2020

42nd Annual Foulston-Siefkin Lecture: The Next Wave of Fourth Amendment Challenges After Carpenter

Matthew Tokson

41ST ANNUAL FOULSTON-SIEFKIN LECTURE: THE NEXT WAVE OF FOURTH AMENDMENT CHALLENGES AFTER *CARPENTER*

Matthew Tokson*

It is an honor to deliver this year's Foulston Siefkin Lecture, and a particular honor to follow in the footsteps of past lecturers like Akhil Amar, Erwin Chemerinsky, Rachel Moran, William Eskridge, Harold Koh, and Ruth Okediji, to name only a few. My topic today is the future of Fourth Amendment law following the Supreme Court's enormously important decision in *Carpenter v. United States*.[1]

Carpenter extends the Fourth Amendment's protections to sensitive information held by third parties, a crucial step towards maintaining the Fourth Amendment's relevance in the digital age. However, the Court's opinion is exceedingly vague and cautious with regard to when and how the Fourth Amendment will protect digital information going forward.

I will argue that the meaning of *Carpenter* ultimately resides in its detailed account of the potential harms threatened by a new form of surveillance. The Court's explanation of these harms and its concerns regarding unregulated government surveillance of citizens' locations take up a large portion of its opinion.[2] It is this discussion, more than any particular line or technical point of distinction from previous cases, that will shape the future of Fourth Amendment law.

Moreover, the Court's practical emphasis on the risk of privacy harm is not a one-off or a sharp break from previous practice. *Carpenter* is consistent with a long

---

* Associate Professor, University of Utah S.J. Quinney College of Law. What follows is an edited and adapted version of the 2019 Foulston Siefkin Lecture, delivered at Washburn University School of Law on March 28, 2019. My thanks to the Washburn University School of Law for its invitation, and to the Washburn faculty members and students for their comments and questions. I also wish to thank Chad Flanders and Hiroshi Motomura for their helpful comments and advice. Special thanks to Christian Clark and Connor Plant for excellent research assistance.

[1] 138 S. Ct. 2206 (2018).

[2] *Id.* at 2215–2220.

line of Supreme Court decisions ignoring or reshaping previous Fourth Amendment doctrines when necessary to protect citizens against unchecked surveillance.[3] It also echoes several previous cases that focus on the revealing, comprehensive, or intimate nature of surveillance when assessing whether a Fourth Amendment search has occurred.[4]

Looking forward, I will discuss some of the novel surveillance technologies that are likely to reach the Supreme Court over the next several years or decades. These technologies include drones, smart homes and devices, web surfing surveillance, and pole cameras targeting a specific suspect's home. Many of these technologies have already been used in police investigations and evaluated by judges in lower court cases. I conclude by discussing how the Supreme Court is likely to resolve these cases, applying the framework of *Carpenter* and its predecessors to make some tentative predictions about the future direction of Fourth Amendment law.

I. THE LAW OF FOURTH AMENDMENT SEARCHES

A. The *Katz* Test

The Supreme Court has generally interpreted the Fourth Amendment to require that the government obtain a warrant or qualify for a warrant exception prior to conducting a "search".[5] But what is a "search" under the Fourth Amendment? Most scholars consider the term to be ambiguous and capable of multiple meanings, and there is no direct drafting history on the subject of the Fourth Amendment's scope.[6]

---

[3] *See,e.g.*, Katz v. United States, 389 U.S. 347, 352–59 (1967); Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001); Florida v. Jardines, 569 U.S. 1, 11 (2013).

[4] *See infra* notes 67–73 and accompanying text.

[5] *See, e.g.,* Weeks v. United States, 232 U.S. 383, 393 (1914). There are several exceptions to the warrant requirement, including exceptions for automobiles, Carroll v. United States, 267 U.S. 132, 153 (1925), exigent circumstances, Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298-99 (1967), and searches incident to arrest, Chimel v. California, 395 U.S. 752, 763 (1969).

[6] *See, e.g.*, Matthew Tokson, Blank Slates; Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 70; Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 395 (1974). *See generally* WILLIAM JOHN CUDDIHY, THE FOURTH AMENDMENT ORIGINS AND ORIGINAL MEANING 602-1791, 713 (2009) ("To the

The Supreme Court initially limited the scope of the Fourth Amendment to "material things"[7] and "constitutionally protected area[s]."[8] This eventually changed after the development of wiretaps and "bugs" that could record people's conversations—technologies that the federal government used extensively and abusively during the mid-twentieth century.[9] The FBI, for instance, recorded nearly a half million conversations from the 1940s to the 1960s.[10] It used these recordings to monitor political groups, record attorney-client conversations, influence judicial appointments, threaten civil rights leaders, and intimidate or discredit members of Congress investigating its activities.[11]

As these abuses were starting to come to light, the Supreme Court expanded the scope of the Fourth Amendment to include intangible things. In the 1967 case *Katz v. United States*, the Court held that government agents conducted an unlawful search when they recorded Katz's telephone conversations without a warrant.[12] The Court rejected the idea that the Fourth Amendment was limited to certain areas or to tangible objects.[13] The majority opinion did not, however, set out any new test for discerning the Fourth Amendment's scope.[14]

Instead, the famous "*Katz* test" comes from Justice Harlan's concurring opinion. He described a two-pronged test as follows: "My understanding … is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that

---

extent that the direct evidence indicates, the amendment's ratifiers took their thoughts about its original meaning to the grave.").

[7] *E.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (ruling that the text of the Fourth Amendment expressly limits its coverage to tangible items).

[8] *E.g.*, Silverman v. United States, 365 U.S. 505, 510–11 (1961) (discussing cases holding that the government did not commit a Fourth Amendment "search" when it did not encroach on any constitutionally protected area, such as a house or office).

[9] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 583 (2011); ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT 17, 24–31 (1992).

[10] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 583 (2011); ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT 17, 24–31 (1992).

[11] *CHARNS*, *supra* note 10 at 77.

[12] 389 U.S. 347, 353 (1967).

[13] *Id.* at 350–51, 353.

[14] *See* Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385 (1974).

society is prepared to recognize as 'reasonable.'"[15] In subsequent cases, this test was simplified, finding a search whenever the government violates a citizen's "reasonable expectation of privacy." In recent years, the Court has held that acts of government trespass on constitutionally protected areas may also violate the Fourth Amendment.[16] But the *Katz* test dictates the scope of Fourth Amendment protection in the vast majority of cases.

B. The Third-Party Doctrine

One of the most controversial applications of the *Katz* test involves what is called the "third-party doctrine." This doctrine provides that that the Fourth Amendment does not apply to personal information disclosed to a third party and obtained by the government from that party. In *Smith v. Maryland*, for instance, the Supreme Court held that the Fourth Amendment did not apply to the telephone numbers that a customer dialed, in part because the customer had voluntarily disclosed the numbers to the telephone company.[17] In *United States v. Miller*, the Court held that the Fourth Amendment did not protect citizens' bank records, which were exposed to bank employees in the ordinary course of business.[18]

As you might imagine, the third-party doctrine is controversial. It's especially problematic in the internet era, when a huge variety of personal data is transmitted over the internet and processed or stored by a variety of internet service providers.[19] The third-party doctrine threatens to erode Fourth Amendment protections for some or all of this data, including emails, web-surfing data, search terms, subscriber information, email to/from data, shared documents stored online, and more.[20] In a recent case, however the Supreme Court limited the third party doctrine's application in important ways.[21] Scholars and lower court judges will be grappling with the ramifications of the Court's decision for years to come.

---

[15] Id. at 361 (Harlan, J., concurring).
[16] United States v. Jones, 132 S. Ct. 945 (2012); Florida v. Jardines, 133 S. Ct. 1409 (2013).
[17] 442 U.S. 735 (1979).
[18] 425 U.S. 435 (1976).
[19] Tokson, supra note 9, at 602–04. For a more direct attack on the third-party doctrine and *Katz*'s privacy-based conception of the Fourth Amendment, *see* Matthew Tokson, *The Normative Fourth Amendment*, 104 Minn. L. Rev. (forthcoming 2019).
[20] *Id.*
[21] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

II. UNDERSTANDING *CARPENTER*

Cell phones work by using radio waves to communicate with cell towers.[22] Cell phone companies typically keep records of when your cell phone signal hits the various antennae on their cell towers.[23] With this information, they can determine your cell phone's approximate location.[24] Cell phone companies generally store this information for up to five years.[25] In other words, cell phone location records can reveal the approximate locations and movements of a cell phone user over a long period of time, potentially revealing intimate and detailed information about their life.[26]

In June of 2018, the Supreme Court decided *United States v. Carpenter*, a Fourth Amendment case involving cell phone location tracking.[27] FBI agents suspected Timothy Carpenter of involvement in a series of robberies in the Detroit area.[28] They requested cell phone signal records from Carpenter's wireless providers (MetroPCS and Sprint).[29] These records allowed the FBI to determine Carpenter's location 12,898 times over a total of 129 days, an average of 101 data points per day.[30] With this information, they could place Carpenter within a sector ranging from one-eighth to four square miles, depending on cell tower density.[31] This evidence placed Carpenter at the location of several of the robberies.

Carpenter sought to have the evidence suppressed, claiming that it amounted to a Fourth Amendment search performed without a warrant.[32] The Supreme Court ruled, in a 5–4 decision, that the government must typically obtain a warrant before accessing a user's cell phone location information (CSLI).[33]

---

[22] *See* Mathew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U.L REV. 139, 160 (2016).
[23] *Id.*
[24] *Id.*
[25] Carpenter, 138 S. Ct. at 2218)
[26] *Id.* at 2217–18.
[27] *Id.* at 2206.
[28] *Id.* at 2212.
[29] *Id.*
[30] *Id.*
[31] *Id.* at 2218.
[32] *Id.* at 2212.
[33] The Court remanded the case to the lower court for further proceedings consistent with their opinion. *Id.* at 2223.

By any standard, *Carpenter* is a profoundly important Fourth Amendment case. But the Court's opinion is notably "cryptic,"[34] and just what it means for future surveillance cases is far from clear. The Court offered no test for determining when the Fourth Amendment would protect information held by a third-party service provider. Echoing the *Katz* majority opinion, the Court mostly just described the privacy problems associated with cell phone location tracking and then declared that such tracking is a Fourth Amendment search.

Can we discern any sort of legal standard or test in the *Carpenter* opinion? To some degree. The key doctrinal line in the case is: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[35] This nominally applies only to cell phone location data. Moreover, it would be easy for future courts to limit *Carpenter* to its facts. CSLI is somewhat unique in that it is collected automatically and is not voluntarily disclosed by the cell phone user.[36]

Yet in practice, the Court's approach is likely to extend Fourth Amendment protections to many forms of digital information. The *Carpenter* opinion focuses on the potentially revealing and comprehensive nature of long-term location tracking. It devotes only a tiny portion of its lengthy opinion to the involuntary nature of the data disclosure.[37] The Court's focus on the privacy harms caused by pervasive digital surveillance suggests that it is these harms, rather than the extent of consumer disclosure to third parties, that will primarily determine the scope of the Fourth Amendment going forward. Moreover, Carpenter is not a one-off decision, nor a drastic break from the Court's approach over the last several

---

[34] Lior Strahilevitz & Matthew Tokson, Ten Thoughts on Today's Blockbuster Fourth Amendment Decision – Carpenter v. United States, Concurring Opinions, *available at* https://web.archive.org/web/20180711125830/https://concurringopinions.com/archives/2018/06/ten-thoughts-on-todays-blockbuster-fourth-amendment-decision-carpenter-v-united-

[35] *Carpenter*, 138 S. Ct. at 2223.

[36] *See* Tokson, supra note 22, at 161–63 (describing how CSLI works and quoting decisions that mention that citizens are unaware they are disclosing their location to their cell service providers).

[37] *See* Carpenter, 138 S. Ct. at 2220. The court's legal analysis on this point is limited to one paragraph. *See id.* at 2219. The opinion also notes that people "compulsively carry cell phones with them all the time," and mentions the number of cell phones in use in the United States. *Id.* at 2218, 2212. The Court's slip opinion ran to twenty-three pages.

decades. It is the continuation of a long trend away from doctrinal rigidity and towards extending Fourth Amendment protection to new surveillance contexts.

A. *Carpenter* and Privacy Harm

The *Carpenter* opinion is largely premised on the "seismic shifts in digital technology," and the greater potential for privacy harm, that cell phones represent.[38] Thus the Court distinguishes the third-party doctrine cases by emphasizing the potential harms posed by cell phone location surveillance and the "detailed and comprehensive record of [a] person's movements" that it reveals.[39] It repeatedly emphasizes the changes wrought by cell phone technology in general and cell phone tracking in particular—technological changes that in turn require legal change. Whereas extended location tracking used to be extremely difficult and costly, cell phones made it cheap and easy.[40] The location records they produce are comprehensive and generally cover up to a five-year period.[41] Because these records contain so much information, they can reveal intimate details about the customer's life, "revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[42]

This largely normative analysis drives the opinion. Because cell phone location data is so revealing and so easy to obtain in large quantities, the Fourth Amendment must apply to it.[43] If the data were more costly to gather, or not stored in such massive quantities, it would be far less of a concern.[44] But because the privacy harms of CSLI are so substantial, not even clear-cut disclosure to a third party is sufficient to eliminate Fourth Amendment protection.[45]

Finally, the opinion suggests the Court's increasing willingness to look

---

[38] Carpenter v. United States, 138 S. Ct. 2206, 2218, 201 L. Ed. 2d 507 (2018)
[39] *Id.* at 2217.
[40] *Id.*
[41] *Id.* at 2218.
[42] *Id.* at 2217 (internal quotation marks omitted) (citing US v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
[43] *Carpenter*, 138 S.Ct. at 2217 ("[T]he time-stamped data provides an intimate window into a person's life…[and] the Government can access each carrier's deep repository of historical location information at practically no expense.").
[44] *Id.*
[45] *Id.* at 2220.

beyond the facts of a case to its broader implications for Fourth Amendment privacy. First in *Kyllo* and then in *Carpenter*, the Court has looked beyond the technology at issue in the case and considered the broader surveillance context. In *Carpenter*, the Court took account of the rapidly improving precision of CSLI tracking, noting that while Carpenter's location could only be determined within a city-block-sized area at best, location tracking had grown more precise since Carpenter's arrest and was likely to continue to advance.[46]

B. The *Carpenter* Evolution

Carpenter substantially limited the reach of the third-party doctrine in the digital era, a development with massive implications for privacy in myriad technological contexts. But the decision itself is more continuous with past Fourth Amendment decisions than commentators have recognized.[47] It is the culmination of a long trend towards protection against serious privacy harm, regardless of other doctrinal factors.

For a start, the *Carpenter* opinion leans heavily on the approach endorsed by five Justices in 2012's *United States v. Jones*.[48] Across two concurrences in *Jones*, five Justices agreed that the continuous monitoring of Jones's car violated his reasonable expectation of privacy, regardless of the fact that the car's location was generally disclosed to the public.[49] As in *Carpenter*, the Justices in *Jones* focused heavily on the privacy harms threatened by GPS tracking: cheap and easy gathering of large amounts of location data with the potential to reveal the details

---

[46] *See id.* at 2219. The Court also noted that the Government could infer Carpenter's location more precisely by combining his cell phone location data with other information over time. *Id.*

[47] *See* Kerr, [new book, or see "Implementing Carpenter on SSRN] (arguing that *Carpenter* was a sharp break from previous *Katz* test cases in that it was not based on property); Paul Ohm, The Many Revolutions of Carpenter, 32 Harv. J.L. & Tech. (forthcoming 2019) (arguing that *Carpenter* was a radically transformational change in law), https://osf.io/preprints/lawarxiv/bsedj.

[48] *See* United States v. Jones, 565 U.S. 400, 413–18 (2012) (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring in the judgment). The majority in *Jones* focused on the fact that the police physically trespassed on Jones's property by touching the underside of his car. *Id.* at 403–05.

[49] *Id.* at 413–18 (2012) (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring in the judgment).

of a person's life.[50] *Carpenter* describes *Jones* as a key precedent[51] and states that "[a] majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements."[52] It describes how cell phone tracking is in some ways more invasive than the tracking in *Jones*.[53] It notes that cell phone tracking is concerning because it is similar to the GPS technology addressed in *Jones*.[54] It also cites *Jones* for the crucial proposition that exposure to third parties does not eliminate Fourth Amendment protection for pervasive location tracking.[55] *Carpenter* enshrines the reasoning of the *Jones* concurrences in a majority opinion. It also gains the support of Justice Roberts while losing that of Justice Alito. But its general approach was largely laid out in the previous case.

To be sure, *Carpenter* required the Court to confront the third-party doctrine more squarely than *Jones* did. The Court's explicit limitation of that doctrine is a massive victory for privacy in the digital age. But *Carpenter* is not the first indication that the third-party doctrine may matter only in a limited set of contexts. Indeed, the third-party doctrine has not been applied by the Court since 1979, and has at times seemed to disappear whenever it would lead to an undesirable result.

Supposedly, the third-party doctrine dictates that exposure of something to a third party eliminates Fourth Amendment protection in that thing.[56] Yet in *Ferguson v. City of Charleston*, the Court held that a state hospital's program of

---

[50] *Id.* at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations … The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility."); *id.* at 429 (Alito, J., concurring in the judgment) ("Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap…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").

[51] *Carpenter*, 138 S.Ct. at 2215.

[52] *Id.* at 2217.

[53] *Id.* at 2218.

[54] *Id.* at 2216 (noting that both forms of tracking data "are detailed, encyclopedic, and effortlessly compiled")

[55] *Id.* at 2220.

[56] *See* United States v. Miller, 425 U.S. 435, 442 (1976).

testing patients' urine for cocaine violated the Fourth Amendment, despite the fact that patients voluntarily turned over their urine to hospital employees.[57] In *Stoner v. California*, the Court held that the police must obtain a search warrant to enter a hotel room despite the fact that "maids, janitors, or repairmen" routinely enter and observe the room in the normal course of business.[58] Similarly, in *Jones*, the routine exposure of one's car to members of the public was insufficient to eliminate Fourth Amendment protection in the car's location over time.[59] In each case, the disclosure of information to third parties was overcome by other considerations, much as it would be in *Carpenter*.

Moreover, even the Court's famous third-party doctrine cases *Miller* and *Smith* did not turn entirely on third party exposure.[60] Both considered at length "the nature of the particular documents sought" and both emphasized the unrevealing and non-intimate nature of the information obtained.[61] Thus *Smith* noted that dialed phone numbers were not "the contents of communications," and revealed "neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed."[62] *Smith* also held that the government could intercept phone numbers dialed for local calls, even though no third party recorded these numbers.[63] *Miller* likewise stressed that bank deposit slips were not "private papers" and checks were "not confidential communications but negotiable instruments to be used in commercial transactions."[64] Even at the apex of the third-party doctrine's influence, the relatively unrevealing nature of deposit slips and dialed phone numbers may have

---

[57] Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001). The court granted certiorari only on the issue of whether the testing met the special needs exception and assumed a lack of patient consent, but the dissenting Justices noted that the patients' consent was obvious and provided a clear basis to resolve the case. *Id.* at 76; *id.* at 92–96 (Scalia, J., dissenting).

[58] 376 U.S. 483, 489–90 (1964).

[59] United States v. Jones, 565 U.S. 400, 410 (2012).

[60] *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (discussing this aspect of *Miller* and *Smith*).

[61] Smith v. Maryland, 442 U.S. 735, 742 (1979) (noting the non-intimate nature of dialed phone numbers); *Miller*, 425 U.S., at 442 (focusing on the non-sensitive "nature of the particular documents sought."

[62] Smith, 442 U.S., at 741.

[63] *Id.* at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.").

[64] *Miller*, 425 U.S., at 442.

played a larger role than their disclosure to bank employees or telephone companies.[65]

Indeed, while the third-party doctrine has only mattered intermittently in cases involving exposure of information to third parties, judicial consideration of the revealing, comprehensive, or intimate nature of surveillance has been a through-line of the Court's Fourth Amendment jurisprudence. This is especially clear in recent cases like *Carpenter* and *Jones*, where the uniquely difficult questions posed by location surveillance have compelled the Court to examine factors relating to privacy harm in detail.[66] But consideration of similar factors can be found throughout the *Katz* test cases. Examples include *Bond v. United States*'s evaluation of the sensitivity of carry-on luggage,[67] *Florida v. Riley's* assessment of the "intimate details connected with the use of the home or curtilage,"[68] and *United States v. Knotts*'s discussion of the possibility of "twenty-four hour surveillance of any citizen."[69] In *United States v. Dunn*, the Court concluded that police could visually inspect a barn because they "possessed objective data indicating that the barn was not being used for intimate activities of the home."[70] In *Dow Chemical Co. v. United States*, it determined that the surveillance of commercial property via sophisticated camera equipment was not a Fourth Amendment search because the "photographs here are not so revealing of intimate details as to raise constitutional

---

[65] See Tokson, supra note 9, at 598–600.

[66] *See Carpenter*, 138 S.Ct. at 2218 ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations … 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."); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society."); *Id.* at 430 (Alito, J., concurring in the judgment) ("[S]ociety'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.").

[67] 529 U.S. 334, 337–338 (2000).

[68] 488 U.S. 445, 452 (1989).

[69] 460 U.S. 276, 283 (1983).

[70] 480 U.S. 294, 302 (1987).

concerns."[71] In *United States v. Place*, it emphasized the limited amount of information disclosed by a drug dog sniff.[72] Numerous other *Katz* test cases have relied upon similar considerations.[73]

As I have argued elsewhere, the intimacy of the place or thing targeted by a surveillance practice, the amount of information sought, and the cost of the investigation are especially important factors driving the outcomes of the Court's Fourth Amendment cases.[74] Indeed, the Court's rulings appear to track these factors in the vast majority of its "reasonable expectation of privacy" decisions to date.[75] Ultimately, these principles are a means of assessing the extent of the privacy harm that a surveillance practice is likely to cause. This assessment

---

[71] 476 U.S. 227, 238 (1986).

[72] 462 U.S. 696, 707 (1983) (noting that the information obtained was "limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure").

[73] *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) ("In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989) ("In light of our society's concern for the security of one's person, it is obvious that this physical intrusion, penetrating beneath the skin, infringes an expectation of privacy that society is prepared to recognize as reasonable. The ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested employee's privacy interests…."It is not disputed … that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic."); O'Connor v. Ortega, 480 U.S. 709 (1987) (plurality) ("The undisputed evidence discloses that Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos."); Oliver v. United States, 466 U.S. 170 (1984) ("[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields."); Rawlings v. Kentucky, 448 U.S. 98 (1980) ("At the time petitioner dumped thousands of dollars worth of illegal drugs into Cox's purse, he had known her for only a few days. According to Cox's uncontested testimony, petitioner had never sought or received access to her purse prior to that sudden bailment."); Terry v. Ohio, 392 U.S. 1 (1968) (police pat-downs are a "serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and [are] not to be undertaken lightly").

[74] Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 Geo. Wash. L. Rev. (forthcoming 2020).

[75] *Id.*

powerfully and consistently influences the Supreme Court's Fourth Amendment jurisprudence.

Carpenter is another in a long line of cases where the substantial privacy harms threatened by surveillance practices outweighed any disclosure to third parties,[76] positive law analysis,[77] or empirical claim about expectations.[78] Its enormous contributions to Fourth Amendment law do not stem from any drastic changes to the Court's conceptual approach. Rather, *Carpenter* makes the Court's approach clearer, gives lower courts more guidance on how to address third-party doctrine questions, and describes how low-cost, revealing, comprehensive surveillance techniques threaten citizen privacy.

III. THE NEXT GENERATION OF FOURTH AMENDMENT ISSUES

Carpenter protects individuals from extensive location monitoring and expressly limits the reach of the third-party doctrine. It does so largely on the basis of a practical examination of how revealing and extensive location tracking can be. Looking forward, it suggests that the Court will protect privacy in several other forms of digital information that are likewise revealing and low-cost.

Of course, the composition of the Court will impact the outcomes of future cases. As currently constituted, there appear to be at least five votes for the harm-focused approach observed in *Carpenter*. Justice Gorsuch also appears to be concerned about new surveillance technologies and citizen privacy, and may be willing to apply the Fourth Amendment to novel surveillance practices, albeit under a very different theory than the other Justices. His opinions as a Tenth Circuit judge tend to favor privacy rights, sometimes to a remarkable degree.[79] His

---

[76] *See Carpenter*, 138 S.Ct. at 2223; Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001); Stoner v. California, 376 U.S. 483, 489 (1964).

[77] See Oliver v. United States, 466 U.S. 170, 183-84 (1984); see also California v. Greenwood, 486 U.S. 35 (1988).

[78] Illinois v. Caballes, 543 U.S. 405, 408-09 (2005); Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); United States v. White, 401 U.S. 745, 751-52 (1971) (plurality).

[79] *See* United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) (concluding that the automated scanning of email for child pornography constituted a trespass and thus triggered the Fourth Amendment, despite a lack of precedent for the proposition that electronic activity that does not interfere with the function of a computer system is a trespass to chattels); United States v. Carloss, 818 F.3d 988, 1003–1015 (Gorsuch, J., dissenting) (arguing that the Fourth Amendment required a warrant before police could

dissent in *Carpenter* suggested that Carpenter likely had a property right and thus a Fourth Amendment right in his location information.[80] Indeed, Gorsuch "reluctantly" ruled against Carpenter largely because his counsel did not raise, and thus forfeited, any property-based argument.[81]

It is difficult to identify any existing concept of property rights that would extend to business records created by one's cell phone company. However, if Gorsuch further develops the theory of property rights in data and electronic signals hinted at in his previous opinions,[82] he may become an important supporter of an expansive Fourth Amendment scope.

In the meantime, the majority of the Court is likely to continue to apply the *Katz* test and the general approach seen in *Carpenter* to the next wave of Fourth Amendment search cases. My goal for the remainder of this lecture is to give a preview of some of the issues that the Court is likely to confront in its upcoming Fourth Amendment cases.

A. Websurfing Data

Records of the websites that a user visits can be collected by a variety of internet service providers (ISPs) or third-party entities.[83] For instance, ISPs generally maintain logs of the IP addresses of each website a user visits along with the volume of data transmitted to and from the user.[84] Some service providers monitor and retain the URL of each individual page visited by a user.[85] Affiliated groups of websites may collect the URLs of each page a user sees within their group.[86] Some entities place "web beacons" on affiliated websites that track in

---

knock on a homeowner's door to ask him questions when the homeowner had posted "No Trespassing" signs on his lawn).

[80] See Carpenter v. United States, 138 S. Ct. 2206, 2261–2272 (2018).

[81] Id. at 2272.

[82] See *id.*; see also *Ackerman*, 831 F.3d 1292; *Carloss*, 818 F.3d 988.

[83] *See, e.g.*, Tokson, Automation, supra note 9, at 588, 603; Peter Segrist, *How the Rise of Big Data and Predictive Analytics are Changing the Attorney's Duty of Competence*, 16 N.C. J.L. & TECH 527, 542–43 (2015).

[84] Tokson, supra note 9, at 603.

[85] See, e.g., Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1424–25, 1432–38.

[86] See, e.g., Omer Tene, *What Google Knows: Privacy and Search Engines*, 2008 UTAH L. REV. 1433, 1447–48.

granular detail the user's activity on a particular site.[87] These service providers and website networks can use this information to target advertisements to the individual user or sell the information to third-party advertisers.[88]

The government has surveilled citizens' websurfing activity and introduced evidence of it in several criminal cases. For instance, in *United States v. Forrester*, government agents installed a "mirror port" on a suspect's account with an ISP, enabling them to record the IP addresses of the websites that he visited and the total volume of information sent to or from his account.[89] The Ninth Circuit held that this was not a Fourth Amendment search, because internet users have no reasonable expectation of privacy in web surfing information disclosed to a third-party ISP.[90] In *United States v. Ulbricht*, law enforcement agents collected IP address data to and from a suspect's wireless router and used the data to help link the suspect to an anonymous internet profile.[91] The Second Circuit ruled that this was not a search, again because users had no privacy rights in data disclosed to a third party's servers.[92]

As law enforcement officials continue to track users' internet use in criminal investigations, more circuit courts will rule on this issue, and the Supreme Court may ultimately be forced to resolve it. How is it likely to do so?

Ultimately, the Supreme Court is likely to protect IP addresses and other web surfing information against government surveillance. Such records can be deeply revealing, especially in the aggregate.[93] Scholars have raised concerns about the detailed surveillance of citizens' reading habits, which have the potential to chill fundamental freedoms of thought and speech.[94]

IP addresses, to be sure, typically disclose only the general websites with which a user communicates.[95] But knowledge of which websites a user contacts, when and how long they do so, and how much information is sent back and forth

---

[87] See Segrist, supra note 81, at 542–43.
[88] *See* Tokson, supra note 9, at 603.
[89] United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2008).
[90] *Id.* at 510.
[91] United States v. Ulbricht, 858 F.3d 71, 83–84 (2d Cir. 2017).
[92] *Id.* at 96
[93] *See, e.g.*, Ohm, Many Revolutions, at 23 (draft on file).
[94] *See,e.g.*, *id.*; Neil M. Richards, *Intellectual Privacy*, 87 Tex. L. Rev. 387, 436 (2008).
[95] *See* Matthew J. Tokson, The Content/Envelope Distinction in Internet Law, 50 WM. & MARY L. REV. 2105, 2148 (2009).

has the potential to reveal the subject matter and often the content of the user's web surfing communications and activities.[96] Even if government agents cannot know with utter certainty what an internet user is reading or seeing, compiling records of the IP addresses that users visit offers the government a revealing and invasive look into users' personal habits, interests, and communications.[97]

The disclosure of such information to third parties is unlikely to eliminate its Fourth Amendment protection. Much as it did in *Carpenter*, the Court is likely to declare that the revealing and comprehensive nature of web surfing data poses high risks of serious privacy violations and thus requires special protection. In such cases, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[98] Moreover, while users do disclose the IP addresses they visit to their ISPs, such disclosure is hardly avoidable in the modern world, where web surfing is as routine and as essential as reading paper media or visiting retail stores.[99] Nor is it likely that most internet users have even the most basic awareness of how internet routing, IP addresses, or TCP/IP protocols work.[100] If a voluminous record of the places where citizens travel in public is too private for the government to obtain without a warrant, the same is likely to apply to a voluminous record of everywhere they travel in cyberspace.

B. Smart Homes

Increasingly, our homes are filled with internet-connected devices, from "smart" speakers like Amazon's Alexa, to Roomba vacuums, to internet connected refrigerators and other appliances. These items can be useful and fun, but nearly all of them collect a great deal of data about their users. This data may be especially sensitive, as it is gathered from inside the home and/or from items worn on users' bodies. Although courts do not yet appear to have opined on whether a warrant is required for police officers to gather such data from service providers or other intermediaries, officers have begun to collect it during criminal

---

[96] *See id.* at 2148–51.

[97] *See id.*

[98] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

[99] See Kerr book, draft at 47.

[100] *See generally* Matthew Tokson, Knowledge and Fourth Amendment Privacy, 111 Nw. U. L. Rev. 139 (2016) (discussing knowledge of new technologies and how it pertains to a person's reasonable expectation of privacy).

investigations.

For example, one man was indicted for murdering his houseguest after his smart utility meter indicated that he had used a large amount of water late at night, possibly to hose down the murder scene.[101] Prosecutors also sought recordings made by the man's Amazon Echo.[102] Another man was charged with murdering his wife after her Fitbit data showed her moving around after she had supposedly been killed by an intruder, and his key fob showed that he was home after he claimed to have left for work.[103] And a suspect charged with aggravated arson and insurance fraud ran into trouble when data obtained from his pacemaker contradicted his story of smashing his bedroom window and fleeing after being awoken by a fire.[104]

The potential for government officials to obtain data about the inside of citizens' homes has raised serious concerns among scholars and commentators.[105] *Carpenter* itself does not address smart home devices, and future courts could easily distinguish them from cell phone tracking. Cell phones are ubiquitous in modern life, and the disclosure of cell phone users' locations happens automatically and likely without cell phone users' knowledge.[106] Most smart

---

[101] Haley Sweetland Edwards, Alexa Takes the Stand: Listening Devices Raise Privacy Issues, Time, May 4, 2017, http://time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues.

[102] *Id.* The charges against Bates were eventually dropped at the prosecutor's request. Nicole Chavez, *Arkansas judge drops murder charge in Amazon Echo case*, CNN.com, Dec. 2, 2017, https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html

[103] Justin Jouvenal, *Commit a crime? Your Fitbit, key fob or pacemaker could snitch on you*, WASHINGTON POST, Oct. 9, 2017, https://www.washingtonpost.com/local/public-safety/commit-a-crime-your-fitbit-key-fob-or-pacemaker-could-snitch-on-you/2017/10/09/f35a4f30-8f50-11e7-8df5-c2e5cf46c1e2_story.html?utm_term=.88b43a23d1ef.

[104] Lauren Pack, *Arson suspect in unique case featuring pacemaker data is back in custody*, THE JOURNAL-NEWS, July 24, 2018, https://www.journal-news.com/news/arson-suspect-unique-case-featuring-pacemaker-data-back-custody/dn6JyzsOemZovpayJMZLNJ/

[105] *See* Andrew Guthrie Ferguson, The "Smart" Fourth Amendment, 102 Cornell L. Rev. 547, 603 (2017) (describing various smart devices and police interest in the data they generate); Neil M. Richards, The Dangers of Surveillance, 126 HARV. L. REV. 1934, 1936–40 (2013) (discussing how the Internet of Things is "subjecting more and more previously unobservable activity" to observation).

[106] Carpenter v. United States, 138 S. Ct. 2206, 2270 (2018); Mathew Tokson, Knowledge and Fourth Amendment Privacy, 111 Nw. U. L. Rev. 139, 187 (2016).

home devices remain very much optional, and even popular devices such as smart speakers (like Alexa) are found in fewer than a quarter of US households.[107] Moreover, when users engage with smart speakers, it is relatively clear that they are disclosing information directly to an internet-connected device.[108] Because the disclosure of information to third parties is more volitional and less automatic in the smart home context than with cell phones, it is certainly possible that a future court would hold that the third-party doctrine eliminates Fourth Amendment rights in information disclosed to smart home devices.

This is, however, an unlikely outcome. First, the Supreme Court has protected the privacy of the home in a wide variety of cases, even against relatively minimal privacy intrusions[109] and even when precedent or logic appeared to dictate a different result.[110] Second, *Carpenter*'s discussion of voluntary disclosure takes up only a tiny portion of the majority opinion, and the issue does not appear to greatly concern the Justices.[111] And finally, the enormous privacy harms that would result from warrantless government surveillance of recordings and other sensitive information from the inside of people's homes are likely to motivate the Court to distinguish or disavow any prior doctrines that would counsel against declaring such surveillance a Fourth Amendment search. Even more so than the surveillance in *Carpenter*, obtaining recordings of people's homes could be extremely revealing and could paint a comprehensive picture of their private

---

[107] Micah Singleton, Nearly a Quarter of U.S. Households Own a Smart Speaker, According to Nielsen, THE VERGE, Sep. 30, 2018, https://www.theverge.com/circuitbreaker/2018/9/30/17914022/smart-speaker-40-percent-us-households-nielsen-amazon-echo-google-home-apple-homepod

[108] To be sure, users may not understand in any meaningful way that their information is stored on third-party servers.

[109] *See* Arizona v. Hicks, 480 U.S. 321, 329 (1987); Kyllo v. United States, 533 U.S. 27, 41 (2001).

[110] *See* Florida v. Jardines, 569 U.S. 1, 7–10 (2013) (holding that a drug dog sniffing the air outside of a home was a search despite the lack of any actionable trespass, which *United States v. Jones* had seemed to require, and despite several precedents holding that dog sniffs of personal properties were not searches); United States v. Karo, 468 U.S. 705, 720 (1984) (holding that tracking a radio beeper inside of can inside of a home was a search despite the imprecision of the beeper, which revealed only the can's presence in the general area of the house, and the Court's conclusion that police could lawfully track the beeper until it entered the house and as soon as it left).

[111] Carpenter, 138 S. Ct. at 2220.

lives.[112] The Court is again likely to address these concerns, regardless of what a strict application of the third-party doctrine might dictate.

C. Pole Cameras

Pole cameras refer to cameras placed on utility poles or street lights for the purpose of observing persons or property. Such cameras are widely used in cities throughout the country, and have been employed by federal agencies as well as local police departments.[113] Perhaps the most interesting legal question arising from the use of pole cameras involves cameras that constantly record video of the exterior of a residence and its curtilage. Although most courts have held that long-term video surveillance of the exterior of a home is not a search, other courts disagree.[114] Moreover, lower courts may be less reluctant to find that pole cameras are a search in the post-*Carpenter* era. In any event, it is somewhat likely that the issue of pole camera surveillance of residential property will eventually reach the Supreme Court.

The facts of pole camera cases may vary, as the cameras may be covert or obvious, may observe the entirety of a suspect's yard or just a portion, and may capture video for a few weeks or several months.[115] Typically, the cases involve

---

[112] *See id.* at 2217–18 (discussing GPS's ability to expose the "privacies of life."); Austin Carr, et al., *Silicon Valley Is Listening to Your Most Intimate Moments*, BLOOMBERG BUSINESSWEEK, Dec. 11, 2019 (discussing the "intimate" and "intense" Alexa recordings that Amazon employees listened to and analyzed).

[113] Timothy Williams, *Can 30,000 Cameras Help Chicago's Crime Problem?*, THE NEW YORK TIMES (May, 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html; Justin Rohrlich & Dave Gershgorn, The DEA and ICE are Hiding Surveillance Cameras in Streetlights, QUARTZ (Nov. 9, 2018), https://qz.com/1458475/the-dea-and-ice-are-hiding-surveillance-cameras-in-streetlights/.

[114] Compare United States v. Vargas, No. CR-13-6025-EFS, at *27 (E.D. Wash. Dec. 15, 2014) (suppressing evidence from a pole camera used to record the outside of an individual's home for six weeks), and South Dakota v. Jones, 903 N.W.2d 101, 111 (S.D. 2017) (holding that long-term video monitoring of the area around a mobile home was a search), with United States v. Cantu, 684 F. App'x 703, 705 (10th Cir. 2017) (holding that video surveillance of the outside of a house was not a search); United States v. Bucci, 582 F.3d 108, 116 (1st Cir. 2009) (same), and United States v. Gilliam, No. 02:12-CR-93, 2015 WL 5178197, at *9 (W.D. Pa. Sept. 4, 2015) (same).

[115] *See, e.g.*, United States v. Stefanyuk, 2018 U.S. Dist. LEXIS 110080 (D.S.D.) (police installed a high-definition camera for two weeks); United States v. Kay, 2018 U.S. Dist. LEXIS 142861 (E.D. Wisc.) (police used a pole camera to video surveil as suspect's home for eighty-seven days, but the camera was largely pointed at the driveway rather than the

monitoring a front yard for several weeks or more, from a vantage point not meaningfully different from that of a passerby on a public street.

In general, cases holding that video surveillance of the exterior of a home is not a search conclude that defendants have no reasonable expectation of privacy because the exterior of their home is exposed to the public.[116] Yet *Carpenter* rejected similar reasoning about the exposure of information. The Court emphasized that mere exposure of something to third parties will not necessarily render it unprotected by the Fourth Amendment. When a surveillance practice is especially invasive, comprehensive, and/or inescapable, it may be prohibited by the Fourth Amendment regardless of whether the information it captures might in theory be observed by others.[117]

Courts finding the use of pole cameras to be a search generally focus on the continuous, long-term nature of the surveillance at issue. Pole cameras capture "activities outside [the] home twenty-four hours a day."[118] Such surveillance is "electronic," "continuous," "intrusive[]," far lower in cost, and easier to hide than traditional, in-person surveillance.[119] Further, as one court noted,

> [T[his type of surveillance does not grow weary, or blink, or have family, friends, or other duties to draw its attention. Much like the tracking of public movements through GPS monitoring, long-term video surveillance of the home will generate "a wealth of detail about [the home occupant's] familial, political, professional, religious, and sexual associations."[120]

These observations echo those later made by the Supreme Court in *Carpenter*. Justice Roberts's opinion for the Court expressed concern about the continuous and voluminous nature of cell phone tracking, which "provides an all-encompassing record of the [user's] whereabouts" and does so "at practically no expense."[121] Cell phone tracking, like continuous video monitoring, is "not about

---

house); United States v. Garcia-Gonzalez, 2015 U.S. Dist. LEXIS 116312 (D. Mass.) (police monitored a house and apartment building with a pole camera for seven months).

[116] *See,e.g.*, *Bucci*, 582 F.3d at 117.

[117] *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[118] South Dakota v. Jones, 903 N.W.2d 101, 112 (S.D. 2017)

[119] United States v. Vargas, 2014 U.S. Dist. LEXIS 184672, *22, *26 (E.D. Wash 2014).

[120] State v. Jones, 2017 SD 59, *P36 (S.D. 2017) (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor , J., concurring) (alteration in original)).

[121] *Carpenter*, 138 S. Ct. at 2217.

… a person's movement at a particular time."[122] Rather, it creates "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years," and is accordingly a Fourth Amendment search, even if momentary or in-person tracking of a suspect would not be.[123]

The resonances between *Carpenter* and the cases holding long-term pole camera surveillance unconstitutional suggest the Court is likely to rule that such surveillance violates the Fourth Amendment. Although one's movements in public are in theory observable by others, the constant tracking of a person's movements for long periods of time by technological means violates their reasonable expectations of privacy.[124] Similarly, although a house and its curtilage are in theory exposed to public view, people reasonably expect that their houses will not be constantly surveilled for weeks or months by a hidden camera. While the outcome of the pole camera issue remains uncertain, especially given the many lower court precedents upholding their warrantless use, it is ultimately probable that the Supreme Court will find long-term pole camera surveillance of a residence to be a Fourth Amendment search.

D. Drones

A drone is an unmanned aircraft guided by remote control or an onboard computer. Law enforcement and other public safety agencies in 49 states have acquired drones for various uses.[125] The most widely owned model used by such agencies has a 20-megapixel camera capable of shooting high resolution video or still photos.[126] It can be controlled at a distance of 4.3 miles and has a top speed of 45 miles per hour.[127] Like most drones operated by public agencies, its surveillance capabilities are somewhat limited by its maximum flight time of thirty minutes.[128] Still, drone capabilities are improving, and many military-grade drones can

---

[122] *Id.* at 2220.
[123] *Id.*
[124] *Id.* at 2217; United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).
[125] Dan Gettinger, *Public Safety Drones An Update*, at 3 (May 2018), https://dronecenter.bard.edu/files/2018/05/CSD-Public-Safety-Drones-Update-1.pdf.
[126] *See id.*
[127] https://www.dji.com/phantom-4-pro
[128] *Id.*

remain airborne for several days.[129] Some commercially available drones offer autopilot modes, including modes that allow for constant camera surveillance of a specific building, object, or location.[130]

In the 1980s, the Supreme Court heard cases involving airplane and helicopter surveillance, and these rulings are relevant to the Fourth Amendment status of drones. In *California v. Ciraolo*, police officers chartered an airplane that flew 1,000 feet over Ciraolo's property, and the officers visually observed marijuana plants in Ciraolo's back yard.[131] The Court held that visual observation of the curtilage of a home from an airplane operating in publicly navigable airspace was not a Fourth Amendment search because it did not violate Ciraolo's reasonable expectations of privacy.[132] The Court reached a similar holding in *Florida v. Riley*, concluding that visual observation from a lawfully operated helicopter was not a Fourth Amendment search.[133] In both cases, the Court emphasized that the aircraft were operated in compliance with applicable regulations, and suggested that only unlawful flights would violate people's reasonable expectations of privacy.[134]

The likely outcome of a future drone surveillance case will depend on the particular facts. If police officers were to lawfully operate a drone in order to surveil a suspect's yard for half an hour, it is likely that the Court would find such surveillance constitutional under *Ciraolo* and *Riley.* Although such surveillance would be cheaper than helicopter or airplane surveillance, it would still be analogous to observation by a manned aircraft. It is unlikely that any differences

---

[129] *See* Luke Dormehl, *7 Drones that can stay airborne for hours—and the tech that makes it possible*, Digital Trends (Oct. 9, 2018), https://www.digitaltrends.com/cool-tech/drones-with-super-long-flight-times; Praveen Duddu, *The 10 longest range unmanned aeriel vehicles (UAVs)*, Air Force Tehnology (Nov. 19, 2013), https://www.airforce-technology.com/features/featurethe-top-10-longest-range-unmanned-aerial-vehicles-uavs.

[130] *See See, e.g.*, Klint Finley, *World's Smallest Drone Autopilot System Goes Open Source*, WIRED (Aug. 28, 2013), https://www.wired.com/2013/08/drone-autopilot; https://www.dji.com/inspire-1/app#autopilot;

[131] *California v. Ciraolo*, 476 U.S. 207, 209 (1986).

[132] *Id.* at 213–14.

[133] *Florida v. Riley*, 488 U.S. 445 (1989); *see also* Dow Chemical Co. v. United States, 476 U.S. 227 (1986) (holding that taking precision photographs of a factory from an airplane was not a Fourth Amendment search).

[134] Riley, 488 U.S. at 451 ("We would have a different case if flying at that altitude had been contrary to law or regulation."); Dow Chemical, 476 U.S. at 239 ("it is open to the view and observation of persons in aircraft lawfully in the public airspace").

between piloted aircraft and manually flown drones would be important enough to distinguish the Court's prior cases. It would also be relatively easy for the officers to comply with federal drone regulations, which set no minimum height for drone flight.[135] The regulations do prohibit drone flights during night hours, but drone operators can apply for a waiver so long as they demonstrate that the operation can be conducted safely.[136] Some state laws prohibit drone surveillance without a warrant, but most do not.[137]

Continuous, auto-piloted drone surveillance for an extended period of time would likely yield a different result. Prolonged visual surveillance of a person's curtilage would begin to resemble the comprehensive, invasive surveillance that the Court identified in *Carpenter* and the *Jones* concurrences.[138] The government could obtain a detailed record of the homeowner's comings and goings, who visited their home and when, and any actions they or their family members take in their front or back yard. As with extended location monitoring in public, observers could build up a revealing dossier of information about an individual's associations and activities around and (via inference) inside of their home.[139] It is unlikely that the Court would allow such harmful government surveillance to go unregulated, even if the drone flight complied with all applicable laws and regulations. Just as the third-party doctrine did not eliminate citizens' privacy interests against cell phone location tracking, mere compliance with drone regulations is unlikely to eliminate homeowners' privacy interests against extended video surveillance of their curtilage. In other words, the Court would likely require the police to obtain a warrant before engaging in extended drone surveillance of a suspect's yard.

---

[135] 14 C.F.R. § 107.1–107.205.

[136] 14 C.F.R. § 107.29, § 107.205.

[137] National Conference of State Legislatures, *Taking Off: State Unmanned Aircraft Systems* 14 (2016), *http://www.ncsl.org/Portals/1/Documents/transportation/TAKING_OFF-STATE_%20UNMANNED_%20AIRCRAFT_SYSTEMS_%20POLICIES_%20%28004%29.pdf*; National Conference of State Legislatures, *Current Unmanned Aircraft State Law Landscape*, Sep. 10, 2018, http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

[138] *See supra* note 123.

[139] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 ("revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'") (quoting Jones v. United States, 565 U.S. 400, 415 (2012).

Predicting the future of Fourth Amendment law is necessarily an uncertain and imprecise endeavor. The composition of the Court could change, the Justices could change their minds, or the law itself could be transformed by subsequent cases. There is likewise no guarantee that the surveillance technologies described above will reach the Court, or that other, as yet unknown techniques will not supersede the ones described here.

Looking toward the future is nonetheless important, especially in the surveillance context. In doing so, "[t]he best way to suppose what may come, is to remember what is past."[140] The next wave of Fourth Amendment challenges is likely to come from technologies that are increasingly ubiquitous, like drones and smart devices, and those on which lower courts have already ruled, like web surfing and pole cameras. And the Court's approach in future cases is likely to be an extension of its approach in previous cases that dealt with then-novel surveillance technologies.

When law enforcement practices capture information that is particularly revealing or comprehensive, and thereby threaten too much harm to citizens' privacy, the Court is likely to require a warrant under the Fourth Amendment. This is true regardless of doctrines or precedents that seem to point in the other direction—though such doctrines may still play a role in borderline cases. *Carpenter* is hardly the first case to exemplify the Court's concern with the nature and extent of the harms caused by modern surveillance. It is nonetheless a major step forward for privacy, and the clearest indication yet that the Fourth Amendment will maintain its relevance in the digital age.

[140] GEORGE SAVILE, POLITICAL, MORAL, AND MISCELLANEOUS REFLECTIONS (1750).