© Alexandr Mitiuc | AdobeStock

The Fourth Amendment and Data: Put Privacy Policies in the Trial Record

One of the Supreme Court's most important recent Fourth Amendment cases, *Carpenter v. United States*,[1] dealt with government agents' access to suspects' cellular telecommunications data. The Court ruled 5-4 for the defendants, finding that access to the data in this particular case required a warrant. That is well and good for the criminal defense bar, but not good enough. In other recent cases dealing with data and technology, the Court has been unanimous in finding that a search invaded the right protected by the Fourth Amendment.[2] The *Carpenter* Court was closely divided, with several Justices moving from pro-defendant to the prosecution's side.

The solo dissent of Justice Neil Gorsuch is probably clearest about what the *Carpenter* dissenters want when defendants' counsel raise Fourth Amendment claims about data. He lamented how "rusty" American courts have become with applying the "traditional" approach to the Fourth Amendment, and he faulted Carpenter's counsel for declining to articulate and press a vigorous claim that the defendant had property rights in his telecommunications data. "I cannot help but conclude," he wrote, "that Mr. Carpenter forfeited perhaps his most promising line of argument."

When the prosecution uses data retrieved from digital service providers such as phone companies and internet service providers ("ISPs"), defense counsel should put the privacy policies and terms of service statements of such providers in the trial record. That is the starting point for answering Justice Gorsuch, because it creates a foundation for arguing that defendants have property rights in their digital papers and effects. Common law property rights are a lynchpin for arguing wrongful search and seizure of data to judges and Justices with a conservative bent.

Arguably, not only Gorsuch, but each of the four dissenters in *Carpenter* — including Justices Kennedy, Thomas, and Alito — could have been brought to the defense's side if counsel had argued the "traditional" property-rights approach based on state common law and contract. If America's trial and appellate judges are anything like the Supreme Court, half or more may be receptive to something other than the "reasonable expectation of privacy" test. So put that privacy policy in the record.

Katz Has Gone to the Dogs

The phrase "reasonable expectation of privacy" is deeply embedded in the minds and language of practitioners, judges, academics, and the public. It was Justice Harlan's solo concurrence in *Katz v. United States* that gave rise to the phrase.[3] Using his formulation, courts have come to equate "search" under the Fourth Amendment with whatever investigatory activ-

BY JIM HARPER

ities upset privacy mores that judges and justices see as widely legitimate.

Both the language and logic of the "reasonable expectation of privacy" test are backward, and a great deal has been written to show it.[4] In its natural sense, a "search" is composed of the actions an investigator takes to locate particular items and to discover information relevant to an investigation. The Fourth Amendment asks whether those actions are reasonable. It does not invite inquiry into whether defendants or members of the public are reasonable in wanting or expecting privacy.

The *Katz* test is more sociological than juridical. It requires judges to make broad pronouncements about privacy, often in cases where rapidly changing technology makes such judgments almost impossible. The result is an endlessly malleable test. As often as courts find that there was a search because privacy has been invaded, they find no search, even when there has been highly directed examination or data-gathering, because it does not offend their stated sense of privacy.[5]

The Search for an Alternative to *Katz*

An important break from "reasonable expectations" occurred in 2001 with the decision in *Kyllo v. United States*.[6] There, Justice Scalia avoided using *Katz* doctrine in finding for the Court that the use of a thermal imager to examine the heat profile of a home was a search. Since the Court's 2014 opinion in *United States v. Jones*,[7] it has been clear that the "traditional" approach to the Fourth Amendment is an important alternative to *Katz*.

Jones assessed the government's use of GPS location tracking on a car. Justice Scalia again, writing for a plurality of the Court, sided with the defendant based on a property invasion that facilitated a high-tech search. Four other justices relied on *Katz*'s "reasonable expectation of privacy" doctrine to concur that there was a search requiring a warrant. A unanimous outcome with a divided rationale.

Carpenter was decided more recently, after the passing of Justice Scalia and his replacement with Justice Gorsuch. Chief Justice Roberts may be taking the lead on Fourth Amendment cases after Justice Scalia's passing. He likes the phrase "get a warrant."[8] But he arrived there in *Carpenter* using doctrine Justice Scalia had scrupulously avoided. The case was arguably retrenchment, with the majority lead by Roberts switching back to the "reasonable expectations" rationale, driving four Justices into dissent.

It may be that a Rubicon has been crossed and that the Court's other conservative appointees can no longer stomach "reasonable expectations." Justice Gorsuch's *Carpenter* dissent in particular called on the defense bar to bring concrete property arguments, fully fleshed out, to America's courts.

Put Privacy Policies in the Record

To answer Justice Gorsuch's call, defense counsel must enter some basic information into the record and prepare to argue for property rights in data at the trial stage. Put simply, if a case involves access to digital data held by any kind of service provider, that provider's privacy policies and terms of services statements should go into the record. This means not only telecommunications providers, ISPs, email service providers, search engines, and websites, but also financial services providers, health care providers, and any other service provider that gave information about a defendant to the government, having collected it or derived it from defendants' use of their services.

In the traditional or "property-rights" approach to Fourth Amendment protection, privacy policies and terms of service statements are contracts that allocate rights in digital data between the service provider and the customer. The heart of the typical privacy policy will say something like this: "Verizon does not sell, license or share information that individually identifies our customers, people using our networks, or website visitors."[9] This arguably creates a bailor-bailee relationship between the customer and the service provider. Importantly, the data is the customer's, which is essential for Fourth Amendment protection.

The contract typically contains a short list of exceptions: "We may, however, disclose your personal information to unaffiliated third-parties as follows:". Note the possessive pronoun. It is the customer's data, even though the service provider has possession. The list of exceptions typically includes a number of sensible reasons for sharing information and a provision allowing data sharing with government investigators. "We may disclose information that individually identifies our customers or identifies customer devices … to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law." As discussed below, this is not a free pass for handing data over to law enforcement. Defense counsel can show this through basic canons of contract interpretation, making sure to press the argument that the data is in relevant part the customer's.

With a privacy policy in the trial record, defense counsel are positioned to make the traditional property-based argument that any demand short of a warrant for accessing a defendant's data was defective. There is much work to be done to rehabilitate this approach and to adapt it to the modern digital age, of course, but in trial courts across the country, in appellate courts, and in as many as four Supreme Court chairs, there are judges and justices who are open to the argument that the Fourth Amendment protects defendants' data even when it is held by third-party service providers.

The 'Traditional' Fourth Amendment

It is a bit of a disservice to call a traditional or textual theory of Fourth Amendment protection the "property-rights" approach. What makes property relevant in the textual approach is the simple fact that the Fourth Amendment includes a short list of items — persons, houses, papers, and effects — that is set off by a possessive pronoun: "their." Defendants' claim to constitutional protection for any such item is restricted to the ones that they own or control as their own: their property.

The first phrase of the Fourth Amendment says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[10] Absent doctrine, courts would analyze its elements as follows:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of the defendant's person, house, papers, or effects?
- Was such a search or seizure reasonable?

If there was a search or seizure, if it was of the defendant's protected things, and if it was unreasonable, then the right has been violated. That "traditional" approach is actually quite clear and refreshing compared to the turgid and malleable "reasonable expectations" doctrine. Rather than

asking courts to opine on society-wide privacy expectations, it invites them to examine the reasonableness of law enforcement actions in the specific factual circumstances before them. This is something that courts are much more capable of doing.

With one exception, the textual elements of the Fourth Amendment are easily satisfied when the government has acquired and examined data about defendants from service providers. (It makes sense to look for seizures first and searches second. This is simply because seizures often precede searches in government investigations.)

If a case involves access to digital data held by any kind of service provider, that provider's privacy policies and terms of services statements should go into the record.

As to seizure, copying of data is a seizure for Fourth Amendment purposes. Doing so does not deprive anyone of possession, but leading Fourth Amendment scholar Orin Kerr has written that copying "freezes" evidence the way seizure of a suspect or crime scene does.[11] It stands to reason another way that there is a seizure when data goes to the government, as a service provider has handed over *something* and has done so on pain of sanctions.[12] The customer has lost something, too: the right to exclude others, which had been accorded to the customer by contract.

Blackstone defined property as "that sole and despotic dominion … exercise[d] over the external things … in total exclusion of the right of any other."[13] The U.S. Supreme Court has focused on exclusion as the critical property right. In *Loretto v. Teleprompter Manhattan CATV Corp.*, the Court called the right to exclude "one of the most treasured strands" of the property rights bundle.[14] *Kaiser Aetna v. United States* called it "one of the most essential sticks."[15] That property right is eviscerated when government takes data from a service provider that it held in trust for its customer.

Seizing and searching are distinct activities, and the distinction matters in some cases. When the government examines the data it has acquired, that activity is a search. While "seizure" is based in legal conclusions about property rights, there is no common law of "search." Natural language must guide whether looking (or other sensing) is so focused or directed that it crosses a threshold into the "search" category.

Kyllo v. United States[16] is a wonderfully instructive search case. In it, government agents aimed a thermal imager at a home to gather radiation from it in a nonvisible part of the electromagnetic spectrum. The thermal imager converted the radiation to visible images that showed unusual heat patterns coming off the garage and a side wall of Kyllo's home.

The data was not seized because it was an emanation available to anyone on the public sidewalk. But converting the invisible heat waves to visible form permitted observation and inferences about what was going on inside the home. "Where, as here, the government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion," the Court held, "the surveillance is a 'search' and is presumptively unreasonable without a warrant."[17] Professor Kerr confirms the analysis: "[T]he transformation of the existing signal into a form that communicates information to a person … constitutes the search."[18]

The next question is whether the thing seized or searched is on the Fourth Amendment's list of protected items. Though mutely, courts have generally updated the concepts of "papers" and "effects" to encompass changed information and communication technologies. It was not flat sheets of cellulose that the Framers sought to protect in the Fourth Amendment, obviously, but the common medium for storage and communication of information.[19]

United States v. Warshak is a rare example of a court being explicit about digital materials being papers. There, the U.S. Court of Appeals for the Sixth Circuit wrote: "Given the fundamental similarities between email and traditional forms of communications, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail."[20] In *Riley v. California*, Chief Justice Roberts twice referred in dictum to digital materials on cellphones as "effects."[21]

After seizure and search of papers or effects, the final step in the analysis is reasonableness. The Fourth Amendment strongly implies that getting a warrant is the reasonable thing to do when a seizure or search will occur in the absence of exigency. Chief Justice Roberts confirmed this in *Carpenter* (while leaving room for the rare warrantless search and for administrative searches): "Although the ultimate measure of the constitutionality of a governmental search is 'reasonableness,' our cases establish that warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing."[22]

That would essentially conclude a textual application of the Fourth Amendment to digital materials. But there is one dimension of the analysis just above that the prosecution is likely to strongly contest. That is the question of who owns the data that was seized and searched by law enforcement agents.

Whose Data Is It?

Justice Thomas put it well in *Carpenter*: "This case should not turn on 'whether' a search occurred. It should turn, instead, on *whose* property was searched."[23] Like Gorsuch, he lamented the paucity of argument on the part of the defense that the data was Carpenter's. "Carpenter stipulated below that the cell-site records are the business records of Sprint and MetroPCS. He cites no property law in his briefs to this Court, and he does not explain how he has a property right in the companies' records under the law of any jurisdiction at any point in American history."[24] In oral argument at the Supreme Court, Carpenter's counsel had actually warned against relying on contracts.[25]

To establish such property rights, counsel must be prepared to explain how privacy policies and terms of service statements, as contracts, allocate property rights in data to customers. To do so, one must return to the "bundle of sticks" notion of property rights taught in law school. Property rights are numerous, and they include the right to possession, the right to use, the right to profits, to sell, and so on. But they especially include the right to exclude others.[26]

Law-abiding technology users leave a tremendous amount of information and data in the hands of others, but all is not lost for them. Possession is with the service provider, but the right to exclude remains mostly with the customer, and that is an essential privacy protection.

A typical privacy policy will speak of the data as the customer's throughout. Verizon's privacy policy says in the very first paragraph, "The privacy of *your* information is a significant responsibility and we value the trust you place in us." The policy has a section titled, "How to limit the sharing and use of *your* information."[27] Justice Gorsuch suggests characterizing the relationship of the customer and service provider as that of a bailor and a bailee.[28]

The government will argue that there is an exception to the general rule against data sharing, and that the exception saves the government's acquisition and analysis of data via subpoena, statute, or regulatory demand. The heart of that exception typically reads something like this:

> We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as:
>
> ❖ to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law….

The prosecution may argue that these terms are descriptive and that statements about withholding data (subject to exceptions) are not contractual commitments to the customer. One has only to point to the prodigious litigation around privacy policies to show the weakness of this argument. The U.S. Federal Trade Commission treats privacy policies as creating enforceable commitments and regularly finds that companies deviating from the terms of their privacy policies have engaged in unfair and deceptive trade practices.[29]

The term allowing for disclosure to law enforcement will typically say or imply that the process must be "valid" (i.e., "to comply with valid legal process"). If not explicitly stated, counsel should be prepared to argue that validity is an implied term. Absurd results would obtain if a contract protecting the privacy of customers allowed information sharing pursuant to invalid law enforcement demands.

The requirement of a "valid" process appears to set up a battle between two equally good arguments. The defense should say that "valid" implies the constitutional standard of a warrant based on probable cause because it is the defendant's data being seized. The prosecution will say that a subpoena or other process is "valid" if it complies with the terms of whatever legislation or rule created it. "Valid" just means proper in form.

Contract interpretation breaks the tie in the defense's favor. According to the surplusage canon ("verba cum effectu sunt accipienda"), every word and every provision of a contract should be given effect, none should be ignored, and none should be given an interpretation that causes it to duplicate another provision or to have no consequence. If "valid" is interpreted only as "following a standard prescribed by law or rule," the provision has no consequence because any jurisdiction in the country — and perhaps in foreign countries — can require that the information be handed over based on any type of request and any standard. Until 2015, for example, the city of Los Angeles required hoteliers to make their records available "to any officer of the Los Angeles Police Department for inspection" with the simple caveat that it happen "at a time and in a manner that minimizes any interference with the operation of the business." The Supreme Court struck that law down because the process provided hoteliers with no opportunity for precompliance review, such as a motion to quash.[30]

On the other hand, if "valid" implies a constitutional standard, then the language means something. It accords something to the customer. It limits sharing of the customer's information to circumstances defined in the contract and fixed to concrete standards. It does not allow the terms of information sharing to be dictated by any legislation, rule, or command promulgated in any political jurisdiction where the service provider does business.

The "story" of the contract hangs together if the data is the customer's and the language requires a constitutional standard. The story of the contract falls apart if it has terms that give the customer nothing.

The traditional use for subpoenas is to require entities to bring their own documents and materials into court. The subpoena process naturally gives the owner of the materials notice of the demand and the power to refuse or contest it. The warrant process, on the other hand, is for gathering the information and evidence of parties who are not present to defend their interests or who must stand by as government agents collect evidence against their will. The warrant requirement introduces a neutral magistrate when an interested party cannot object to seizures and searches.

When data owned by a customer is taken from a service provider, the natural logic of the criminal discovery world is for a warrant to be required. Because of its contractual commitment, the service provider owes the customer insistence on a warrant that is legally valid in all respects, and it should reject overbroad and otherwise invalid warrants, too.

Bringing *Carpenter*'s Dissenters into the Fold

Few defense counsel will take a case to the Supreme Court, but it is not hard to imagine arguing before judges whose sympathies are with the *Carpenter* dissents. Arguably, each one of them could have been brought to the side of the defense had Carpenter's counsel argued for property rights founded in state common law. Defense counsel in data-based Fourth Amendment cases must do the same.

Justice Kennedy no longer serves on the Court, having been replaced by Justice Kavanaugh, but his dissent was premised on *Carpenter*'s lacking property interest in the data. "[I]ndividuals have no Fourth Amendment interests," he wrote, "in business records which are possessed, owned, and controlled by a third party."[31] He could write this because Carpenter's counsel gave short shrift to the property rights argument. Kennedy likely would have been far more circumspect, and may have joined the other side, had the case been made that Carpenter had property rights in his cell site data.

As earlier noted, Justice Thomas believed that the case turned on whose records were searched. Carpenter "did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them," Thomas wrote in the first page of his dissent. "Neither the terms of his contracts nor any provision of law makes the records his."[32] He could say this because Carpenter's defense declined to lay the groundwork for the full property rights argument.

Justice Alito noted during oral argument, "I guess we don't have the actual contract in the record here."[33] His opinion likewise rooted his objection in the presumption that Carpenter lacked property

rights in his data. For this reason, he objected to the Court's treatment of a subpoena ("requiring a party to look through its own records") as a search. He did not conceive of the records as Carpenter's, whose constitutional rights should be protected by the warrant requirement.[34] Justice Alito believed that the majority allowed a defendant to object to the search of a third-party's property.[35] Without sufficient argument that the data was Carpenter's, Alito was left to conclude this.

During oral argument, Justice Gorsuch asked Carpenter's counsel about developments in state courts that would substantiate the property rights argument. "[W]e placed the source of the property right here in federal law, not state law," counsel responded. In his dissent, Justice Gorsuch was as clear as possible about wanting defense counsel to argue state common law property and bailment.

> Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a bailment. A bailment is the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose." Black's Law Dictionary 169 (10th ed. 2014); J. Story, Commentaries on the Law of Bailments §2, p. 2 (1832) ("a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust"). A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the "implication[s] from their conduct" if they don't. 8 C. J. S., Bailments §36, pp. 468–469 (2017). A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion. *Id.*, §43, at 481; *see Goad v. Harris*, 207 Ala. 357, 92 So. 546, (1922); *Knight v. Seney*, 290 Ill. 11, 17, 124 N. E. 813, 815–816 (1919); *Baxter v. Woodward*, 191 Mich. 379, 385, 158 N. W. 137, 139 (1916).[36]

These are arguments that defense counsel should bring to court when government agents have procured data about defendants from service providers. They are a bite at the apple that Carpenter's defense counsel declined to take, and it cost as many as four Justices. In future cases, defense counsel should put the service providers' privacy policies and terms and conditions statements in the record. This permits the argument that data seized and searched by the government was by contract the property of the defendant, so a warrant was required.

The Property-Rights Argument and Expectations

Even if the defense does not win on property rights, deploying the argument can help with courts inclined to use *Katz* 's "reasonable expectations of privacy" test. This is yet another reason privacy policies and terms of service should be put in the record.

Courts almost never actually investigate both prongs of the reasonable expectation of privacy test. The first step in the test is whether a defendant manifested an actual expectation of privacy. That has fallen into disuse.[37] When they reach the second step — the question whether an expectation of privacy is objectively reasonable — the inquiry rarely goes beyond what the judges themselves think.

Research shows that the existence and language of privacy policies and terms of service statements suggest to laypeople that their information is protected. A 2014 survey, for example, found that 52 percent of people believe that when a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users.[38] This is not technically true (though it is also not quite as starkly false as many people claim).

The privacy policy is a signal that personal information is kept confidential, and with respect to government information demands, it largely does. Privacy policies create widespread expectations. Defense counsel can share privacy policies and research showing their influence on public perceptions to courts that are inclined to use "reasonable expectation of privacy" doctrine in Fourth Amendment cases.

In a way, Justice Kennedy suggested in *Carpenter* that "reasonable expectations" and the property-rights argument should be combined. "This case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy," he wrote.[39] It is certainly reasonable to expect that the terms of a contract will be fulfilled. Defense counsel should put that contract in the record.

Conclusion

The phrase "reasonable expectation of privacy" is so cemented into public consciousness that it is sometimes hard to remember that the language was engrafted onto the Fourth Amendment through a solo concurrence just 50 or so years ago. And that concurrence was not necessary to the outcome of the case.

There is a way of interpreting the Fourth Amendment that gets away from airy inquiries about what society deems "reasonable" and returns courts to examining what is real. In cases where the government has accessed data about a person that was subject to a privacy policy, that data was something of the defendant's. When it was seized and then searched, it affected a real legal interest of the defendant's. That interest was a property right in data about him or her, even though the data was held by a service provider. What makes that interest real is the privacy policy and terms of services statements that allocate property rights in the data to customers.

To make this argument, defense counsel should put privacy policies and terms of services statements in the record. That is the foundation for arguing that data about defendants is their property, even when it is held by service providers. It is the foundation for making a Fourth Amendment claim about that data.

Notes

1. 585 U.S. ___, 138 S. Ct. 2206 (2018).
2. *See Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473, 189 L.Ed.2d 430 (2014); *United States v. Jones*, 565 U.S. 400, 132 S. Ct. 945, 181 L.Ed.2d 911 (2012).
3. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
4. See Daniel T. Pesciotta, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 Case W. Res. L. Rev. 187, 189 (2012).
5. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 741, 99 S. Ct. 2577, 61 L.Ed.2d 220 (1979); *Illinois v. Caballes*, 543 U.S. 405 (2005).
6. 533 U.S. 27 (2001).
7. 565 U.S. 400, 405, 406, n.3, 132 S. Ct. 945, 181 L.Ed.2d 911 (2012).
8. *See Carpenter*, 138 S. Ct. 2206, 2221; *Riley*, 134 S. Ct. 2473, 2495.

9. This is the heart of Verizon's privacy policy, nested in language that caveats it appropriately. See https://www.verizon.com/about/privacy/full-privacy-policy. For illustration, this article uses the current Verizon policy throughout.

10. U.S. Const. amend. IV.

11. Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 709 (2010), *available at* https://digitalcommons.law.yale.edu/ylj/vol119/iss4/2.

12. *See, e.g.*, 18 U.S.C. § 2703.

13. 2 William Blackstone, Commentaries 2.

14. 458 U.S. 419, 435 (1982).

15. 444 U.S. 164, 176 (1979).

16. 533 U.S. 27 (2001).

17. *Id.* at 40.

18. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 553 (2005).

19. *See United States v. Seljan*, 547 F.3d 993, 1014-17 (9th Cir. 2008) (Kozinski, J., dissenting), *cert. denied*, 129 S. Ct. 1368 (2009) ("What makes papers special — and the reason why they are listed alongside houses, persons and effects — is the ideas they embody, ideas that can only be seized by reading the words on the page.").

20. 631 F.3d 266, 285-86 (6th Cir. 2010).

21. *Riley*, 134 S. Ct. 2473, 2485 ("[W]e ask instead whether application of the search incident to arrest doctrine to this particular category of effects [data on cellphones] would 'untether the rule from the justifications underlying the *Chimel* exception'"); *id.* at 2492 ("[A]pplying the *Gant* standard to cellphones would in effect give 'police officers unbridled discretion to rummage at will among a person's private effects.'").

22. *Carpenter*, 138 S. Ct. 2206, 2221.

23. *Carpenter*, 138 S. Ct. 2206, 2235 (Thomas, J., dissenting) (internal citation omitted).

24. *Carpenter*, 138 S. Ct. 2206, 2242 (Thomas, J., dissenting).

25. Oral Argument at 15:10, *Carpenter v. United States*, 138 S. Ct. 2206 (2018), https://www.oyez.org/cases/2017/16-402. ("I think I should caution the Court that — that relying too heavily on those contractual documents in either direction here would, to paraphrase the Court in *Smith*, threaten to make a crazy quilt of the Fourth Amendment because we may end up with a, you know, hinging constitutional protections on the happenstance of companies' policies.").

26 *See* David L. Callies & J. David Breemer, *The Right to Exclude Others from Private Property: A Fundamental Constitutional Right*, 3 Wash. U. J. L. & Pol'y 39 (2000).

27. https://www.verizon.com/about/privacy/full-privacy-policy (emphasis added).

28. *Carpenter*, 138 S. Ct. 2206, 2268 (Gorsuch, J., dissenting).

29. *See* Federal Trade Commission, "Privacy and Security Enforcement" webpage, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

30. *Los Angeles v. Patel*, 576 U.S. ___ (2015). The case dealt with these records to the extent they are the hoteliers' and not as records belonging to hotel guests. The former are entitled to a subpoena-like process. The latter, who are not represented in the process that would divest them of the control of records, are entitled to a warrant requirement.

31. *Carpenter*, 138 S. Ct. 2206, 2223 (Kennedy, J., dissenting), citing *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979).

32. *Carpenter*, 138 S. Ct. 2206, 2235 (Thomas, J., dissenting).

33. Oral Argument at 14:03, *Carpenter v. United States*, 138 S. Ct. 2206 (2018), https://www.oyez.org/cases/2017/16-402.

34. *Carpenter*, 138 S. Ct. 2206, 2247 (Alito, J., dissenting).

35. *Carpenter*, 138 S. Ct. 2206, 2247 (Alito, J., dissenting).

36. *Carpenter*, 138 S. Ct. 2206, 2268-69 (Gorsuch, J., dissenting).

37. *See* Orin Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).

38. Pew Research Center, *What Internet Users Know About Technology and the Web*, (Nov. 2014) at 7, https://www.pewresearch.org/wp-content/uploads/sites/9/2014/11/PI_Web-IQ_112514_PDF.pdf.

39. *Carpenter*, 138 S. Ct. 2206, 2235 (Kennedy, J., dissenting). ■

About the Author

Jim Harper is a Visiting Fellow at the American Enterprise Institute, where he focuses on privacy issues and select legal and constitutional issues. He filed amicus briefs in *Jones*, *Patel*, *Riley*, and *Carpenter*, as well as *Florida v. Jardines* and *United States v. Microsoft*.

Jim Harper
American Enterprise Institute
Washington, DC
202-862-5800
Email jim.harper@gmail.com
Website www.aei.org
Twitter @Jim_Harper

The Details Beyond Body-Worn Camera Footage

(Continued from page 30)

Security, Not Just Compliance at 5, https://axon.cdn.prismic.io/axon%2Fff836667-69a2-4169-ad2a-498d9a0f0577_security+white+paper.pdf (last visited May 15, 2019) ("Evidence.com is uniquely sensitive to the needs that surround the handling of evidence. For instance, automatic audit trails keep a complete and unalterable log of who has uploaded, accessed, edited, or shared each evidence file and when, in order to ensure that the proper chain of custody is maintained.").

16. Axon, *Viewing the evidence audit trail*, https://help.axon.com/hc/en-us/articles/221457487-Viewing-the-evidence-audit-trail (last visited May 15, 2019).

17. Axon, *supra* note 14, at 199-201.

18. Axon, *Axon View*, https://www.axon.com/products/view (last visited May 15, 2019).

19. Axon, *supra* note 14, at 229-232.

20. Axon, *supra* note 14.

21. Beryl Lipton, *Shifting from Tasers to AI, Axon Wants to Use Terabytes of Data to Automate Police Records and Redactions*, Muckrock, Feb. 12, 2019, https://www.muckrock.com/news/archives/2019/feb/12/algorithms-ai-task-force (last visited May 15, 2019).

22. Ian Wren & Scott Simon, *Body Camera Maker Weighs Adding Facial Recognition Technology*, NPR, May 12, 2018, 8:07 AM, https://www.npr.org/2018/05/12/610632088/what-artificial-intelligence-can-do-for-local-cops. ■

About the Author

Harlan Yu is the Executive Director of Upturn, a nonprofit research and advocacy organization. Upturn promotes equity and justice in the design, governance, and use of digital technology. Harlan holds a Ph.D. in computer science, and he is on NACDL's Fourth Amendment Center Advisory Board.

Harlan Yu
Upturn
Washington, DC
202-677-2359
Email harlan@upturn.org
Website www.upturn.org
Twitter @harlanyu