even now this conduct has not been determined to be inappropriate, as the Supreme Court in *Carpenter* specifically declined to extend its holding to information obtained by police through a 'tower dump.'"); and United States v. Pendergrass, No. 1:17-CR-315-LMM-JKL, 2018 WL 7283631, at *13–14 (N.D. Ga. Sept. 11, 2018), *report and recommendation adopted*, No. 1:17-CR-315-LMM-JKL, 2019 WL 102377 (N.D. Ga. Jan. 4, 2019) ("The Court agrees with the government that, assuming solely for the sake of argument that *Carpenter* applies to tower dumps, the good faith exception to the exclusionary rule applies. . . . Here, [law enforcement] obtained a court order for the tower dumps on January 30, 2017, pursuant to the Stored Communications Act, nearly seventeen months before Carpenter came down. . . . At that time, the law in this Circuit was that communications records obtained under the Stored Communications Act could be obtained by a court order without the need of a search warrant.") (internal citations omitted).
[124] United States v. Adkinson, 916 F.3d 605, 610–11 (7th Cir. 2019), *cert. denied*, 139 S. Ct. 2762 (2019).
[125] Commonwealth v. Dunkins, 229 A.3d 622, 629 (Pa. Super. Ct. 2020).
[126] The policy authorized the college to collect and disclose all internet data composed, transmitted, or received through the campus computer system and its network connections. *Dunkins*, 229 A.3d at 630.

[127] Google charges police as little as $245 to retrieve data on potentially thousands of devices. Dance and Valentino-DeVries, "Have a Search Warrant for Data?" Some cell phone providers report charging fees for tower dump records. However, as of 2013 these fees were minimal. According to a *U.S. News* report, "For cellphone tower dumps, which give police access to the call information of everyone whose cell signal was routed through a tower in a specific period of time, the pricing is more distinct. Verizon charges nothing for a tower dump, whereas Cricket bills $185 and AT&T charges $75. T-Mobile offers two rates for tower dumps: $100 for raw data or $150 for numbers and 'corresponding subscriber information.'" Steven Nelson, "Cell Providers Collect Millions from Police for Handing Over User Information," *U.S. News & World Report*, December 9, 2013, https://www.usnews.com/news/articles/2013/12/09/cell-providers-collect-millions-from-police-for-handing-over-user-information.

[128] The intimacy of the data revealed by a reverse location search may depend on the type of search. For example, while a tower dump of an area encompassing a mosque might not reveal which devices were inside due to the inherent limitations of CSLI data, it will reveal information about every single device in the surrounding area based on which devices connected to nearby cell towers. From this, it is possible for law enforcement to infer information like someone's religious affiliation or associations. This is especially true if the density of cell towers is such that proximity to a cell tower indicates an individual's presence in a fairly narrow geographic area. The information available to law enforcement from Google in a reverse location search is much more accurate. Using both CSLI and GPS information, Google can pinpoint whether a device was actually inside the mosque or not.

[129] Ángel Díaz, *New York City Police Department Surveillance Technology*, Brennan Center for Justice, October 4, 2019, https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

[130] The maker of the Stingray device, formerly known as the Harris Corporation, recently announced that it planned to discontinue sales of its technology to local law enforcement and phase out software updates. However, this has not dissuaded departments like the New York State Police and the Florida Department of Law Enforcement from turning to other manufacturers, often with financial assistance from federal grants. Dell Cameron and Dhruv Mehrotra, "Cops Turn to Canadian Phone-Tracking Firm after Infamous 'Stingrays' Become 'Obsolete,'" *Gizmodo*, October 23, 2020, https://gizmodo.com/american-cops-turns-to-canadian-phone-tracking-firm-aft-1845442778; and American Civil Liberties Union of New York, "Legislative Memo: In Support of a Warrant Requirement for the Use of Stingrays," accessed on January 21, 2020, n1, https://www.nyclu.org/en/legislation/legislative-memo-support-warrant-requirement-use-stingrays (explaining that "'Stingray' is the name of one model of cell site simulators manufactured by the Florida-based Harris Corporation. It is often used in public discourse, and is used in this memorandum, to refer to all models of cell site simulators. Other models of cell site simulators available include Kingfish, Triggerfish, Hailstorm, and Harpoon."). See also *Hearing on "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats" Before the Subcomm. on Oversight of the H. Comm. on Science, Space, and Technology*, 115th Cong. (2018) (written testimony of Jonathan Mayer, assistant professor of computer science, Princeton University, June 27, 2018), https://docs.house.gov/meetings/SY/SY21/20180627/108486/HHRG-115-SY21-Wstate-MayerJ-20180627.pdf.

[131] Brief of *Amici Curiae* the American Civil Liberties Union, American Civil Liberties Union of the Nation's Capital, and Electronic Frontier Foundation Supporting the Appellant and Reversal, Jones v. United States, 168 A.3d 703 (D.C. Cir. 2017) (No. 15-CF-322), https://www.aclu.org/sites/default/files/field_document/amicus_brief_-_prince_jones_-_final_share.pdf; Curtis Waltman, "Revisiting the Cell Simulator Census," *MuckRock*, December 4, 2017, https://www.muckrock.com/news/archives/2017/dec/04/revisiting-cell-site-simulator-census; and American Civil Liberties Union of New York, "Warrant Requirement for the Use of Stingrays."

[132] American Civil Liberties Union, "Stingray Tracking Devices: Who's Got Them?," last updated November 2018, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them.

[133] Report of the House Committee on Oversight and Government Reform, *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations*, 114th Cong. (2016), December 19, 2016, https://info.publicintelligence.net/US-CellSiteSimulatorsPrivacy.pdf.

[134] 18 U.S.C. § 2518 (2020).

[135] Several states, including California, Illinois, Utah, Virginia, and Washington have passed laws requiring law enforcement agencies to obtain a warrant before deploying cell site simulators. House Committee on Oversight and Government Reform, *Law Enforcement Use of Cell-Site Simulation Technologies*, 30.

[136] See, e.g., Jones v. United States, 168 A.3d 703 (D.C. Cir. 2017) (No. 15-CF-322) (holding that the DC Metropolitan Police Department's warrantless use of Stingray technology in an investigation violated the Fourth Amendment); People v. Gordon, 68 N.Y.S.3d 306 (N.Y. Sup. Ct. 2017) (requiring a warrant for the New York Police Department's use of Stingrays); United States v. Ellis, 270 F. Supp. 3d 1134, 1146 (N.D. Cal. 2017) ("[T]he court holds that Ellis had a reasonable expectation of privacy in his real-time cell phone location, and that use of the Stingray devices to locate his cell phone amounted to a search requiring a warrant, absent an exception to the warrant requirement."); and State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016) (holding that the Baltimore Police Department's use of Hailstorm, an upgraded version of the Stingray, required a valid search warrant based on probable cause).

[137] *Gordon*, 68 N.Y.S.3d 306.

[138] State v. Sylvestre, 254 So. 3d 986, 991 (Fla. Dist. Ct. App. 2018) (internal citations omitted) ("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. . . . This is especially true when the cell phone is in a private residence . . . or other private locations beyond public thoroughfares including doctor's offices, political headquarters, and other potentially revealing locales.").

[139] United States v. Woodson, No. 4:16CR541AGF, 2018 WL 7150388, at *9 (E.D. Mo. Nov. 21, 2018), *report and recommendation adopted*, No. 4:16CR541AGF, 2019 WL 398453 (E.D. Mo. Jan. 31, 2019) ("Unlike the CSLI in *Carpenter*, which would allow agents to use a known telephone number to track the location of a suspect, the signaling information in this case was obtained by tracking the physical location of [the defendant] so that agents could obtain his previously unknown telephone number.").

[140] Millions March N.Y.C. v. N.Y. Police Dep't, No. 100690/2017 (N.Y. Sup. Ct. N.Y. Cnty. 2018) (memorandum of law in support of verified petition), https://www.nyclu.org/sites/default/files/field_documents/2018-10-05_final_amended_mol_iso_petition_for_filing_00067082-2xb2d9a.pdf; and Larry Greenemeier, "What Is the Big Secret Surrounding Stingray Surveillance?," *Scientific American*, June 25, 2015, https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance.

[141] *Hearing on "Bolstering Data Privacy and Mobile Security"* (written statement of Jonathan Mayer).
[142] Curtis Waltman, "Here's How Much a StingRay Cell Phone Surveillance Tool Costs," *Vice*, December 8, 2016, https://www.vice.com/en_us/article/gv5k3x/heres-how-much-a-stingray-cell-phone-surveillance-tool-costs.
[143] House Committee on Oversight and Government Reform, *Law Enforcement Use of Cell-Site Simulation Technologies*, 7 ("DHS has provided more than $1.8 million in grant money to state and local law enforcement to purchase cell-site simulators."). *Hearing on "Examining Law Enforcement Use of Cell Phone Tracking Devices" Before the Subcomm. on Info. Tech. of the H. Comm. on Oversight and Gov't Reform*, 114th Cong. (2015) (responses to questions for the record submitted to Seth Stodder, Assistant Secretary, Threat Prevention and Security Policy, U.S. Department of Homeland Security, by Hon. Jason Chaffetz, Chairman, House Committee on Oversight and Government Reform), https://www.govinfo.gov/content/pkg/CHRG-114hhrg21433/html/CHRG-114hhrg21433.htm.
[144] *Jones*, 168 A.3d at 714 (quoting *Kyllo*, 533 U.S. at 34.).
[145] David J. Roberts and Meghann Casanova, *Automated License Plate Recognition (ALPR) Use by Law Enforcement: Policy and Operational Guide, Summary*, International Association of Chiefs of Police, August 2012, https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf; and Kaveh Waddell, "How License-Plate Readers Have Helped Police and Lenders Target the Poor," *Atlantic*, April 22, 2016, https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436.
[146] David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, International Association of Chiefs of Police, September 2012, https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf; and Electronic Frontier Foundation, "Automated License Plate Readers (ALPRs)," last updated August 28, 2017, https://www.eff.org/pages/automated-license-plate-readers-alpr.
[147] Electronic Frontier Foundation, "ALPRs."
[148] Electronic Frontier Foundation, "ALPRs."
[149] Dave Maass and Jeremy Gillula, "What You Can Learn from Oakland's Raw ALPR Data," Electronic Frontier Foundation, January 21, 2015, https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data; and Alex Campbell and Kendall Taggart, "A Traffic Cop's Ticket Bonanza in a Poor Texas Town," *BuzzFeed*, January 26, 2019, https://www.buzzfeednews.com/article/alexcampbell/the-ticket-machine#.stGnbbDMQ.
[150] Yael Grauer, "Arizona Police Agencies Gather and Share License Plate Data, but Few Ensure Rules Are Being Followed," *Arizona Mirror*, last updated July 8, 2019, https://www.azmirror.com/2019/07/08/arizona-police-agencies-gather-share-license-plate-data-but-few-ensure-rules-are-being-followed.
[151] See, e.g., Federal Bureau of Investigation, "National Crime Information Center (NCIC)," accessed January 21, 2021, https://www.fbi.gov/services/cjis/ncic (showing that NCIC database includes 21 files, including a Gang File and an Immigration Violator File); and Ángel Díaz and Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Center for Justice, September 10, 2020, https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.
[152] Josh Kaplan, "License Plate Readers Are Creeping into Neighborhoods across the Country," *Slate*, July 10, 2019, https://slate.com/technology/2019/07/automatic-license-plate-readers-hoa-police-openalpr.html.
[153] Lily Hay Newman, "Internal Docs Show How ICE Gets Surveillance Help from Local Cops," *Wired*, March 13, 2019, https://www.wired.com/story/ice-license-plate-surveillance-vigilant-solutions.
[154] See Tanvi Misra, "Who's Tracking Your License Plate?," *CityLab*, December 6, 2018, https://www.citylab.com/equity/2018/12/automated-license-plate-readers-privacy-data-security-police/576904.
[155] National Conference of State Legislatures, "Automated License Plate Readers: State Statutes," October 23, 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx.
[156] National Conference of State Legislatures, "Automated License Plate Readers"; compare Paula T. Dow, "Directive No. 2010-5: Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data," memorandum, State of New Jersey, December 3, 2010, https://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersI-120310.pdf; and John J. Hoffman, "Revision to Attorney General Guidelines for the Use of Automated Licence Plate Readers (ALPRs) and Stored ALPR Data Concerning Data Retention Period," memorandum, State of New Jersey, November 18, 2015, https://www.state.nj.us/lps/dcj/agguide/directives/2015-1118_ALPR_data_retention.pdf; with Me. Rev. Stat. Ann. 29-A § 2117-A(2) (2020).
[157] See *Knotts*, 460 U.S. at 281. See also Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion); Jones v. Town of Woodworth, 132 So. 3d 422, 424–25 (La. App. 2013); State v. Davis, 239 P.3d 1002 (Ore. App. 2010); State v. Myrick, 659 A.2d 976 (N.J. Super. Ct. Law Div. 1995); People v. Davila, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. Bronx Cnty. 2010); United States v. Diaz-Castaneda, 494 F.3d 1146 (9th Cir. 2007); United States v. Ellison, 462 F.3d 557 (6th Cir. 2006); Olabisiomotosho v. City of Houston, 185 F.3d 521, 529 (5th Cir. 1999); United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989); and United States v. Matthews, 615 F.2d 1279 (10th Cir. 1980).
[158] Díaz and Levinson-Waldman, *Automatic License Plate Readers*.
[159] Mariko Hirose, "Documents Uncover NYPD's Vast License Plate Reader Database," American Civil Liberties Union, January 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.
[160] Fox News, "Use of License-Plate Scanners Expands amid Privacy Concerns, Court Battles," last updated December 20, 2015, https://www.foxnews.com/politics/use-of-license-plate-scanners-expands-amid-privacy-concerns-court-battles; and Brief of *Amici Curiae* Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Nevada Supporting Appellant, United States v. Yang, 958 F.3d 851 (9th Cir. 2020) (No. 18-10341), https://www.eff.org/files/2019/03/20/18-10341_us_v._yang_amicus_iso_appellant_eff_aclu_aclu_nevada_.pdf.
[161] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).
[162] Cyrus Farivar, "We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from the Cops," *Ars Technica*, March 24, 2015, http://arstechnica.com/tech-policy/2015/03/we-knowwhere-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/.

[163] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); and at 430 (Alito, J., concurring).
[164] Joseph Cox, "This Company Built a Private Surveillance Network. We Tracked Someone with It," *Vice*, September 17, 2019, https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn.
[165] *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34).
[166] Kaplan, "License Plate Readers Are Creeping into Neighborhoods across the Country" (noting the "sudden affordability" of ALPRs and the resulting increase of use of the technology); and Tom Simonite, "AI License Plate Readers Are Cheaper — So Drive Carefully," *Wired*, January 27, 2020, https://www.wired.com/story/ai-license-plate-readers-cheaper-drive-carefully ("Police can add computer-vision software to ordinary security cameras for as little as $50 a month.").
[167] *Carpenter*, 138 S. Ct. at 2217.
[168] *See, e.g.*, *United States v. Miranda–Sotolongo,* 827 F.3d 663, 668 (7th Cir. 2016) ("Because the police conducted a check of a database containing only non-private information and did so using only registration information that could be seen by any member of the public, the police did not conduct a Fourth Amendment search."); *Diaz–Castaneda*, 494 F.3d at 1152 (stating that "when police officers see a license plate in plain view, and then use that plate to access additional non-private information about the car and its owner, they do not conduct a Fourth Amendment search"); and *Ellison*, 462 F.3d at 563 ("Thus, so long as the officer had a right to be in a position to observe the defendant's license plate, any such observation and corresponding use of the information on the plate does not violate the Fourth Amendment.").
[169] See, e.g.*, Yang*, 958 F.3d at 863 (determining that the defendant did not have standing to challenge the government's use of the ALPR database because he was driving an overdue rental car and consequently had not established he had a reasonable expectation of privacy in the location history of the vehicle); Commonwealth v. McCarthy, 484 Mass. 493, 494 (2020), https://cases.justia.com/massachusetts/supreme-court/2020-sjc-12750.pdf?ts=1587124946 (finding four cameras at the ends of two bridges was insufficient to trigger constitutional protections, but noting that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and constitute a search for constitutional purposes."); and Uhunmwangho v. State, No. 09-19-00119, 2020 WL 1442640, at *6 (Tex. App. Mar. 25, 2020) (distinguishing *Carpenter* on the grounds that it involved monitoring over a lengthy period of time, whereas in this case the police had stopped the defendant for speeding).
[170] *Yang*, 958 F.3d at 863 (Bea, J., concurring).
[171] Nick Wingfield, "A Field Guide to Civilian Drones," *New York Times*, last updated August 29, 2016, https://www.nytimes.com/interactive/2015/technology/guide-to-civilian-drones.html.
[172] Wingfield, "Field Guide to Civilian Drones."
[173] Telegraph Foreign Staff, "Israeli Drone the Size of a Boeing 737 Crashes," *Telegraph*, January 29, 2012, https://www.telegraph.co.uk/news/worldnews/middleeast/israel/9047664/Israeli-drone-the-size-of-a-Boeing-737-crashes.html; Jay Stanley and Catherine Crump, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*, American Civil Liberties Union, December 2011, https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf; and W. J. Hennigan, "It's a Bird! It's a Spy! It's Both," *Los Angeles Times*, February 17, 2011, https://www.latimes.com/archives/la-xpm-2011-feb-17-la-fi-hummingbird-drone-20110217-story.html.
[174] Dan Gettinger, *Public Safety Drones,* 3rd ed., Center for the Study of the Drone at Bard College, March 2020, 7, https://dronecenter.bard.edu/projects/public-safety-drones-project/public-safety-drones-3rd-edition.
[175] Alex Gatopoulos, "All You Need to Know about the Global Hawk Spy Drone Shot Down by Iran," Al Jazeera, June 20, 2019, https://www.aljazeera.com/features/2019/6/20/all-you-need-to-know-about-the-global-hawk-spy-drone-shot-down-by-iran; and Maria Valdovinos, James Specht, and Jennifer Zeunik, *Community Policing and Unmanned Aircraft Systems (UAS): Guidelines to Enhance Community Trust*, Office of Community Oriented Policing Services, U.S. Department of Justice, 2016, https://rems.ed.gov/docs/COPS_Community-Policing-UAS.pdf.
[176] Electronic Frontier Foundation, "Surveillance Drones," accessed January 21, 2021, https://www.eff.org/issues/surveillance-drones; and DJI, "Mavic 2 Enterprise Series," accessed January 21, 2021, https://www.dji.com/mavic-2-enterprise (describing design specifications of one of the most commonly used models of law enforcement drones).
[177] Electronic Privacy Information Center, "Domestic Unmanned Aerial Vehicles (UAVs) and Drones," accessed January 22, 2021, https://epic.org/privacy/drones/#background.
[178] Electronic Privacy Information Center, "UAVs and Drones."
[179] Electronic Privacy Information Center, "UAVs and Drones."
[180] Gettinger, *Public Safety Drones*.
[181] Gettinger, *Public Safety Drones*, 9.
[182] Ashley Southall and Ali Winston, "New York Police Say They Will Deploy 14 Drones," *New York Times*, December 4, 2018, https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.
[183] Jerod MacDonald-Evoy, "What We Know about Police Drones in Arizona and How They're Used," *Arizona Mirror*, July 1, 2020, https://www.azmirror.com/2020/06/30/what-we-know-about-police-drones-in-arizona-and-how-theyre-used; Faine Greenwood, "Can a Police Drone Recognize Your Face?," *Slate*, July 8, 2020, https://slate.com/technology/2020/07/police-drone-facial-recognition.html; Faine Greenwood, "How to Regulate Police Use of Drones," Brookings Institution, September 24, 2020, https://www.brookings.edu/techstream/how-to-regulate-police-use-of-drones; Greg Stanley, "Few Answers on Who Asked Feds to Circle a Predator Surveillance Drone over Minneapolis Protests," *Minnesota Star Tribune*, June 5, 2020, https://www.startribune.com/which-agency-wanted-drone-flown-over-minneapolis-protests/571051962; and John D. McKinnon and Michelle Hackman, "Drone Surveillance of Protests Comes under Fire," *Wall Street Journal*, June 10, 2020, https://www.wsj.com/articles/drone-surveillance-of-protests-comes-under-fire-11591789477.
[184] California v. Ciraolo, 476 U.S. 207, 209, 214–15 (1986).
[185] *Riley*, 488 U.S. at 451.
[186] Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[187] See Policing Project at New York University School of Law, *Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program*, November 2020, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5fc290577acac6192a142d61/1606586458141/AIR+Program+Audit+Report+vFINAL+%28reduced%29.pdf; and Brennan Center for Justice, "Leaders of a Beautiful Struggle, et al. v. Baltimore Police Department, et al." (court case tracker), December 7, 2020, https://www.brennancenter.org/our-work/court-cases/leaders-beautiful-struggle-et-al-v-baltimore-police-department-et-al.
[188] Leaders of a Beautiful Struggle v. Baltimore Police Department, 979 F.3d 219 (4th Cir. 2020).
[189] *Leaders of a Beautiful Struggle*, 979 F.3d at 228–29.
[190] Policing Project at New York University School of Law, "The Policing Project's Audit of Baltimore's Aerial Investigation Research Program," December 12, 2020, https://www.policingproject.org/news-main/2020/12/12/the-policing-projects-audit-of-baltimores-aerial-investigation-research-program (noting that "The U.S. Court of Appeals for the Fourth Circuit recently upheld the constitutionality of the AIR Program. But that decision was based on an incomplete understanding of the facts. The Policing Project has filed an amicus brief urging the court to vacate its decision."); see *Leaders of a Beautiful Struggle*, 979 F.3d at 235 (Gregory, J. dissenting) ("[The majority's] conclusions rest on a fundamentally warped understanding of the facts, accepting the Government's promises about the AIR program and ignoring the plaintiffs' contrary evidence. The AIR program does, indeed, amount to long-term surveillance that compiles 'a detailed and comprehensive record' of a person's past movements.").
[191] Petition for Rehearing En Banc, *Leaders of a Beautiful Struggle*, 979 F.3d 219 (4th Cir. Nov. 19, 2020) (No. 20-1495), https://www.aclu.org/legal-document/petition-rehearing-en-banc; and Brennan Center, "Leaders of a Beautiful Struggle."
[192] Electronic Privacy Information Center, "UAVs and Drones."
[193] Albert Fox Cahn and Vanessa L. Gibson, "NYPD Spy Drones Fly into Privacy Headwinds," Just Security, January 22, 2019, https://www.justsecurity.org/62304/nypd-spy-drones-fly-privacy-headwinds.
[194] For example, in its Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program, the Policing Project describes how the combination of aerial and ground technologies allows AIR to track individuals or vehicles over multiple days. Policing Project, *Policing Project's Audit of Baltimore's AIR Program*. See also Police Executive Research Forum, *Drones: A Report on the Use of Drones by Public Safety Agencies — and a Wake-Up Call about the Threat of Malicious Drone Attacks*, Community Oriented Policing Services, 2020, https://cops.usdoj.gov/RIC/Publications/cops-w0894-pub.pdf.
[195] See DJI, "Phantom 4 Pro," https://www.dji.com/phantom-4-pro; and Jim Fisher, "The Best Drones for 2021," *PCMag*, updated December 17, 2020, https://www.pcmag.com/picks/the-best-drones.
[196] Gettinger, *Public Safety Drones*.
[197] Police Executive Research Forum, *Drones*.
[198] National Conference of State Legislatures, "2016 Unmanned Aircraft Systems (UAS) State Legislation Update," March 20, 2017, https://www.ncsl.org/research/transportation/2016-unmanned-aircraft-systems-uas-state-legislation-update.aspx.
[199] *Kyllo*, 533 U.S. 27; and Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (noting that the "reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent").
[200] See Ángel Díaz, "Law Enforcement Access to Smart Devices," Brennan Center for Justice, December 21, 2020, https://www.brennancenter.org/our-work/research-reports/law-enforcement-access-smart-devices.
[201] Fitbit home page, accessed January 22, 2021, https://www.fitbit.com/us/home; and Apple Watch home page, accessed January 22, 2021, https://www.apple.com/watch.
[202] See, e.g., Katherine Britton, "IoT Big Data: Consumer Wearables, Data Privacy and Security," *Landslide*, November/December 2015, https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security.
[203] Apple, "Back Up Your Apple Watch," updated January 28, 2021, https://support.apple.com/en-us/HT204518.
[204] Fitbit, "Fitbit Privacy Policy," accessed January 22, 2021, https://www.fitbit.com/global/us/legal/privacy-policy.
[205] Compare Dance and Valentino-DeVries, "Have a Search Warrant for Data?" (noting that "Google's fees range from $45 for a subpoena and $60 for a wiretap to $245 for a search warrant") with Bankston and Soltani, "Tiny Constables and the Cost of Surveillance," 350 (finding that cover car pursuit cost $275 per hour in 2014).
[206] Marguerite Reardon, "Your Alexa and Fitbit Can Testify against You in Court," *CNET*, April 5, 2018, https://www.cnet.com/news/alexa-fitbit-apple-watch-pacemaker-can-testify-against-you-in-court.
[207] Christine Hauser, "Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing," *New York Times*, October 3, 2018, https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html; and Amanda Watts, "Cops Use Murdered Woman's Fitbit to Charge Her Husband," CNN, April 26, 2017, https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html.
[208] Ring, "Ring Video Doorbells," accessed January 22, 2021, https://shop.ring.com/pages/doorbell-cameras.
[209] Caroline Haskins, "Amazon Is Hiring a News Editor for Its 'Neighborhood Watch' App," *Vice*, April 30, 2019, https://www.vice.com/en_us/article/gy4q8j/amazon-is-hiring-a-news-editor-for-its-neighborhood-watch-app.
[210] Nest, "Know Who's Knocking," Google Store, accessed February 26, 2021, https://store.google.com/product/nest_hello_doorbell.
[211] Compare Florida v. Jardines, 569 U.S. 1 (2013) (holding that law enforcement officers' use of drug-sniffing dog on front porch of home was a trespassory invasion of the curtilage which constituted a "search" for Fourth Amendment purposes) with Ciraolo, 476 U.S. 207 (holding that aerial observations of a backyard from publicly navigable airspace did not constitute a search under the Fourth Amendment).
[212] Paige Leskin, "Use This Map to See If Your Local Police Department Has Access to Amazon Ring's Unofficial Surveillance Network of Video Doorbells," *Business Insider*, August 28, 2019, https://www.businessinsider.com/amazon-ring-video-doorbell-map-police-departments-with-access-2019-8 ("Recent investigations into Ring have found that law enforcement agencies across the US have partnered with Amazon to gain access to an online portal showing a map of Ring video doorbells in their neighborhood. The portal allows police to figure out which cameras in a certain area may have captured surveillance footage, for which authorities need to request permission from homeowners to access.").

[213] Ring, "Neighbors," accessed February 8, 2021, https://ring.com/neighbors. See also Samantha Masunaga, "Police Can Keep Video from Ring Doorbells Indefinitely, Adding to Privacy Concerns," *Los Angeles Times*, November 20, 2019, https://www.latimes.com/business/story/2019-11-20/ring-doorbell-video-data-privacy.
[214] Ring, "How Public Safety Agencies Use Neighbors," accessed January 22, 2021, https://support.ring.com/hc/en-us/articles/360031595491-How-Law-Enforcement-Uses-the-Neighbors-App.
[215] AP News, "Mississippi Program to Use Door Cameras to Fight Crime," November 5, 2020, https://apnews.com/article/technology-mississippi-jackson-ce2c47c83d086bab1dc679e731a637eb.
[216] Poe v. Ullman, 367 U.S. 497, 550 (1961) (Harlan, J., dissenting) ("[T]he sweep of the Court's decisions, under both the Fourth and Fourteenth Amendments, amply shows that the Constitution protects the privacy of the home against all unreasonable intrusion of whatever character."); *Kyllo*, 533 U.S. at 37 ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."); Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("[W]e think that mere categorization of these films as 'obscene' is insufficient justification for such a drastic invasion of personal liberties guaranteed by the First and Fourteenth Amendments. Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home."); and Lawrence v. Texas, 539 U.S. 558, 562 (2003) ("Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home.").
[217] Matthew Guariglia and Dave Maass, "LAPD Requested Ring Footage of Black Lives Matter Protests," Electronic Frontier Foundation, February 16, 2021, https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests.
[218] *Carpenter* 138 S. Ct. at 2214 (first quoting *Boyd*, 116 U.S. at 630; then quoting *Di Re*, 332 U.S. at 595).
[219] *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting) ("The Court suggests that less than seven days of location information may not require a warrant. . . . But the Court does not explain why that is so, and nothing in its opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history.") (internal citations omitted).
[220] David Nield, "Here's All the Data Collected from You as You Browse the Web," *Gizmodo*, December 6, 2017, https://gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304.
[221] Federal Trade Commission, "Internet Cookies," accessed January 22, 2021, https://www.ftc.gov/site-information/privacy-policy/internet-cookies.
[222] *Hearing on "FCC Overreach: Examining the Proposed Privacy Rules" Before the Subcomm. on Commc'n and Tech. of the H. Comm. on Energy & Commerce*, 114th Cong. 5 (2016) (statement of Paul Ohm, professor, Georgetown University Law Center).
[223] Tom Warren, "Google Is Making It Easier to Wipe Out Your Search History," *Verge*, October 24, 2018, https://www.theverge.com/2018/10/24/18017832/google-search-privacy-changes-2018 ("Google stores a record of everything you search for on Google.com if you're logged into your Google Account. You can clear your local browser history, but that won't clear what's stored on Google's servers. While you've been able to dig into the Google Account page and find an activity stream of search history, Google is making it a lot easier to delete this history within search itself today.").
[224] Statista, "Number of Explicit Core Search Queries Powered by Search Engines in the United States as of October 2020," January 18, 2021, https://www.statista.com/statistics/265796/us-search-engines-ranked-by-number-of-core-searches/; Lily Hay Newman, "Limit How Long Google Keeps Your Data with This Overdue Setting," *Wired*, May 7, 2019, https://www.wired.com/story/google-auto-delete-data-privacy-setting.
[225] Alfred Ng, "Google Is Giving Data to Police Based on Search Keywords, Court Docs Show," *CNET*, October 8, 2020, https://www.cnet.com/news/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show; and Dance and Valentino-DeVries, "Have a Search Warrant for Data?"
[226] Kristen Hicks, "How IP Addresses Are Tracked," HostGator, February 13, 2020, https://www.hostgator.com/blog/how-ip-addresses-are-tracked ("IP addresses provide generalized location data (usually based on where your ISP is located)."); and Ng, "Google Is Giving Data to Police Based on Search Keywords."
[227] *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).
[228] Gabriel Weinberg, "Is It True That My ISP Is Spying on My Web Browsing? Does DuckDuckGo Fix That?," Quora, June 10, 2019, https://www.quora.com/Is-it-true-that-my-ISP-is-spying-on-my-web-browsing-Does-DuckDuckGo-fix-that/answer/Gabriel-Weinberg.
[229] United States v. Okparaeka, No. 17-CR-225, 2018 WL 3323822, at *12 (S.D.N.Y. July 5, 2018).
[230] *Carpenter*, 138 S. Ct. at 2214.