THE MANY REVOLUTIONS OF *CARPENTER*

PAUL OHM[1]

forthcoming 32 HARV. J.L. & TECH ___ (2019)

Carpenter v. United States, the 2018 Supreme Court opinion that requires the police to obtain a warrant to access an individual's historical whereabouts from the records of a cell phone provider, is the most important Fourth Amendment opinion in decades. Although many have acknowledged some of the ways the opinion has changed the doctrine of Constitutional privacy, the importance of Carpenter has not yet been fully appreciated. Carpenter works many revolutions in the law, not only through its holding and new rule, but in more fundamental respects. The opinion reinvents the reasonable expectation of privacy test as it applies to large databases of information about individuals. It turns the third-party doctrine inside out, requiring judges to scrutinize the products of purely private decisions. In dicta, it announces a new rule of technological equivalence, which might end up covering more police activity than the core rule. Finally, it embraces technological exceptionalism as a centerpiece for the interpretation of the Fourth Amendment, rejecting backwards-looking interdisciplinary methods such as legal history or surveys of popular attitudes. Considering all of these revolutions, Carpenter is the most important Fourth Amendment decision since Katz v. United States, a case it might end up rivaling in influence.

[1] Professor of Law and Associate Dean, Georgetown University Law Center. Thanks for excellent comments to the faculty of the University of Baltimore School of Law and the students of Fordham and the University of Texas. Special thanks to Lindsey Barrett, Alvaro Bedoya, Danielle Citron, Julie Cohen, Andrew Ferguson, Marty Lederman, and Laura Moy for comments. Thanks also to Mario Trujillo for research assistance.

INTRODUCTION

The Supreme Court's opinion in *Carpenter v. United States*[2] has been heralded by many as a milestone for the protection of privacy in an age of rapidly changing technology.[3] Despite this, scholars and

[2] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[3] Daniel Solove, Carpenter v. United States, *Cell Phone Location Records, and the Third Party Doctrine*, PRIVACY + SECURITY BLOG (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine/; Lior Strahilevitz, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision* – Carpenter v. United States, CONCURRING OPINIONS (June 22, 2018), https://concurringopinions.com/archives/2018/06/ten-thoughts-on-todays-blockbuster-fourth-amendment-decision-carpenter-v-united-states.html [hereinafter Strahilevitz, *Ten Thoughts*]; Orin Kerr, *First Thoughts on Carpenter v.*

commentators have failed to appreciate many of the important aspects of this landmark opinion. *Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of Constitutional privacy in this country for a generation or more.

The most obvious revolution is the case's basic holding—for the first time, the Court has held that the police must secure a warrant to require a business to divulge information about its customers compiled for the business's purposes, reinventing the reasonable expectation of privacy test and significantly narrowing what is known as the third-party doctrine.[4] Information about the location of cell phone customers held by cell phone providers is now protected by the Fourth Amendment, at least when the police seek seven days or more of such information.[5] This cell-site location information (CSLI) has become a key source of evidence for the investigation of crimes, so this holding will revolutionize the way the police build their cases, requiring a warrant where none has been required before.[6]

Building outward, the reasoning of the majority opinion, written by Chief Justice Roberts and commanding five votes, revolutionizes the law of police access to many other types of information, in addition to CSLI.[7] Databases that can be used, directly or indirectly, to ascertain the precise location of individuals over time are likely now covered by the Fourth Amendment. The police will probably need a warrant to obtain location information collected by mobile apps, fitness trackers, connected cars, and many so-called "quantified self" technologies.[8]

The reasoning extends beyond location information, although predicting the scope and shape of this revolutionary step requires a bit more speculation. The majority opinion promulgates a new, multi-factor test that will likely cover other commercially significant data that the police has begun to access in its investigations.[9] Massive databases of web browsing habits stored by internet service providers (ISPs) will probably now require a warrant to access.[10] Perhaps most

---

United States, THE VOLOKH CONSPIRACY (June 22, 2018), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta.

[4] Carpenter, 138 S. Ct. at 2206.

[5] *Id.* at 2217 & n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

[6] *Id.* at 2233 (Kennedy, J., dissenting) ("[T]he Court's holding . . . limits the effectiveness of an important investigative tool for solving serious crimes.")

[7] *Infra* Part I.C.

[8] Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 591-95 (2017), http://scholarship.law.cornell.edu/clr/vol102/iss3/1 (Discussing Fourth Amendment implications of GPS monitors attached to the body). For discussion of these technologies, *see infra* note 59.

[9] *Infra* Part I.C.

[10] *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1438–40 (2009), https://illinoislawreview.org/wp-content/ilr-

surprisingly, the majority's reasoning will apply even to massive databases of telephone dialing and banking records, cutting back on the holdings of two cases, *Smith v. Maryland*[11] and *Miller v. United States*,[12] that the *Carpenter* Court expressly declined to overrule.[13] Those two cases are in a much more precarious state than other commenters have recognized.[14]

Looking beyond the central holding and reasoning, to dicta from the majority and dissenting opinions, another class of revolutions comes into view. The Court has breathed new life into *Kyllo v. United States*, the 2001 case that required the police to obtain a warrant to aim a thermal imaging device at a private home.[15] At least seven justices of the *Carpenter* Court suggest a heretofore unrecognized rule building on *Kyllo*: the *rule of technological equivalence*. If a technology, or a near-future improvement, gives the police a power to gather information that is the "modern-day equivalent" of activity that has been held to be a Fourth Amendment search, the use of that technology is also a search.[16] This is a far simpler and more straightforward test to apply than the multi-factor core test of *Carpenter*, and for that reason, could end up becoming the *Carpenter* rule cited most often as the basis for requiring the police to get a warrant.

The rule of technological equivalence, although dicta, finds expression in at least three forms in these opinions. The first is the *rule of equivalence to the home*. *Kyllo* remains the best example, building on Justice Scalia's conclusion that, "in the home, our cases show, *all* details are intimate details . . . ."[17] After *Carpenter*, this rule will likely cover many consumer products sold under the banner of the Internet of Things.[18] It will also likely cover the information gathered

---

content/articles/2009/5/Ohm.pdf, [hereinafter Ohm, *Invasive ISP Surveillance*] (describing the power of ISPs to scrutinize the private browsing habits of customers).

[11] 442 U.S. 735 (1979).

[12] 425 U.S. 435 (1976).

[13] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not disturb the application of *Smith* and *Miller* . . . .").

[14] Daniel Solove, Carpenter v. United States*, Cell Phone Location Records, and the Third Party Doctrine*, PRIVACY + SECURITY BLOG (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine/ ("The Supreme Court should have overruled the Third Party Doctrine or at least carved out a greater chunk of it.").

[15] 533 U.S. 27 (2001).

[16] *Id.* at 2222 (calling Justice Kennedy's "modern-day equivalent" discussion a "sensible exception"); *Id.* at 2230 (Kennedy, J., dissenting).

[17] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[18] *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 835–853 (2016) (discussing the Fourth Amendment implications of Internet of Things devices located within the home pre-*Carpenter*).

by so-called "smart home" devices such as smart thermostats, doorbells, security systems, light bulbs, speakers (like Amazon's Echo), refrigerators, and televisions.[19] Many "connected city" technologies, such as smart grid devices similarly gather information about the interior of homes and would be covered as well.[20]

The second rule of technological equivalence is the *rule of equivalence to bailment*. Both Justices Kennedy and Gorsuch suggest that any information stored with a 21st century digital bailor—such as a cloud storage provider like Dropbox—is protected by a reasonable expectation of privacy.[21]

The third rule is the *rule of communications equivalence*. Any communications technology equivalent to postal mail or the telephone is covered by the Fourth Amendment.[22] Most importantly, all nine justices sign on to opinions in *Carpenter* that suggest that the police are not allowed to access the content of email messages without a warrant, something the Court has never before held.[23] It is likely that this reasoning will cover other communications technologies in addition to email, such as instant messaging, text messaging, and person-to-person communications features of social networking services.[24]

The last revolution is a revolution of legal reasoning. In his opinion, the Chief Justice evinces, as he did in the majority opinion in *Riley v. California*,[25] a profound *technology exceptionalism*.[26] Recent advances in information technology are different in kind not merely in degree from what has come before. This idea finds substantial support in two decades of legal scholarship about threats from technology to information privacy, work that has never before received such a profound endorsement from the Supreme Court.

---

[19] *See infra* note 209–212

[20] Naperville Smart Meter Awareness v. Naperville, No. 16-3766 (7th Cir. Aug. 16, 2018), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2018/D08-16/C:16-3766:J:Kanne:aut:T:fnOp:N:2203659:S:0; Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 5 (Ctr. for Energy and Envtl. Sec., Working Paper No. 09-001, 2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731.

[21] *Id.* at 2228 (Kennedy, J., dissenting); *Id.* at 2268–69 (Gorsuch, J., dissenting).

[22] *Id.*

[23] *Id.* at 2222 (majority opinion) (favorably discussing Kennedy's citation of *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)); *Id.* at 2230 (Kennedy, J., dissenting with Justices Alito and Thomas) (favorably citing *Warshak* 631 F.3d at 266*)*; *Id.* at 2269 (Gorsuch, J., dissenting) (. . . "few doubt that e-mail should be treated much like the traditional mail it has largely supplanted . . . .").

[24] *See infra* note 231.

[25] Riley v. California, 134 S. Ct. 2473 (2014).

[26] *Infra* Part II.C.

In embracing tech exceptionalism, the Court expressly declined invitations from scholars and amici to base its Fourth Amendment reasoning in traditional disciplines such as history or economics.[27] Scholars coming from those interdisciplinary traditions have expressed disappointment about this choice, which is an understandable reaction to having been heard and rejected.[28]

Carpenter is an inflection point in the history of the Fourth Amendment. From now on, we'll be talking about what the Fourth Amendment means in pre-*Carpenter* and post-*Carpenter* terms. It will be seen as being as important as *Olmstead*[29] and *Katz*[30] in the overall arc of technological privacy.

This article proceeds in four parts. Part I lays out the basic rule of *Carpenter*, which protects large databases full of information from unreasonable police access according to a new, multi-factor test, and applies the test to other private databases of information. Part II explains how *Carpenter* has turned the government action rule of the Fourth Amendment on its head and created three new rules of technological equivalence. Part III discusses the technology exceptionalism at the heart of *Carpenter* and how it changes Fourth Amendment reasoning. Finally, Part IV argues that *Carpenter* might replace rather than merely apply *Katz* and the reasonable expectation of privacy test, at least for cases involving complex modern technology.

I. THE BASIC RULE OF *CARPENTER*

Carpenter holds that the government collection of cell-site location information (CSLI) is a search by introducing a new, multi-factor test.[31] This test serves the dual purpose of deciding whether access to large databases full of personal information about individuals constitutes a search under the Fourth Amendment and whether the third-party doctrine should extend to such access.[32]

The Court does not exhaustively specify or defend the new test, although a close reading of the opinion reveals the critical factors and why they matter. The importance of these factors finds great support in recent legal scholarship. When lower courts apply these factors, they

---

[27] *Infra* Part III.F.

[28] *Id.*

[29] Olmstead v. United States, 277 U.S. 438 (1928) (holding that a wiretap is not a search, embracing the trespass theory of the Fourth Amendment).

[30] Katz v. United States, 389 U.S. 347, 351 (1967) (holding that placing a recording device on the exterior of a telephone booth is a search).

[31] Carpenter v. United States, 138 S. Ct. 2206, 2223 ("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.").

[32] *Id.*

are likely to extend the Fourth Amendment to cover many important commercial databases that have never before required a warrant for the police to access.

A. *Carpenter's* Broad New Rule[33]

Carpenter holds that the police may not collect historical CSLI from a cellphone provider without a warrant.[34] Footnote three restricts the holding, for now, to seven days of collection.[35]

This is the opinion most privacy law scholars and privacy advocates have been awaiting for decades.[36] Oceans of ink have been spilled by those worried about how the dramatic expansion of technologically fueled corporate surveillance of our private lives automatically expands police surveillance, too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine.[37] The Fourth Amendment protects only that which is protected by a "reasonable expectation of privacy" (REP).[38] This requires a two-pronged analysis, "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[39] The third-party doctrine says that information a person voluntarily discloses to a third party is not protected by a reasonable expectation of privacy.[40]

With *Carpenter*, the Supreme Court reinvents the REP test. Until now, the Supreme Court has always paid more attention to the nature of the police intrusion required to obtain information than to the nature of the information obtained. Information has been deemed

---

[33] This subpart is adapted from a blog post I authored shortly after the *Carpenter* decision was handed down. Paul Ohm, *The Broad Reach of* Carpenter v. United States, JUST SECURITY (June 27, 2018), https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states/.

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

[35] *Id.* at 2217 n.3.

[36] DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017); DANIEL J. SOLOVE, NOTHING TO HIDE (2011); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 746 (2011) [hereinafter Freiwald, *Cell Phone Location Data*].

[37] Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U.L. REV. 1441 (2017); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007) [hereinafter Freiwald, *First Principles*].

[38] Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring) (articulating the reasonable expectation of privacy test).

[39] *Id.*

[40] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 566–570 (2009), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1348&context=mlr.

protected by REP because the police obtained it using advanced thermal imaging tools,[41] or a wireless beeper located inside a house.[42] Information has fallen outside an REP when obtained from trash left on the curb,[43] low-flying aircraft,[44] or a wireless beeper traveling on public roads.[45] The analysis has always turned primarily on the invasion and only secondarily on the information.

Carpenter heralds a new mode of Constitutional analysis, because the Court finds an REP based largely on an analysis of the information divorced from the actions of the police, database owner, or surveillance target. The most important holding—which commanded the votes of five justices—"is that "individuals have a reasonable expectation of privacy in the whole of their physical movements."[46] The Court explains that a database full of CSLI meets this standard using an analysis focused exclusively on the nature of the data in the database and the target's role in the initial collection of it.

Next, with *Carpenter*, the Supreme Court has declared the third-party doctrine to be almost dead. The majority opinion decline[d] to extend" the third-party doctrine to the collection by the FBI from cellphone providers of seven-days of CSLI.[47] "Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection."[48]

Even on their own terms, these two holdings have sweeping consequences for privacy and law enforcement. But it's the way Chief Justice Roberts reasoned his way to them that assures that this opinion will be applied far beyond the facts of this case.

First, as described in the majority and dissenting opinions, the CSLI that has just been protected isn't terribly precise.[49] If the majority had placed an exaggerated gloss on the precision of CSLI at issue in this case, it would have given the government a way in future cases to distinguish other types of location information: "the data at issue in this case is not controlled by Carpenter," the government could have argued, "because it is far less precise than CSLI."

It will be difficult to make this argument because the majority opinion informs us that the CSLI records in this case "placed

---

[41] Kyllo v. United States, 533 U.S. 27, 36 (2001).
[42] United States v. Karo, 468 U.S. 705, 717 (1984)
[43] California v. Greenwood, 486 U.S. 35, 40 (1988).
[44] Florida v. Riley, 488 U.S. 445 (1989).
[45] United States v. Knotts, 460 U.S. 276 (1983).
[46] Carpenter, 138 S. Ct. at 2217 *quoting* United States v. Jones, 565 U.S. 400, 430, 415 (concurring opinions of Justices Alito and Sotomayor).
[47] Carpenter, 138 S. Ct. at 2220.
[48] *Id.* at 2217.
[49] *Id.* at 2218.

[Carpenter] within a wedge-shaped sector ranging from one-eighth to four square miles."[50] In his dissent, Justice Kennedy characterizes these dimensions as "covering between a dozen and several hundred city blocks" in cities and "up to 40 times more imprecise" in rural areas.[51] GPS this certainly is not. The Chief Justice waves this away, in part, because "the rule this Court adopts 'must take account of more sophisticated systems that are already in use or in development'".[52]

Second, the majority opinion is not restricted to CSLI, even on its own terms. Instead, this is an opinion about information the police can use to locate people generally, not CSLI specifically.[53] Part III of the opinion is all about the privacy interests individuals have in "the whole of their physical movements."[54] This is a meditation on the nature of location information, whatever form it takes. Geolocation information, when there is enough of it, "provides an intimate window into a person's life", quoting Justice Sotomayor's celebrated opinion from *Jones*, revealing "familial, political, professional, religious, and sexual associations."[55] This case is "not about 'using a phone' . . . [i]t is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[56] It is about "a trail of location data."[57]

By focusing on the nature of the information rather than on the telecommunications nitty-gritty used to gather the information or the structure of the database in which the information was held, this opinion clearly signals that its holding will apply to other massive collections of historical geolocation information, of which there are many. Many smartphone apps collect precise GPS information, including apps that have no need for this kind of information except to sell to advertisers.[58] It's not just your smartphone, as GPS information

---

[50] *Id.* at 2218.
[51] *Id.* at 2225 (Kennedy, J., dissenting).
[52] *Id.* at 2210 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).
[53] *Id.* at 2217–18.
[54] *Id.* at 2217.
[55] *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
[56] *Id.* at 2220.
[57] *Id.*
[58] KENNETH OLMSTEAD & MICHELLE ATKINSON, PEW RESEARCH CENTER, APP PERMISSIONS IN THE GOOGLE PLAY STORE 22 (2015) http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/11/PI_2015-11-10_apps-permissions_FINAL.pdf (finding that in 2014, 24 percent of apps in the Google Play store requested access to precise GPS location information, while 21 percent asked for approximate location information). *See e.g.*, Press Release, Federal Trade Commission, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

is gathered by the companies that provide fitness trackers, connected cars, and smart watches. Internet of Things gizmos place location trackers in our clothes, bags, and even our bodies.[59] It might not be that every database of location information generated by every technology listed above will fall within the *Carpenter* reasoning, but the police should think twice before trying to collect any of it without a warrant.

Third, the majority opinion will probably even apply to information that does not expressly reveal location but from which location may be inferred. "[T]he Court has already rejected the proposition that 'inference insulates a search'",[60] quoting *Kyllo* once again. The opinion highlights how the government could use CSLI "in combination with other information, [to] deduce a detailed log of Carpenter's movements."[61] Many databases that do not store location information directly can be used to infer location information. Credit card records, automatic toll transponder records, automated license-plate records, etc., can all generate inferences about a person's location that are far more precise than CSLI.[62] Any time the government

---

[59] *See e.g.*, Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217, 221 (2012) (describing GPS monitoring in at least one wristband sensor); Lisa Eadicicco, *A New Wave Of Gadgets Can Collect Your Personal Information Like Never Before*, BUSINESS INSIDER (Oct. 9, 2014), https://www.businessinsider.com/privacy-fitness-trackers-smartwatches-2014-10 (describing location tracking in smartwatches and fitness trackers); OFFICE OF SEN. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 8–12 (2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (describing private GPS tracking of connected cars); Damon Beres, *These High-Tech Shirts And Pants Can Help Protect Kids With Autism*, THE HUFFINGTON POST (Feb. 18, 2015), https://www.huffingtonpost.com/2015/02/18/autism-gps-device_n_6705368.html (describing location tracking in clothing for autistic children); Carey Dunne, *Forget Fitbits: This T-Shirt Embeds Fitness Sensors Into Its Fabric*, FAST COMPANY (March 6, 2014), https://www.fastcompany.com/3027278/forget-fitbits-this-t-shirt-embeds-fitness-sensors-into-its-fabric (describing location tracking in exercise clothing); Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 591-95 (2017), http://scholarship.law.cornell.edu/clr/vol102/iss3/1 (Discussing Fourth Amendment implications of GPS monitors attached to the body); Yael Grauer, *A practical guide to microchip implants*, ARS TECHNICA (Jan. 3, 2018) (describing transponder implants in humans but not referring to GPS).

[60] *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

[61] *Id.*

[62] *See e.g.*, United States v. Kragness, 830 F.2d 842, 865 (8th Cir. 1987) (describing government's use of credit-card records to prove defendant's travel history); In re U.S. for Historical Cell Site Data, 724 F.3d 600, 614 n.13 (5th Cir. 2013) (". . . [W]hen a customer makes a credit card purchase at a store or restaurant, he does not directly convey the location of the transaction to his credit card company. Nevertheless, law enforcement officers can obtain his credit card records from the company with a

accesses a privately assembled database in order to track location without a warrant, it risks suppression under *Carpenter*.

This gives the lie to something the majority said that has puzzled commenters: "We do not . . . call into question conventional surveillance techniques and tools, such as security cameras."[63] What the Chief Justice misses in this simple statement is how facial recognition technology has advanced to the point that a huge archive of security camera footage can easily be transformed into a huge database tracking the location of identified individuals.[64] It might be that CSLI records track location far more comprehensively than security camera footage connected to facial recognition software—we will examine the role of the comprehensiveness below[65]—but the majority cannot literally mean that security camera footage is categorically not a search given the reasoning of the opinion.

In sum, criminal defendants will test the outer boundaries of *Carpenter's* reasoning whenever the police use massive databases assembled by private parties that reveal location information, directly or by inference. Other defendants will challenge the collection of data unrelated to location. The broad reasoning of the majority's opinion will give all of them plenty to work with. Anticipating this, risk-averse police departments will err on the side of caution, getting a warrant for data whenever they can, and turning promising leads into dead ends whenever they can't. It's a powerful reminder of the ability the Supreme Court has to protect civil liberties and reshape the contours of our relationship with the state. This opinion does no less, finally, at long last, giving us a tool to disrupt—at least for a moment—the steady march to a surveillance state.

---

subpoena. . . and use them to track his location.") Mariko Hirose, *Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York*, ACLU (April 24, 2015), https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass (describing location tracking through toll transponders); Reepal S. Dalal, Note, *Chipping away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights*, 86 B.U. L. REV. 485, 494-495 (2006) (discussing the Fourth Amendment implications of toll collection data); AMERICAN CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 7 (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf (describing location tracking through license-plate records); *infra* note 191 (discussing Fourth Amendment implications of license plate readers).

[63] *Carpenter*, 138 S. Ct. at 2220.

[64] CLARE GARVIE ET AL., GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY, THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 22 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[65] *Infra* Part I.B

B. What is the *Carpenter* Test?

The test that emerges from the majority opinion will also be applied to collections of information maintained by third parties that do not track location, not even by inference, but are of interest to law enforcement. Going forward, whenever the government obtains a copy of a massive database of information containing non-public information about individuals, judges will conduct a qualitative and quantitative assessment of the information, using a new, multi-factor test. This assessment will answer two questions: first, does the individual whose information has been obtained have a reasonable expectation of privacy in the database? Second, even if that information has been collected and is being maintained by a private third party, does the third-party doctrine apply?

There is likely to be disagreement about the precise list of *Carpenter* factors, given the wide ranging nature of the opinion. Different characteristics of CSLI data and smartphone use are emphasized throughout the Chief Justice's opinion.[66] Still, in concluding the opinion, he helpfully isolates three factors: (1) "the deeply revealing nature" of the information; (2) "its depth, breadth, and comprehensive reach"; (3) "and the inescapable and automatic nature of its collection."[67] To this list, I would add a fourth factor, how much does access to this data give the police a gain in efficiency as compared to historical surveillance practice?[68] In weighing each of these, the Chief Justice keeps in view two overarching purposes for the Fourth Amendment: "to secure 'the privacies of life' against 'arbitrary power'" and "'to place obstacles in the way of a too permeating police surveillance.'"[69]

Later, we will probe the theoretical foundations and normative desirability of this test,[70] but for now, let us note the similarity of the test to the work of Susan Freiwald.[71] Freiwald has long advocated that the Court embrace her own four factor test for deciding whether there is an invasion of REP in electronic surveillance.[72] She argues that courts should inquire whether the police are using a "hidden, intrusive,

---

[66] *Id.* at 2216–20.
[67] *Id.* at 2223 (emphasis added).
[68] *Infra* Part I.B.4
[69] *Carpenter*, 138 S. Ct. at 2214.
[70] *Infra* Parts III & IV.
[71] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 746 (2011) [hereinafter Freiwald, *Cell Phone Location Data*]; Patricia L. Bellia, Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121 (2008); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007) [hereinafter Freiwald, *First Principles*].
[72] Freiwald, *First Principles*, *supra* note 71, at *50.

indiscriminate, and continuous method of surveillance."[73] Using this test, she bested the Supreme Court by seven years, arguing in 2011 that the police should be required to obtain a warrant to access CSLI.[74] I will highlight in the discussion below how the Freiwald factors correspond to the *Carpenter* factors.

Let us consider each of the *Carpenter* factors in turn. The sections that follow will highlight the key language from the majority opinion about each factor, as well as focus on language from the various dissents that sharpen the meaning or import of each factor. These sections will also connect most of the factors to the broader world of privacy law and scholarship beyond this case. This is meant to address a criticism that has been directed at the majority's opinion: its failure to cite any legal scholarship.[75] The Court could have supported each of its points with scholarly citation. This opinion resonates with two decades of writing about the Fourth Amendment in an age of rapidly changing technology, regardless of whether the Chief Justice was aware of any of this work. Consider this the majority's missing cite check, demonstrating the rigor and theoretical underpinnings of this approach.

1. First Factor: Deeply Revealing Nature

The *Carpenter* test protects information only if it is "deeply revealing" of some private quality of the person under surveillance.[76] "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."[77] These location records "hold for many Americans the 'privacies of life.'"[78]

This factor is perhaps the most important. Information stored by a private third party must in some way be deemed sensitive or intimate to fall within the reasonable expectation of privacy test. These two words, although similar to one another, have different meanings. Sensitive information is information that can be used to cause an individual or group harm.[79] In contrast, intimate information reveals something important and not widely known about a relationship between individuals.[80]

---

[73] *Id.*
[74] Freiwald, *Cell Phone Location Data*, *supra* note 71, at 746-48.
[75] Strahilevitz, *Ten Thoughts*, *supra* note 3.
[76] *Carpenter*, 138 S. Ct. at 2223.
[77] *Id.* at 2217 (citation omitted).
[78] *Id.* at 2217 (citation omitted).
[79] Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133–34 (2015) [hereinafter Ohm, *Sensitive Information*].
[80] JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992).

The connection between sensitive and intimate information and the REP test has a long doctrinal lineage. Professor Orin Kerr argues that the Supreme Court has adopted four different models for assessing whether police practice implicates a reasonable expectation of privacy, one of which is a "private facts" model, which measures the sensitivity and intimacy of the information obtained.[81] This factor mirrors Freiwald's "intrusiveness" factor, which considers what a surveillance technique reveals.[82]

The road to the Court's recognition of this factor was paved by the two blockbuster opinions from recent years about technology and the Fourth Amendment, *United States v. Jones* and *Riley v. California.*[83] The notion that detailed location information can reveal the "familial, political, professional, religious, and sexual associations" comes from Justice Sotomayor's concurrence in *Jones*, perhaps the single most important quote ever uttered in a Supreme Court opinion about the sensitivity of information.[84] The idea that a smart phone can "hold for many Americans, the 'privacies of life'" comes from the Chief Justice's opinion in *Riley*.[85]

As discussed earlier, this factor focuses exclusively on an analysis of the intrinsic nature of the information itself, divorced from any consideration of what the police had to do to obtain it, the company's incentives for gathering it, or the individual could have done to prevent it. This is a fundamental break from Fourth Amendment analyses of the past, which always placed police action and individual counter-action at the center, and information on the periphery.

2. Second Factor: Depth, Breadth, and Comprehensive Reach

The *Carpenter* test protects information that possesses "depth, breadth, and comprehensive reach".[86] Like the first factor, this focuses on the intrinsic nature of the information.

Justice Kennedy, in dissent, provides his own list of the factors he sees in the majority's opinion, to criticize the majority's "unstable foundation".[87] His list boils down this factor into a single one, "comprehensiveness,"[88] but it is better to treat this as three distinct

---

[81] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 512-16 (2007) [hereinafter Kerr, *Four Models*]. The other three models are "probabilistic", "positive law", and "policy". *Id.* at 506. We will return to this later.

[82] Freiwald, *First Principles*, *supra* note 71, at *66.

[83] United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 134 S. Ct. 2473 (2014).

[84] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

[85] *Riley*, 134 S. Ct. at 2494–95 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

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

[87] *Id.* at 2234 (Kennedy, J., dissenting).

[88] *Id.*

requirements (meaning our three factors might instead be treated as five). All three speak to the quantity, primarily, of information stored. But they measure a database along three distinct dimensions.

Depth refers to the detail and precision of the information stored.[89] This is closely related to the deeply revealing nature factor, as it is the precision of location information that triggers Justice Sotomayor's litany of private inferences—location information betrays a person's political, sexual, religious associations only if is sufficiently precise to imply visits to particular storefronts, homes, or other individual locations.[90] The *Carpenter* majority emphasizes that CSLI stores "the whole of [a person's] physical movements"[91] as well as "a detailed chronicle of a person's physical presence."[92]

In contrast, *breadth* refers to time in two ways: how frequently is the data collected, and for how long has the data been recorded?[93] CSLI qualifies as broad in both senses, because the database at issue in *Carpenter* stored "an average of 101 data points every day" of the defendant's location,[94] and because cell phone providers tend to store data for five years.[95] Every one of us "has effectively been tailed every moment of every day for five years."[96] It is information "compiled every day, every moment, over several years."[97]

Finally, *comprehensive reach* refers to the number of people tracked in the database.[98] This recognizes that "there, but by the grace of the police, go I." "Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation— this newfound tracking capacity runs against everyone."[99] This is critical because, "[u]nlike with the GPS device in

---

[89] *Id.* at 2218 ("From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial.").

[90] *Id.* at 2217.

[91] *Id.* at 2219.

[92] *Id.* at 2200.

[93] *Id.* at 2212 ("Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.").

[94] *Id.*

[95] *Id.* at 2218.

[96] *Id.*

[97] *Id.* at 2200.

[98] *Id.* at 2218 ("Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.").

[99] *Id.* at 2218.

Jones, police need not even know in advance whether they want to follow a particular individual, or when."[100]

Two of Freiwald's four factors anticipated these *Carpenter* factors, the "continuous" and "indiscriminate" nature of surveillance.[101] She considers these factors important because they increase the odds that the government will conduct surveillance "without sufficient justification" and which reveals "activities that are entirely unrelated to criminal actions."[102]

By identifying these factors, the Court embraces the mosaic theory of privacy.[103] The mosaic theory is animated by an idea that finds support both in folk wisdom and modern machine learning: the whole is greater than the sum of the parts.[104] It first found expression in Fourth Amendment jurisprudence in *United States v. Maynard*, the D.C. Circuit opinion that was renamed *United States v. Jones* on its way to the Supreme Court.[105] In the majority opinion in *Maynard*, Judge Ginsburg concluded that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."[106] Although the *Jones* majority chose not to embrace the mosaic theory, focusing instead on the physical trespass that occurred during the installation of the GPS tracking device, *Carpenter* seems to revive the idea.

The mosaic theory bring us to footnote three of *Carpenter*:

> The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Contrary to Justice KENNEDY's assertion, we need not decide whether there is a limited period for which the Government may obtain an individual's historical

---

[100] *Id.* at 2218.
[101] Freiwald, *Cell Phone Location Data*, *supra* note 71, at 747-48.
[102] *Id.* at 747. These three subfactors echo a proposal offered by Luke Milligan. Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1333 (2011). Milligan proposes new technologies should be given "fresh analysis" when they alter the "amount of data available" or the "government's ability to aggregate information over time and across the population." *Id.*
[103] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) [hereinafter Kerr, *Mosaic Theory*].
[104] *Id.* at 326.
[105] 615 F.3d 544 (D.C. Cir. 2012), *aff'd sub nom.* United States v. Jones, 565 U.S. 400 (2012).
[106] *Id.* at 562.

> CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.[107]

Several dissents criticized the seeming arbitrariness of this seven-day rule.[108] Footnote three is likely to spark scholarly criticism and commentary.[109] Any opinion that tries to give force to the mosaic theory has to draw a line.[110] Given the role that the quantity factors play in the majority's reasoning, it seems likely that a database containing a single datum that revealed a single registration between a cell phone and cell site would not trigger nearly the same privacy concerns. A single data point would be neither as deep, broad, nor comprehensive, as seven days (much less five years) of CSLI. For that reason, it would not be nearly as "deeply revealing". A future court asked to rule on the warrantless access of a single datum of location information might well distinguish it from the facts and reasoning of *Carpenter*.

While one point of information might not suffice, one should not read too much into the seven day figure. For one thing, this is the figure that the facts presented: the government sought seven days of CSLI.[111] In fact, the order seeking seven days of information elicited only two days of CSLI.[112] The Court gave no principled reason for selecting seven days as the cut-off, so we ought not consider it the precise dividing line. Future opinions will need to analyze the relationship between the temporal breadth of data and the impact on privacy interests.

These quantitative facts are sure to be the source of confusion in the lower courts—and inside police stations—and the target of criticism from other scholars. What if a database has only two forms of quantitative comprehensiveness—say depth and breadth—but about only one person rather than with comprehensive reach? What if a database reveals deep information about many people, but recorded at a single moment in time?

One potential complicating scenario was expressly referenced in the majority opinion: does a real-time, future-looking, prospective

---

[107] Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018) (citations omitted).
[108] *Id.* at 2234 (Kennedy, J., dissenting); *Id.* at 2266–67 (Gorsuch, J., dissenting).
[109] Ohm, *supra* note 33 ("[G]et used to a lot of scholarly commentary about Carpenter, footnote three!").
[110] Kerr, *Mosaic Theory*, *supra* note 103, at 333–34 (discussing the need to draw lines based on time for a mosaic theory approach to the Fourth Amendment).
[111] *Carpenter*, 138 S. Ct. at 2212. *See id.* at 2217 n.3 (citing the government's suggest of a seven-day cutoff).
[112] *Id.* at 2212.

collection of data trigger this factor and thus the *Carpenter* rule?[113] The majority opinion expressly declined to say.[114] At the same time, it emphasizes repeatedly the retrospective nature of CSLI information, and indeed, Justice Kennedy includes "retrospectivity" in his summary of the factors, although the majority opinion does not.[115] What will lower courts say about real-time CSLI collection?

On the one hand, it is clear that the majority opinion is quite worried about the time travel nature of the CSLI database, which isn't implicated in the same way by real-time data gathering.[116] Real-time CSLI gathering can be "switched on" for a specific target, allowing it to be pinpointed rather than amassed indiscriminately.

But on the other hand, retrospectivity is just one version of problematic "breadth", and should be seen as such, rather than treating retrospectivity as a necessary requirement. There might be databases that collect a broad swath of data across time without being retrospective in the same way as the CSLI database. A police order commanding a phone company to collect CSLI in real-time about one individual for seven days, would be an example.[117] Or consider a database that stores retrospective information only about some people

---

[113] *Id.* at 2220 (declining to express an opinion about "real-time CSLI").

[114] *Id.*

[115] *Id.* at 2218 ("With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts . . . ."); *id.* at 2234 (Kennedy, J., dissenting) (listing factors, in dissent by Justice Kennedy, including retrospectivity); *id.* at 2223 (listing factors, in majority opinion, not including retrospectivity).

[116] *Id.* at 2218. The metaphor of treating police access to historical data as travel in a time machine was first proposed by legal scholar Steven Henderson. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PENN. J. CON. L. 933 (2016).

[117] *Compare* Jones v. United States, 168 A.3d 703, 713 (D.C. 2017) (holding that the use of a cell-site simulator to locate a suspect's phone in real time "invaded a reasonable expectation of privacy and was thus a search."), *with* United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017), cert. denied, 138 S. Ct. 2705 (2018) (holding that "government did not conduct a search under the Fourth Amendment when it tracked the real-time GPS coordinates of" suspect's phone outside the home for seven hours). *See also* United States v. Wallace, 866 F.3d 605, 609 (5th Cir. 2017), opinion withdrawn and superseded, 885 F.3d 806 (5th Cir. 2018) (noting that it is an open question whether it is a search to obtain real-time E911 data but holding that police are covered by good-faith exception to exclusionary rule nonetheless); United States v. Banks, 884 F.3d 998, 1013 (10th Cir. 2018) (declining to decide whether "tracking a cell-phone's real-time location is a search" because parties did not thoroughly brief the issue; however, assuming a search and finding exigent circumstances exception applied). *See generally* Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (Originally published in 2015).

but not everybody in the database.[118] So long as the information is deep, broad, and of comprehensive reach, it should trigger this factor, whether or not it is retrospective in the same way.

3. Factor Three: Inescapable and Automatic Nature of the Collection

The first two factors focus on the intrinsic nature of the information. They analyze information as a database designer would, interrogating the qualitative and quantitative information content of the data, and the inferences that can be drawn from them. The other two factors operate in a much more traditional mode, focusing in factor three on what the database owner and data subject have done (or could have done) and in factor four on how the information empowers the police.

The third factor, the final factor the majority cites, is the "inescapable and automatic nature" of how the information is collected.[119] This factor speaks to whether the targets of the surveillance could be said to have assumed the risk of the data collection or knowingly exposed information to the private party.[120] This factor (really two separate factors) brings into the analysis the idea that individuals might sometimes relinquish their Fourth Amendment rights when they assume the risk of surveillance, for example by publishing information to the general public.

This connects to Freiwald's factor of "hidden" surveillance. She argues that surveillance conducted without the awareness of the person being observed introduces a risk "that agents will exceed the scope of a proper investigation with impunity."[121]

Some data collections are *inescapable* because they relate to a service one needs to use to be a functioning member of modern society. In the case of CSLI, cell phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in

---

[118] For example, under the USA FREEDOM Act, the NSA can request telephony metadata records relating to a suspect and everyone within "two hops" of contact with of the suspect. 18 U.S.C. § 1861(c)(2)(F)(iii)-(iv) (permitting two hops of production of call detail records). Researchers estimate that this can net the records of approximately 25,000 subscribers with a single search. Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROC. NAT'L ACAD. SCI. 5536, http://www.pnas.org/content/113/20/5536.

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

[120] *Id.* at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements." *quoting Smith,* 442 U.S., at 745).

[121] Freiwald, *Cell Phone Location Data*, *supra* note 71, at 747.

modern society."[122] The opinion makes this point in dramatic fashion, borrowing from the Chief Justice's opinion in *Riley*:

> Unlike the bugged container in Knotts or the car in Jones, a cell phone—almost a "feature of human anatomy," Riley, 573 U. S., at ___ (slip op., at 9)—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. See id., at ___ (slip op., at 19) (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admit- ting that they even use their phones in the shower"); contrast Cardwell v. Lewis, 417 U. S. 583, 590 (1974) (plurality opinion) ("A car has little capacity for escaping public scrutiny.").[123]

Perhaps reflecting how some members of modern society feel shackled to these devices, the Chief Justice deploys an especially evocative simile: "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[124]

Inescapability is not the same as the *automatic* nature of the information collected. CSLI is automatically part of cell service because the records are generated whenever the service is used, and there is no opportunity to opt out.[125]

> [A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[] the risk" of turning over a comprehensive dossier of his physical movements.[126]

---

[122] *Carpenter*, 138 S. Ct. at 2220.
[123] *Id.* at 2218.
[124] *Id.* at 2218.
[125] *Id.* at 2220.
[126] *Id.* at 2220.

Once again, lower courts might have difficulty applying this factor to technologies that are automatic but not inescapable—say tracking by a particular mobile app that is voluntarily installed and can be deleted with one click—or tracking that is inescapable but not automatic—say the manual logging of a patient's symptoms taken by a doctor who provides a meaningful opt-out.

4. Factor Four? Efficiency Gain

One other factor played a vital role in the analysis of the majority opinion, yet is not listed in the helpful summary at the end: the relative efficiency with which the data allows the police to learn information about a target, as compared to what it would have required to collect equivalent data in an earlier technological age.[127]

> Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." For that reason, "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." . . . 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.[128]

The two internal quotes come from Justice Alito's concurrence in *Jones*, which also placed great weight on preventing the power of the police to increase dramatically through the progress of technology.[129] It connects to the *Carpenter* majority's invocation of the idea that the "central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance."[130] *Carpenter* puts to rest the dictum in *United States v. Knotts* that "We have never equated police efficiency with unconstitutionality, and we decline to do so now."[131]

The notion that the Fourth Amendment should prevent massive and sudden gains in police power thanks to technology connects to a

---

[127] In a different summary of the reasoning of the opinion, the Chief Justice did focus on this factor: "Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and *effortlessly compiled*." *Id.* at 10.
[128] *Id.* at 12.
[129] United States v. Jones, 565 U.S. 400, 429–430 (2012) (Alito, J., concurring).
[130] *Carpenter*, 138 S. Ct. at 2214.
[131] 460 U.S. 276, 284 (1983).

broad range of legal scholarship.[132] Of most direct relevance, it stems from an important article by Kevin Bankston and Ashkan Soltani.[133] They argue that the police engage in a Fourth Amendment search whenever a new technology makes it "much less expensive" to collect information about individuals.[134] The Article presents a compelling case that the facts of *Jones* meets this standard, because a police-installed GPS tracker significantly reduces the cost of location tracking. They lend rigor to this conclusion by meticulously reading FBI pursuit manuals and cross-referencing them to FBI Special Agent salary tables to conclude that a GPS tracker is twenty-eight times cheaper than covert pursuit, while tracking location by cell phone—akin to the facts of *Carpenter*—is almost twice as cheap as GPS.[135]

Bankston and Soltani pay due to other scholarship, most importantly Orin Kerr's theory of equilibrium adjustment.[136] According to this influential theory, "When new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[137] *Carpenter* is the ultimate embrace of both the Bankston-Soltani theory of efficiency and the Kerr theory of equilibrium adjustment.[138]

5. The Test

To summarize, *Carpenter* promulgates a new four-factor test that should be applied not necessarily to the specific facts of a case but

---

[132] *See also* Milligan, *supra* note 102, at 1333 (arguing that the increased efficiency of the government should be a factor in considering whether a court should engage in a "fresh" analysis of a legal doctrine).

[133] Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 YALE L.J. ONLINE 335 (2014).

[134] *Id.* at 337.

[135] *Id.* at 354 (depicting visually the efficiency multipliers of using technology to track location as opposed to manual surveillance).

[136] *Id.* at 337-38 (citing Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [hereinafter Kerr, *Equilibrium*]). They also generously connect it to my earlier writing. *Id.* at 337 *citing* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1312 (2012). The final building block is the work of Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

[137] Kerr, *Equilibrium*, *supra* note 136, at 480.

[138] Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision (arguing that the majority opinion embraces equilibrium-adjustment theory). No less than Edward Snowden has embraced this reading! Edward Snowden (@Snowden), Twitter (June 22, 2018, 11:23 AM), https://twitter.com/Snowden/status/1010196684066959360 ("The Bankston-Soltani Principle is alive and well").

rather to the category of information being sought. The court should ask whether that category of information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; (3) results from an inescapable and automatic for of data collection; and (4) represents a powerful gain in the efficiency of the police.

C. Applying the *Carpenter* Test

Under this test, what other databases full of third-party collected records are likely to be found protected by a reasonable expectation of privacy and fall outside the third-party doctrine? Consider a few examples.

1. Very Likely Covered: Web Browsing Records

I am confident that the *Carpenter* test will extend Fourth Amendment protection to web-browsing records collected by ISPs (or browser or operating system manufacturers). Justice Kennedy raises this prospect, complaining that the majority opinion doesn't reveal whether the seven-day threshold "should apply to information like IP addresses or website browsing history."[139]

Web browsing records possess a "deeply revealing nature", even if they record only the IP addresses of websites visited.[140] In 2009, I argued that "[t]he potential inconvenience, embarrassment, hardship, or pain that could result from the trove of data of [ISP monitoring] is limited only by the wickedness of one's imagination."[141] More recently, and succinctly, I testified to Congress that:

> The list of websites an individual visits, available to a [broadband Internet access service] provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.[142]

---

[139] Carpenter v. United States, 138 S. Ct. 2206, 2234 (2018) (Kennedy, J., dissenting).
[140] *See* Ohm, *Invasive ISP Surveillance*, *supra* note 10, at 1417.
[141] *Id.* at 1444.
[142] *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the H. Subcomm. on Commc'n & Tech. of the H. Comm. on Energy and Commerce*, 114th Cong. 5 (2016) (statement of Georgetown Law Professor Paul Ohm),

Similarly, Neil Richards has written about the sensitivity of records of "intellectual privacy" like these.[143] "Intellectual records—such as lists of Web sites visited, books owned, or terms entered into a search engine—are in a very real sense a partial transcript of the operation of a human mind. They implicate the freedom of thought and the freedom of intellectual exploration."[144] He argues that First Amendment concerns add a gloss to the Fourth Amendment and should require warrants for access to records like these.[145]

The efficiency gain represented by web-browsing records is profound. Just as CSLI has given the police unprecedented power tracking the location of targets at very low cost, so too can the police for the first time in human history access the reading habits of millions through their web browsing records with very little expense or effort.[146]

The "depth, breadth, and comprehensive nature" factor is sure to be more contestable when applied to web browsing records. This precise question has recently been debated publicly in the Federal Communications Commission, which enacted a sweeping broadband privacy rule in the final days of the Obama administration only to have Congress roll back the rule in the early days of the Trump administration.[147] In those proceedings, ISP lobbyists argued that their view into individual reading habits was far from comprehensive—in *Carpenter's* terms, they lacked depth and breadth—because individuals surf the web via different ISPs.[148] In the course of a single day, many people surf on their phone, their home broadband connection, and their work connection, using a different ISP for each one.[149] The police might plausibly argue that this distinguishes web browsing data from CSLI, because people tend to carry their cell phone

---

https://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-OhmP-20160614-U1.pdf.

[143] *See generally* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1108268.

[144] *Id.* at 436.

[145] *Id.* at 440.

[146] *Id.*

[147] Protecting the Privacy of Customers of Broadband, 81 Fed. Reg. 87274 (Dec. 2, 2016), https://www.federalregister.gov/documents/2016/12/02/2016-28006/protecting-the-privacy-of-customers-of-broadband-and-other-telecommunications-services (rule as enacted); Joint Resolution Providing for Congressional Disapproval effective April 3, 2017, Pub. L. No. 115-22, 131 Stat. 88, https://www.congress.gov/115/plaws/publ22/PLAW-115publ22.pdf (joint resolution reversing the rule).

[148] Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less Than Access by Others* 24–25 (Institute for Information Security & Privacy at Georgia Tech working paper, Feb. 29, 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

[149] *Id.*

in their pockets or purses throughout the day. Your cell phone works like a passive tracking device, sending pings to the nearest cell tower whenever you are using your phone and sometimes even when you are not.[150]

Finally, the police might argue that that web browsing records generated by an ISP are not "inescapable and automatic" in the same way as CSLI, because web browsing is an intentional and visible behavior—a record is logged whenever you use your phone or computer's web browser to access the web.[151]

Lower courts thus might struggle with the uncertainty inherent in a multi-factor test. ISP-generated web browsing records are much more deeply revealing and represent more of an efficiency gain than CSLI records.[152] Although they are deep, broad, of comprehensive reach, inescapable, and automatic, they might not rise for these factors to the same levels as CSLI.

I predict courts will have little difficulty holding that massive databases that record the IP addresses visited by an individual will meet the four factor test, even though a few factors cut in the other direction. Police access to these records will constitute a search and the third-party doctrine will not extend to cover them. Going forward, the police are well-advised to seek records like these only after first obtaining a warrant.

2. Most Likely Covered: Massive Collections of Telephone and Bank Records

Perhaps counter-intuitively, the police most likely now need a warrant to obtain massive collections of phone records or bank records, the same category of records held not to require a warrant in the third-party doctrine cases, *Smith v. Maryland*[153] and *Miller v. United States*.[154] Even though the Court declined to overturn those cases, hints throughout the *Carpenter* opinions suggest that, some day, these two opinions will be narrowed to the relatively non-comprehensive quantities available in the 1970s.[155]

---

[150] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) ("Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features.").

[151] *Cf.* Ohm, *Invasive ISP Surveillance*, *supra* note 10, at 1476 (describing the automatic nature of ISP surveillance, but concluding that it is conducted without meaningful consent).

[152] *Id.* at 1444; Richards, *supra* note 143, at 436.

[153] 442 U.S. 735 (1979)

[154] 425 U.S. 435 (1976)

[155] *Carpenter*, 138 S. Ct. at 2217 (declining to extend but not overturning *Smith* and *Miller*).

Bank records and phone records can be as deeply revealing as CSLI. *Carpenter's* dissenting opinions make this plain. Justice Kennedy concludes that "[t]he troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records."[156] Justice Gorsuch asks, "[w]hy is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)?"[157] These passages will be quoted the first time a defendant challenges the warrantless access by police to large quantities of this kind of information. Say the police use a subpoena to obtain years of credit card transactions or the NSA uses sub-warrant process to obtain millions of telephone metadata. It is now quite likely that courts will require a warrant for this kind of information, citing *Carpenter's* new test.

These courts will now be able to distinguish *Smith* and *Miller* because modern technology tends to produce databases of telephone or financial information that are far more voluminous and detailed than the records at issue in those 1970s cases. With the ubiquity of credit and decline of cash, almost every commercial transaction we make ends up in a bank record. These might today include great detail about what has been purchased, or a note by the merchant. Similarly, more metadata about communications is collected by today's telephones than in the past. Computer storage is much cheaper and easier to access than the paper records of the 1970's, reducing the incentive to ever delete anything.[158]

This shines new light on the dueling district court opinions that passed judgment on the NSA's massive telephony metadata program in 2013, one distinguishing *Smith* and the other feeling bound by the precedent. In *Klayman v. Obama*, Judge Richard Leon of the District Court for the District of Columbia held that the telephony program likely violated the Fourth Amendment, expressly declining to follow *Smith*.[159] "[T]he *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[160] Less than two weeks later, Judge William Pauley, in *ACLU v. Clapper*, came to the opposite conclusion, finding

---

[156] *Id.* at 2232 (Kennedy, J., dissenting).
[157] *Id.* at 2262 (Gorsuch, J., dissenting).
[158] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2011).
[159] 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated on other grounds*, 800 F.3d 559 (DC. Cir. 2015).
[160] *Id.* at 37.

that *Smith* controlled.[161] "Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment."[162]

History, in the form of *Carpenter*, has been much kinder to Judge Leon. A lower court judge trying to rule today that *Smith* controls would have to work much harder than Judge Pauley did, to distinguish *Carpenter*. Judge Pauley's reasoning seemed essentially to be that zero times a massive number is still equal to zero. *Smith* found no protectable Fourth Amendment interest in the numbers dialed for a single telephone customer, and no Fourth Amendment interest springs forth from the collection of the dialing habits of tens of millions of customers.[163]

Carpenter makes clear that the scale of data collection matters.[164] Constitutionally meaningful privacy can spring forth when records amass in the millions. Judge Pauley's reasoning should now be seen as defective, especially held next to Judge Leon's approach, which anticipated the *Carpenter* reasoning, albeit using different factors and language. Judge Leon offered four reasons to distinguish the NSA program from the facts of *Smith*. First, *Smith* involved data collected over a shorter time frame—14 days versus months or years.[165] Second, the detailed program between the NSA and the telephone companies created a far more intertwined relationship than the one-off request in *Smith*.[166] Third, the NSA had the technological capability "to store and analyze the phone metadata of every telephone user in the United States," providing perhaps the closest parallel between this opinion and *Carpenter*.[167] Finally, telephony metadata can reveal much more sensitive information than the phone records of the late-1970s.[168]

Had Judge Leon's opinion been written after *Carpenter*, it would have been seen as a direct application of the new opinion. Massive databases of telephony phone records implicate every one of Chief Justice's concerns about CSLI. The NSA's program implicated the Fourth Amendment, notwithstanding the supposed continued vitality

---

[161] 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *vacated on other grounds*, 785 F.3d 787 (2d Cir. 2015).

[162] *Id.* at 752.

[163] *Id.* ("The fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata." (citing *Smith*, 442 U.S. at 745)).

[164] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today.").

[165] *Klayman*, 957 F. Supp. 2d at 32.

[166] *Id.* at 32–33.

[167] *Id.* at 33.

[168] *Id.* at 33–34.

of *Smith*. Just like in *Carpenter* itself, I predict courts would "decline to extend *Smith* and *Miller*" to NSA-scale databases of telephony metadata.[169]

3. Uncertain Application: Databases of Medical Records and Genetic Information

The examples covered so far—massive databases of web browsing habits, telephone dialing records, and financial records—each satisfy all, or nearly all, of the four *Carpenter* factors and thus are likely to be found to be searches. But other databases of investigatory interest face a far less certain fate under the new test.

Under rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), law enforcement can access medical records stored by a covered provider with a grand jury subpoena.[170] Has *Carpenter* upset this rule, rendering this regulatory scheme now unconstitutional? Does a large database of health information now require a warrant to access?

For two of the four *Carpenter* factors, one could argue that medical records deserve as much or even more protection than CSLI. Medical records contain symptoms, diagnoses, and prescriptions, information that are likely far more deeply revealing than location information.[171] Even compared to owning a smartphone, individuals cannot easily choose to avoid professional medical care, making the production of these records more inescapable and automatic. The breadth and efficiency gain sub-factors probably weigh about the same for these records as for CSLI: most medical providers keep records dating back to the beginning of the interaction with the patient, and it would cost the police an exorbitant sum to compile the kind of information it can access for very little.

The other subfactors and factors cut the other way. The main subfactor that distinguishes CSLI from medical records is depth. The metronomic regularity with which an individual's location is tracked seemed quite important to the majority opinion.[172] In contrast, most people interact with the health care system only on occasion.[173]

While the creation of medical records might be as inescapable as CSLI, they usually are not as automatic. Unlike the take-it-or-leave-it and invisible quality of CSLI gathering, most medical records are

---

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

[170] 45 C.F.R. § 164.512(f)(1)(ii) (permitting disclosure of protected health information pursuant to a court order or grand jury subpoena).

[171] Ohm, *Sensitive Information*, *supra* note 79, at 1150–53.

[172] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

[173] The exceptions are hospitalized patients and people diagnosed with chronic or terminal conditions. Many of these people might be connected to 24/7 electronic devices that generate information in exactly the same fashion as a smart phone.

populated in clearly delineated interactions, when we are aware that we are being literally poked, prodded, and measured.

Finally, although the rise of electronic health records has made access to historical health information more efficient, it has always been the case that your doctor maintained a historical record of your health history, in a single location that they could access with little expense, and that they could be compelled to hand over to the police bearing a subpoena or a warrant. The efficiency gains in this situation are not nearly as dramatic as they are for the tracking of location or reading habits.

For these reasons, lower courts will consider this to be a relatively close call. For ordinary, healthy individuals, their medical records—while undoubtedly sensitive—are not nearly the product of the same kind of "tireless and absolute surveillance" at issue in *Carpenter*.[174] The digitization of these records has not experienced the same dramatic gains in efficiency as the tracking of location or reading habits.

What about a copy of an individual's DNA stored with a private third party? In his dissent Justice Gorsuch opines without analysis that "most lawyers and judges today" would require a warrant and probable cause to access DNA voluntarily stored with 23andMe.[175] This provides an important window into Justice Gorsuch's baseline attitude about the Fourth Amendment, and it might offer a window into how to directly appeal to him in the future. But this conclusion certainly doesn't flow from the *Carpenter* factors.

Without doubt, a copy of an individuals' genome satisfies the deeply revealing nature factor. Genetic information reveals propensity to disease, physical and mental characteristics, parentage, and genealogy.[176] It reveals this not only for the individual who uploaded the DNA but also for close relatives.[177]

None of the other factors seem to trigger the same concerns as CSLI. A single copy of the three billion base pairs that comprise a human DNA does not track activity and change over time, as with most of the other examples we have considered. At least under 23andMe's current business model, submissions are fundamentally voluntary, although close relatives who did not submit their DNA will be able to argue about the inescapable nature of their presence in the

---

[174] *Carpenter*, 138 S. Ct. at 2218.

[175] *Id.* at 2262 (Gorsuch, J., dissenting).

[176] Mike Silvestri, Note, *Naturally Shed DNA: The Fourth Amendment Implications in the Trail of Intimate Information We All Cannot Help But Leave Behind*, 41 U. BALT. L. REV.165, 168 (2011).

[177] Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 313 (2010).

data, if the police target them through their relatives' submissions.[178] Finally, there are other ways to obtain and sequence DNA of a known individual that will be only marginally less efficient than a subpoena from 23andMe.[179]

It seems unlikely that a court would require a warrant for DNA evidence held by a private third party based on a straight application of the *Carpenter* factors. This is not to say that there might not be other applications of the reasonable expectation of privacy test that would protect this information. It is a reminder that Carpenter is not the only path to finding that a Fourth Amendment search has occurred.

The basic rule of *Carpenter* alone presents a fundamental change to Fourth Amendment doctrine. It requires a warrant in many situations where none were required before. But this important change is just the first of many found within the reasoning of this opinion.

II. BEYOND THE CORE TEST OF *CARPENTER*

Based on the new substantive rule it announces, *Carpenter* is already on par with some of the most consequential Fourth Amendment cases of all time. But when you look beyond the core rule to some of the other revolutions wrought in the opinion, it is possible to conclude that *Carpenter* represents a fundamental shift, not merely an incremental adaptation. It turns the third-party doctrine inside out, requiring the government to account for the database design and information gathering decisions of private parties, decisions made without any state intervention. Its broad reasoning will apply not only when third parties are involved but also when the government conducts detailed digital surveillance by itself. And it creates three new rules of technological equivalence, which are much more straightforward to apply than the multi-factor test and which might end up be applied more often than the core rule.

A. The Third-Party Doctrine, Inside Out

Carpenter concludes that location information is protected "[w]hether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier . . . ."[180] This quote is breathtaking. It calls into question the bedrock rule that the Fourth Amendment concerns itself only with the activities of the government.[181] The police has never before had to account so fully for

---

[178] *Id.* at 337.

[179] Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U.L. REV. 857, 860-62 (2006).

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

[181] United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("This Court has also consistently construed this protection as proscribing only governmental action; it is

the independent decisions or actions of private actors. A private citizen could literally break into a house, break into a safe inside the house, steal what lay within the safe, and deliver the contents of the safe to the police.[182] So long as the police had nothing to do with the thief before he arrived at the stationhouse, they would be free to use the contents in court.[183]

For the first time, even though the police aren't responsible for the decisions that led to the creation of a collection of potential evidence, they nevertheless are held to account for the nature of the information collected. This has blurred the government action requirement in some important ways.

Of the four *Carpenter* factors, the one that is most influenced by the choices made by private actors is "depth, breadth, and comprehensive reach."[184] To be clear, the Court doesn't seem to be delving into the motivations of cell phone providers; warrant suppression hearings will not turn on the testimony of a T-Mobile executive explaining why the company structures its data the way it does. But the Constitutional meaning of the word "search" in cases like these now turn intrinsically on the results of the business decisions of companies.

Consider the breadth factor. The majority opinion emphasizes the importance of the "time machine" quality of CSLI. "With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintains records for up to five years."[185] For the most part, corporate retention policies are not set by regulation, at least not in the United States.[186] Each company must

---

wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.").

[182] *See* United States v. Jarrett, 338 F.3d 339, 346 (2006) (holding no government action and thus no Fourth Amendment violation to receive evidence from an anonymous hacker who had taken files from defendant's computer).

[183] *Id.*

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

[185] *Id.* at 2218.

[186] *See* Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 193 (2003) (discussing the role of "data preservation" in the United States, in the absence of a data retention mandate). One rare exception is that the FCC requires telephone companies to keep billing information about telephone toll calls for eighteen months. 47 C.F.R. § 42.6. In 2006, the European Union enacted a Data Retention Directive that mandated providers of some communications services to retain certain data for six to twenty-four months. Council Directive 2006/24, art. 1, 2006 O.J. (L 105) 54 (EC). It was declared invalid by the Court of Justice of the EU in 2014. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Ireland, 2014 E.C.R. 238, 21, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN.

weigh the potential benefits of having access to old data against the cost of data storage and the potential trouble in the form of cybersecurity risk or regulatory scrutiny. Practices vary widely even between companies in the same industry.[187] These choices are not made in consultation with the police, yet *Carpenter* has now given these private decisions Constitutional weight.[188]

The same can be said for the depth factor. Every company decides how much information to track and retain. Returning again to web-browsing surveillance, some ISPs retain very little evidence of the web browsing habits of their customers; others deploy deep packet inspection to view and store information about the content of communications between individuals and websites.[189] The first time the government is forced to defend against a challenge to the warrantless access to this kind of information, its fate might turn on where the ISP chose to position itself along this spectrum.

It could be argued, then, that the Court did more than narrow the third-party doctrine; it turned the third-party doctrine inside out. Not only does the mere fact that a target trusted personal information with a third party no longer insulate that data from Fourth Amendment scrutiny, but also the Constitutional duties imposed on the police might now turn on the independent decisions of third parties.

B. *Carpenter* and Direct Government Surveillance

Carpenter's reasoning should apply even when third parties are not involved. Its multi-factor test focuses most of its attention on the quality of the database alone, so it should apply even to databases compiled directly by the government. It might apply, for example, to analyze the use by the police of suspicionless, automated data collection techniques such as drone monitoring or facial recognition techniques used on surveillance camera data.[190]

Consider automated license plate readers.[191] These devices contain stationary cameras that sit for days, weeks, or longer on the

---

[187] Ernesto Van der Sar, *How Long Does Your ISP Store IP-Address Logs?*, TORRENTFREAK (June 29, 2012) https://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629/ (reporting IP address retention policies by ISPs from two weeks to eighteen months).

[188] *Carpenter*, 138 S. Ct. at 2218 (focusing on importance of fact that CSLI is stored for five years).

[189] Ohm, *Invasive ISP Surveillance*, *supra* note 10, at 1432–37

[190] Garvie et al., *supra* note 64, at 31-33.

[191] Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 544-46 (2017); Randy L. Dryer & S. Shane Stroud, *Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action*, 55 JURIMETRICS J. 225 (2015);

side of the road, deployed by government officials for the express purpose of recording the license plate numbers of cars that pass by a particular location.[192] These records are fed into databases from which the police can search for particular vehicles and that are sometimes automatically searched to locate stolen or unregistered cars, kidnap victims, or missing persons.[193]

A simplistic view of *Carpenter* would assume it had nothing to say about ALPRs. Because this technology does not involve private parties doing the data collection, this falls out of the potential application of the third-party doctrine.[194] Ignoring *Carpenter*, this case might be seen as a fairly straight application of Fourth Amendment cases involving plain view, knowing exposure, and reduced expectations of privacy in automobiles.[195] This simplistic view would suggest that no justification or judicial review is required to collect ALPR—much less a search warrant.[196]

The better reading is to understand that *Carpenter* has rewritten the rules for assessing the reasonable expectation of privacy in massive data gathering efforts, whether or not they are instigated by private actors.

How, then, does ALPR fare under the *Carpenter* factors? Because ALPR gives the police the ability to track the location and movement of cars, it seems superficially similar to CSLI. But because ALPR measures location only at fixed points throughout a city, it is likely to be seen as less problematic than CSLI for many of the *Carpenter* factors.[197] ALPR generates data that is neither as deep, broad, nor comprehensive as CSLI.[198] Because there is less data, it

---

Jessica Gutierrez Alm, Note, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127 (2015).

[192] Dryer & Stroud, *supra* note 191, at 229-36.

[193] Kimberly J. Winbush, *Use of License Plate Readers*, 32 A.L.R. 7TH Art. 8.

[194] To be clear, some ALPR implementations are run by private companies, who sell the data collected to state entities.

[195] New York v. Class, 475 U.S. 106, 114 (1986) (holding no reasonable expectation of privacy in automobile's vehicle identification number); Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality) ("One has a lesser expectation of privacy in a motor vehicle . . . .").

[196] United States v. Yang, 2018 WL 576827 (D. Nev. 2018) (holding no reasonable expectation of privacy in data collected in commercial license plate location database).

[197] Alm, *supra* note 191, at 151–52 (conceding that ALPR data is more intermittent and thus less sensitive than GPS data collected over the same period of time).

[198] *Id.*; *Yang*, 2018 WL 576827, at *6 (distinguishing *Jones* because ALPR does not "provide[] continuous contemporaneous information about the location of a vehicle" and does not "create[] a travel history of all of the movements of the targeted vehicle").

collectively is less deeply revealing than CSLI.[199] It is just as inescapable and automatic as CSLI, and the efficiency gain is approximately the same.

In the end, courts must balance these factors and determine whether ALPR implicates privacy enough to qualify as an invasion of a reasonable expectation of privacy. It is likely to be a very close call. But *Carpenter's* reasoning and multi-factor test should apply no less to it, even though third parties are not involved.

C. The New Rule of Technological Equivalence

Up to this point, I have focused almost entirely on the rules deriving from the majority opinion signed by five justices. Even more can be surmised by what the dissents added, because even though they disagreed with the majority's holding and reasoning, they provide tantalizing concessions suggesting that they too are willing to read the Fourth Amendment to cover more police conduct than the Court has recognized in the past. Reading all of the *Carpenter* opinions together suggests a broad new rule of technological equivalence. Any police activity that is the modern-day equivalent to activity that has been long protected under the Fourth Amendment is now protected.[200]

The new test relies on a simple syllogism: The Court in the past has held that information in a particular, traditional privacy context is protected by the Fourth Amendment. A technology produces information that is a modern-day equivalent to the information produced in the traditional context of step one. The information in the modern context is also protected by the Fourth Amendment.

There are three major strands of this new test in these opinions: activity that is technologically equivalent to prying into: the intimacy of the home, papers held in bailment, and private communications. Consider each in turn.

1. Information from Inside the Home

The rule of technological equivalence springs from *Kyllo*, the 2001 case involving the use by police of a thermal imaging device pointed at a suburban home in Florence, Oregon.[201] To prove that the defendant was growing marijuana inside his home, they used the device to reveal the heat that emanated from powerful grow lights and compared it to the ordinary heat patterns of his neighbors.[202] The Supreme Court, in an opinion by Justice Scalia, held that using a thermal imager on a home constituted a Fourth Amendment search.[203]

---

[199] Alm, *supra* note 191, at 151–52.
[200] Carpenter v. United States, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).
[201] *Kyllo*, 533 U.S. at 29.
[202] *Id.* at 30.
[203] *Id.* at 34–35.

Carpenter cites two crucial propositions from *Kyllo*.[204] The first is the idea that an inference can be a search.[205] The second is the proposition that when courts assess the impact of rapidly changing technology under the Fourth Amendment, it looks not only at the technology used in the facts of the case, but it extrapolates to future, more powerful versions of the technology. "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[206]

Putting these together, the first rule of technological equivalence applies to any information that reveals details from inside a home. The centerpiece of Justice Scalia's reasoning in *Kyllo* was that "in the home . . . *all* details are intimate details."[207] This kind of reasoning is quite likely to extend Fourth Amendment protection to the information generated by many devices that comprise the Internet of Things, because so much of it focuses on the interior of the home.[208] Smart speakers such as the Amazon Echo and Google Home record sounds from the inside of a home.[209] Smart TVs record the entertainment consumed in a home.[210] The Nest thermostat records the temperature of the home.[211] And the Ring doorbell records visitors to the home.[212]

---

[204] Carpenter v. United States, 138 S. Ct. 2206, 2218–19 (2018).

[205] *Kyllo*, 533 U.S. at 36; *Id.* at 44 (Stevens, J., dissenting) (criticizing the majority: "For the first time in its history, the Court assumes that an inference can amount to a Fourth Amendment violation"). The word Kyllo appears in the same paragraph as any form of the word "infer" 38 times in opinions and 112 times in secondary sources, based on a Westlaw search performed on August 6, 2018.

[206] *Id.* at 36. The word Kyllo appears in the same paragraph as the phrase "more sophisticated systems" 13 times in opinions and 99 times in secondary sources, based on a Westlaw search performed on August 6, 2018.

[207] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[208] Ferguson, *supra* note 18, at 836–40.

[209] Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done about It*, 29 LOY. CONSUMER L. REV. 229, 239–241 (2017) (Discussing privacy implications of Amazon Echo and OK Google); Michael Harrigan, *Privacy Versus Justice: Amazon's First Amendment Battle in the Cloud*, 45 W. ST. L. REV. 91, 91–93 (2017) (discussing government's attempt to obtain Amazon Echo recording during murder trial).

[210] *Rediger*, *supra* note 209, at 241–42 (discussing Samsung Smart TV privacy scandal).

[211] Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV. 192, 196–99 (2016) (Discussing privacy implications of Nest Labs products); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 511 (2016) (discussing privacy implications of Google Nest and competitors).

[212] Reed Albergotti, *How Amazon's Latest Security Device Let People Spy on You*, THE INFORMATION (May 11, 2018), https://www.theinformation.com/articles/how-amazons-latest-security-device-let-people-spy-on-you (discussing privacy vulnerability of Ring doorbell system). *Cf.* James O'Toole, *Cops can access your connected home data*, CNN

The *rule of equivalence to the home* suggests that the police now need a warrant to obtain any of this information. The *Kyllo* reasoning suggests that we need not even consider the sensitivity or intimacy of the information obtained, because "all details are intimate details."[213]

Notice that the technological equivalence rule is far simpler and more predictable to apply than the majority's multi-factor test. Once the equivalence is made, the conduct is ruled a search, and the analysis ends. One need not endure the multi-factor gymnastics required to analyze the status of CSLI.

Just a few months after *Carpenter* was decided, the Seventh Circuit already applied this rule. In *Naperville Smart Meter Awareness v. Naperville*,[214] the court held that a city's mandatory use of smart meters on homes constituted a search under the Fourth Amendment.[215] Because different appliances produce different "load signatures," "researchers can predict the appliances that are present in a home and when those appliances are used."[216] This "reveals when people are home, when people are away, when people sleep and eat, what types of appliances are in the home, and when those appliances are used."[217] Although the case cites *Carpenter* in a brief passage declining to apply the third-party doctrine, its core reasoning is an application of the revitalized *Kyllo*.[218] This is just the beginning. *Carpenter* has given *Kyllo* new life. This might turn out to be as profound a legacy of *Carpenter* as its core reasoning.

2. Bailment

Both Justices Kennedy and Gorsuch lean on the law of bailment, suggesting a revitalization of this ancient legal concept by prosecutors and criminal defense lawyers. Consider Justice Gorsuch's academic disquisition on the idea:

> [T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest

---

(June 16, 2014), https://money.cnn.com/2014/06/16/technology/smart-home-footage/index.html (discussing tech companies' requirements to release home security footage to law enforcement).

[213] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[214] No. 16-3766 (7th Cir. Aug. 16, 2018), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2018/D08-16/C:16-3766:J:Kanne:aut:T:fnOp:N:2203659:S:0.

[215] The court ruled that the search was reasonable because the smart meter information was gathered for a non-criminal-investigation government purpose, and the benefits of the program outweighed the intrusion on privacy. Naperville Smart Meter Awareness, slip op. at 10–12.

[216] *Id.*

[217] *Id.* at 6.

[218] *Id.* at 8–9.

> in them. 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) . . . . 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 . . . . These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents. Whatever may be left of *Smith* and *Miller,* few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest.[219]

Justice Kennedy, while not engaging with the idea at such length, seems to agree that modern-day equivalents to bailment ought not to be subject to the third-party doctrine.[220]

This reasoning, by two justices in dissent,[221] signals quite clearly that the Court will someday rule that "modern-day papers and effects" held by third parties will be protected by the Fourth Amendment. This seems to describe almost perfectly the contemporary state of cloud computing. Services like Google Drive and Dropbox allow individuals to move their modern-day papers into the cloud.[222] Services like

---

[219] *Id.* at 2268-69 (Gorsuch, J., dissenting).

[220] *Id.* at 2228 (noting that the private parties in *Smith* and *Miller* "were not bailees or custodians of the records" at issue). *Id.* at 2259 n.6 ("[T]his is not a case in which someone has entrusted papers that he or she owns to the safekeeping of another, and it does not involve a bailment.").

[221] Four, if you include Justices Alito and Thomas, who signed Justice Kennedy's dissent.

[222] Mickey Meece, *A User's Guide to Finding Storage Space in the Cloud*, N.Y. Times, May 16, 2012, https://www.nytimes.com/2012/05/17/technology/personaltech/a-computer-users-guide-to-cloud-storage.html; Dropbox, *What is Dropbox*, https://www.dropbox.com/features (last visited Aug. 12, 2018); Google Drive, *Features*, https://gsuite.google.com/products/drive/ (last visited Aug. 12, 2018).

Amazon Web Services create dedicated virtualized computers on cloud servers, which customers can fill with data, which other users are not permitted to access.[223] If law enforcement tries to obtain any information stored on services such as these, it seems quite likely that lower courts will rule such accesses to be controlled by the *technological equivalence of bailment* rule, thus requiring a warrant.

3. Private Communications

Similarly, all nine justices signed onto opinions that declare that the police need a warrant to read the content of email messages.[224] Although this is still merely dicta, it is stated clearly enough so that lower courts can and should begin to rely on the clear signal.

This is important because, to date, only one appellate court, the Sixth Circuit, has required the police to obtain a warrant to access the content of stored email messages, in the 2010 case *United States v. Warshak*.[225] *Warshak* itself is cited approvingly in *Carpenter* in three separate opinions: the majority,[226] and the dissents by Justices Kennedy,[227] and Gorsuch.[228]

This is yet another application of the rule of technological equivalence, the *rule of equivalence to private communications*. Email messages are to modern communications what postal letters were at the time of *Ex Parte Jackson*.[229] As the *Warshak* court said, "[e]mail is the technological scion of tangible mail."[230]

More than a bare majority of the court's justices have now signaled they would hold that the contents of email are protected by the Fourth Amendment. The police must obtain a search warrant, or proceed under an exception to the warrant requirement such as exigent circumstances, to access the contents of email messages.

It is likely that this rule will protect other forms of technologically abetted communications other than email. Any person-to-person communications are likely protected. The police most likely now need a warrant to obtain, from storage or in real-time, instant

---

[223] Alex Hern, *Amazon Web Services: The Secret to the Online Retailer's Future Success*, THE GUARDIAN, Feb. 2, 2017, https://www.theguardian.com/technology/2017/feb/02/amazon-web-services-the-secret-to-the-online-retailers-future-success; Amazon Web Services, *What is AWS?*, https://aws.amazon.com/what-is-aws/ (last visited Aug. 12, 2018).

[224] Carpenter, 138 S. Ct. at 2222; *Id.* at 2230 (Kennedy, J., dissenting); *Id.* at 2269 (Gorsuch, J., dissenting).

[225] 631 F.3d 266, 288 (6th Cir. 2010).

[226] *Id.* at 2222.

[227] *Id.* at 2230.

[228] *Id.* at 2269.

[229] 96 U.S. 727 (1877) (requiring a warrant to open sealed letters in the possession of the postal service).

[230] 631 F.3d at 286.

messages, direct messages on a social networking service, or text messages.[231]

Carpenter upends Fourth Amendment doctrine. Its most revolutionary contribution, however, might be what it has done to Fourth Amendment reasoning.

III. *CARPENTER*'S TECHNOLOGY EXCEPTIONALISM

The beating heart of the *Carpenter* majority opinion is its deep and abiding belief in the exceptional nature of the modern technological era. This seems to come directly from Chief Justice Roberts, who revealed the same attitude four years earlier, in the majority opinion in *Riley v. California*.[232] Recent advances in technology such as the smartphone and the Internet have led to differences in kind and not merely in degree from the technology of the past.

The Chief Justice's break with the technological past supports a break with judicial precedent in several ways. A belief in the exceptionalism of modern technology leads one to dismiss otherwise conventional analogies. *Riley* and *Carpenter* refuse to compare smartphones to address books, diaries, or even telephones. Because analogical reasoning sits at the heart of legal reasoning and stare decisis, the Court's rejection of analogies like these gives it an opening to chart a new path.

Reasoning about exceptional technology requires courts to develop a deep understanding of technology, and these opinions are notable for the way they rely heavily on technological explication. They are full of citations to amici briefs and they press the boundaries of judicial notice.

Finally, the Court's tech exceptionalism closes the door on scholars who have been trying to reinvent *Katz* by appealing to surveys, history, or positive law. Each of these three approaches peer into our past and rely on the ability of lay people to understand what has changed. *Carpenter* and *Riley* instead look into the future, and for that reason, reject all three of these proposals.

---

[231] *See* Robin Miller, *Expectation of Privacy in Text Transmissions to or from Pager, Cellular Telephone, or Other Wireless Personal Communications Device*, 25 A.L.R. 6th 201 (Originally published in 2007) (aggregating Fourth Amendment cases about text messages). *Compare* Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 282-284 (2016) (analyzing text messages and direct social media messages under the Fourth Amendment and applying a modern-day equivalent analysis), *with* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 504-505 (2012) (analyzing text messages under the Fourth Amendment and rejecting a modern-day equivalent analysis).

[232] Riley v. California, 134 S. Ct. 2473 (2014).

A. Rejecting Conventional Analogies

In *Riley*, the Chief Justice famously, dismissively said:

> The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items [such as billfolds, address books, purses, and wallets]. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.[233]

This is a surprising, wholesale rejection of a conventional analogy: The government urged the Court to compare a digital technology to a physical world precursor, and the Court not only refused to do so but responded with sarcastic exaggeration. Understanding this quote is the key to understanding both *Riley* and *Carpenter* and, more broadly, the key to understanding how profoundly these cases have transformed the way the Court will reason through Fourth Amendment cases.

The horseback quote is only the most extreme example of the Court refusing to draw an analogy to an ordinary, physical world item or activity. The court similarly dispenses with many other traditional analogies: a search through a cell phone is not like rifling through a diary or pockets;[234] the term 'cell phone' itself is misleading, because these are "minicomputers that also happen to have the capacity to be used as a telephone";[235] and accessing CSLI is nothing like tailing a car.[236]

The Court did embrace some analogies in these opinions, but these tended to feel far more fanciful than the ones it rejected, drawn essentially from science fiction rather than conventional reality. Cell phones might be mistaken by aliens to be "features of human anatomy";[237] tracking CSLI is akin to "attaching an ankle monitor to the phone's user";[238] searching through a cell phone is more invasive than searching through a house.[239]

Legal scholars have long analyzed the critical role of reasoning by analogy to legal reasoning.[240] Judges decide cases by determining

---

[233] *Id.* at 2488.
[234] Riley v. California, 134 S. Ct. 2473, 2484 (2014).
[235] *Id.* at 2489.
[236] Carpenter, 138 S. Ct. at 2218.
[237] Riley, 134 S. Ct. at 2484.
[238] Carpenter, 138 S. Ct. at 2218.
[239] Riley, 134 S. Ct. at 2491-92.
[240] EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING (Chicago, 2d ed 2013); LLOYD L. WEINREB, LEGAL REASON: THE USE OF ANALOGY IN LEGAL ARGUMENT (Cambridge, 2005); Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV.

whether new fact pattern X is similar to previously analyzed fact pattern Y in relevant respects.[241] Analogical reasoning gains force in legal reasoning because it is the "usual form of reasoning in daily life."[242]

In Fourth Amendment jurisprudence, analogies play a dominant role. Tracking beepers are like following a car on city streets;[243] hidden microphones are like the human memory;[244] and pen registers are like human telephone operators.[245] The *Carpenter c*ourt's rejection of conventional analogies is thus a significant development. By refusing to credit the government's preferred analogies, the Court could distinguish *Smith* and *Miller* without needing to overturn the forty-year-old precedents.

What *Carpenter* and *Riley* have done to analogy and precedent might be their most important and lasting revolution. The Court seems to be signaling that a foundation stone of legal reasoning—drawing comparisons to the ordinary, physical stuff of life—has been rendered impermissible. We are all now living in a science fictional universe, at least when making arguments to the Court. Why has the Court made this move, is it justified, and what does it mean for Fourth Amendment law going forward?

B. The Chief Justice's Technology Exceptionalism

What causes these analogies to fail, in the eyes of the Court, is the nature of the technological era in which we are living. The Chief Justice has declared in successive landmark decisions that the information age has produced technological changes that are different in kind not merely in degree from the technology of the past.[246] He first announced this worldview, writing for eight Justices, in *Riley v. California*, which held that the police need a warrant to search the contents of a cell phone incident to valid arrest.[247] In *Carpenter*, he

---

741 (1993); Frederick Schauer, *Analogy in the Supreme Court: Lozman V City of Riviera Beach, Florida*, 2013 SUP. CT. REV. 405, 407 (2013).

[241] Sunstein, *supra* note 240, at 745.

[242] *Id.* at 743.

[243] United States v. Knotts, 460 U.S. 276, 285 (1983) (comparing the use of a tracking beeper to following a suspect in a police car).

[244] United States v. White, 401 U.S. 745, 751 (1971) (comparing a hidden microphone to an informant who writes down what he has heard).

[245] Smith v. Maryland, 442 U.S. 735, 745 (1979) (comparing automatic telephone switching information to a human operator).

[246] *E.g.,* Riley v. California, 134 S. Ct. 2473, 2488 (2014) ("The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.").

[247] *Id.*

exhibits the same beliefs, this time to even more consequential doctrinal import.

The Chief Justice writes these opinions with a palpable, wide-eyed amazement at the speed with which the power and scale of technology has changed. In *Riley*, he marvels that in the five short years from arrest to Supreme Court ruling, the world had rendered obsolete the flip phone used by one of the defendants in the cases being reviewed.[248] Similarly, in *Carpenter* he compares with astonishment the costly task of tracking a person's location on foot to the efficiency of doing so by downloading their CSLI.[249]

He emphasizes the sheer scale of modern technology. These opinions are replete with mentions of the word "millions"—"millions of pages of text;"[250] "over a million apps available;"[251] "396 million cell phone service accounts in the United States—for a nation of 326 million people";[252] and a database automatically tracking the location of "400 million devices".[253]

Some of the words and phrases used in these opinions would seem more at home in science fiction than the U.S. Reports. These opinions invoke time travel,[254] space travel,[255] and visits from Martians.[256]

The Chief Justice is equally impressed with the social dynamics of technological change, the rate with which technology like the smartphone has been adopted by Americans and has shaped our social interactions. In both opinions, he cites statistics and surveys demonstrating the large percentage of Americans who use these devices.[257] He punctuates both with a statistic that has clearly left a lasting impression: "12% [of smartphone owners] admit[] that they even use their phones in the shower."[258]

---

[248] *Riley*, 134 S. Ct. at 2484.
[249] Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018).
[250] *Riley*, 134 S. Ct. at 2489.
[251] *Id.* at 2490.
[252] *Carpenter*, 138 S. Ct at 2211.
[253] *Id.* at 2218.
[254] *Id.* at 2218.
[255] *Riley*, 134 S. Ct. at 2487.
[256] *Id.* at 2484.
[257] *Id.* at 2490 (citing statistic that 90% of American adults who own a cell phone use it to store private documents); *Carpenter*, 138 S. Ct at 2211 (noting that Americans own 396 million cell phones, meaning more devices than people).
[258] *Riley*, 134 S. Ct. at 2490 (citing HARRIS INTERACTIVE, 2013 MOBILE CONSUMER HABITS STUDY (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf); *Carpenter*, 138 S. Ct at 2218. Do these people simply use their phone next to their shower to listen to audio inside the shower, or are they wrapping their device in a waterproof pouch and bringing it in with them? The Chief Justice does not say.

The Chief Justice connects this wide-eyed technology exceptionalism into Fourth Amendment doctrine with this key move: the "[m]odern cell phone is not just another technological convenience. With all they contain and all they reveal, they hold for many Americans, the privacies of life."[259] Nothing that has come before can compare to these devices for the amount and variety of sensitive and intimate information about individuals.[260] In the passage perhaps most bristling with Constitutional import in these opinions, the Chief Justice declares that a person's privacy interest in the contents of a smartphone is more significant than the privacy interest in a home, the ancient, paradigmatic high water mark for privacy.[261]

What flows directly from the conclusion that these devices are unprecedented vessels for sensitive information is the recognition that technology has significantly increased the power of the police.[262] Keeping with the science fiction theme, these devices and the records they produce essentially transform the police into crime fighting robots outfitted with superhuman powers. They can peer into the past, avoiding the "frailties of recollection."[263] They can tail every suspect "every moment of every day for five years."[264] They are "tireless,"[265] "ever alert, and their memory is nearly infallible."[266]

All of this powerful rhetoric about the power of information technology has a profound impact on the reasoning of the court by allowing it to discard analogies to what have come before. For an institution that places historical continuity, *stare decisis*, and analogical reasoning at its core, this opinion's refusal to accept straightforward analogies is jarring.

C. The Argument for Technology Exceptionalism

The Court's tech exceptionalism is not science fiction; it is well justified. Changes in information technology in recent years have posed challenges to privacy that are different in kind not merely in degree than what has come before. Advances in the past two decades, in particular, have dramatically decreased the ability with which individuals can understand, much less control, the ways they are observed and even controlled.

---

[259] *Riley*, 134 S. Ct. at 2494-95.
[260] *Id.* at 2489–91.
[261] *Id.* at 2491 ("[I]t also contains a broad array of private information never found in a home in any form—unless the phone is.").
[262] Kerr, *Equilibrium*, *supra* note 136.
[263] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).
[264] *Id.* at 2218.
[265] *Id.*
[266] *Id.* at 2219.

Ryan Calo has written about the tech exceptionalism of our time.[267] He argues that the field of Cyberlaw is premised on the idea that fundamental advances in technology such as the Internet or robotics are so qualitatively and quantitatively different from what has come before that they force changes in the law.[268] Specifically, "a technology is exceptional when its introduction into the mainstream requires a systematic change to the law or legal institutions in order to reproduce, or if necessary displace, an existing balance of values."[269] This is precisely what the Chief Justice argued that the smartphone and CSLI have wrought.

The Chief Justice's arguments are backed by two decades of scholarly writing. This is perhaps best seen in the output of the annual Privacy Law Scholars Conference (PLSC), now in its twelfth year.[270] Authors in this conference have presented almost six hundred articles, the vast majority of which have argued that specific changes in technology have threatened information privacy.[271]

Articles presented at PLSC establish that technological advances increase the quantity and quality of information available to third parties.[272] They highlight the role inference plays in disrupting settled expectations of privacy, because it is no longer enough to look at what is literally in the data;[273] advances in technology such as machine learning give individuals the power to learn more than what is on the surface.[274]

PLSC articles have documented how these advances consistently thwart expectations and put pressure on social norms.[275] A massive literature chronicles the harms that these incursions into privacy have wrought on individuals, groups, and institutions.[276] Many articles have

---

[267] Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CAL. L. REV. 513, 550-553 (2015)

[268] *Id.* at 552.

[269] *Id.* at 552.

[270] 2018 Privacy Law Scholars Conference (PLSC2018), https://www.law.berkeley.edu/research/bclt/bcltevents/2018annual-privacy-law-scholars-conference/ (visited August 12, 2018).

[271] Data on file with author.

[272] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2006).

[273] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[274] Steven M. Bellovin et. al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY 556 (2014)

[275] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

[276] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1196 (2015).

identified harms that go beyond traditional injury to harms that interfere with autonomy and personal development.[277] Another massive literature discusses the futility of self-help techniques for addressing these risks.[278]

It is fair to say that almost no scholarly writing refutes the argument that recent changes in technology have put significant pressure on privacy and privacy law. The very small number of detractors or skeptics who write in the field tend to argue instead that the harms are either poorly supported by empirical support or outweighed by the harm that would be caused by changes to the law.[279]

The Chief Justice's tech exceptionalism finds support from a significant body of scholarly argument. Far from being just the unfounded opinion of a sixty-something jurist,[280] tech exceptionalism is an argument well within the mainstream of contemporary academic writing in information privacy law.

D. Expertise and Analogy

Having established that Chief Justice Roberts views modern technology as exceptional, and having defended this view, how does exceptionalism lead him to disregard analogy and break with the Court's precedents? How does tech exceptionalism change Fourth Amendment jurisprudence? When tech exceptionalism collides with the legal system, it creates a fundamental problem of expertise. Non-technical lawyers are simply not trained to explicate the ways in which fundamental changes in complex technology put pressure on privacy and increase government power.[281] They need to seek help outside experts. This is especially necessary when the complex technology

---

[277] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999).

[278] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008).

[279] Adam Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 467 (2014); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 (2011); Lior Jacob Strahilevitz, *Privacy Versus Antidiscrimination*, 75 U. CHI. L. REV. 363 (2008); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of A Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

[280] Strahilevitz, *Ten Thoughts*, *supra* note 3 ("The majority text and approach are consistent with the Chief's dim views about legal scholarship generally and with his stated preference for minimalist decisions.").

[281] *See* Calo, *supra* note xx at 560 (describing the "tradition of melding legal and technical expertise" in cyberlaw).

continues to change, presenting not only a complex target of analysis, but a moving one.

This leaves the Court needing to turn to unusual sources of technological explication.[282] *Riley* cites multiple amici briefs for detailed, technical details about technology that were never entered into the lower court record.[283] It cites to reports by government agencies known for objective scientific expertise.[284] It also contains what is probably the first Supreme Court citation ever to a smartphone operating system manual.[285]

Carpenter cites fewer external sources for technological facts than *Riley*, in part because it can cite *Riley* for some of its facts.[286] Still, the only citation in the majority opinion to an amici brief is to one authored by digital civil rights groups including the Electronic Frontier Foundation, which provides critical facts about the improved precision of cell tower tracking techniques since the facts of the case.[287]

Tech exceptionalism's expertise problem explains and justifies the Court's rejection of the simplistic, conventional analogies offered by the government in *Riley* and *Carpenter*, such as the refusal to compare a smartphone to an address book.[288] In order to make proper sense of an analogy comparing an old X to a new Y one must be expert enough to understand the relevant similarities and differences between X and Y.

---

[282] Milligan, *supra* note 102 (arguing that public interest groups and litigants should educate courts when simple analogies fail).

[283] Riley, 134 S. Ct. at 2486 (citing Brief of United States as amicus curiae about unbreakability of iPhone encryption); *id.* at 2487 (citing Brief for Criminal Law Professors about use by law enforcement of "Faraday bags"); *id.* at 2489 (citing Brief for Center for Democracy & Technology about amount of physical world document equivalent to 16 gigabytes of digital storage); *id.* at 2490 (citing Brief for Electronic Privacy Information Center about number of smartphone apps installed by the average user).

[284] *Id.* at 2486 (citing report by National Institute for Standards and Technology); *id.* at 2487 (citing report by National Institute of Justice).

[285] *Id.* at 2487 (citing iPhone User Guide for iOS 7.1 Software 10 (2014).

[286] Carpenter, 138 S. Ct. 2206, 2214 (citing *Riley* about "'immense storage capacity' of modern cell phones"); *id.* at 2218 (citing *Riley* for cell phone ownership and use statistics).

[287] *Id.* at 2219 ("[W]ith new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.") (citing Brief for Electronic Frontier Foundation et al.).

[288] *Supra* Part III.A. *See* Marc McAllister, The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning, 36 S. Ill. U. L.J. 475, 477 (2012) ("In rejecting Fourth Amendment claims involving warrantless use of sophisticated technologies, courts often rely upon analogies to prior 'search' cases, but these supposed analogies are so far removed from the new forms of surveillance that analogies to them only confuse, rather than clarify, the actual analysis required by Katz.").

This connection between analogy and expertise has been explored by legal scholars, to support the argument that lawyers can sometimes see analogies that non-lawyers cannot. Frederick Schauer and Barbara Spellman offer one account.[289] A lawyer sees instantly the relevant similarities between "Nazis and civil rights demonstrators of the 1960s," a comparison the non-lawyer might see as "bizarre, even offensive."[290] When viewed through the domain-specific expertise of First Amendment law, the similarities between groups wishing to march in public places but opposed by viewpoint-based laws comes into view.[291]

Tech exceptionalism turns the tables on lawyers, relegating them to the role of the non-experts who cannot understand the failure of a given analogy by stripping them of their ability to accurately characterize Y or to compare it to X.[292] Luke Milligan argues that when faced with complex technology in surveillance cases, courts should deploy an "analogy breaker," rejecting simple analogies in favor of a "fresh default analysis.[293]

The challenge for criminal lawyers and scholars going forward is to grapple with the nuances of technology. The Court now places great emphasis on the subtle intricacies of how technology operates, and how it differs in important ways from what has come before. We need to look to computer scientists and engineers to serve as experts and to write legal scholarship, to help guide the way.[294] But this is not simply a scientific or engineering exercise, because the Court cares also about the sociology of technology, putting an impetus on new interdisciplinary bridges between law and fields such as Science and Technology Studies and Human-Computer Interaction.[295]

The Court's new focus on the legitimate and appropriate sources of facts should spur some modest institutional changes. Both prosecutors and defense lawyers now need sophisticated technological

---

[289] Frederick Schauer & Barbara A. Spellman, *Analogy, Expertise, and Experience*, 84 U. CHI. L. REV. 249, 264-65 (2017).

[290] *Id.* at 264.

[291] *Id.* at 264.

[292] *Id.* at 266-67 (arguing against skeptics who claim that all analogical reasoning rests on an appeal to the underlying principle).

[293] Milligan, *supra* note 102, at 1333. Milligan weighs this proposal down with concepts of "mono-analogical" and "poly-analogical" features of comparisons. *Id.* at 1324-35. Although I do not find these to be useful additions to the theory, I believe they lead to an identical place to the theory I am proposing.

[294] *See* Calo, *supra* note xx, at 561 ("Whether at conferences or hearings, in papers or in draft legislation, the legally and technically savvy will need to be in constant conversation.").

[295] SERGIO SISMONDO, AN INTRODUCTION TO SCIENCE AND TECHNOLOGY STUDIES (2001); JEFF JOHNSON, DESIGNING WITH THE MIND IN MIND: SIMPLE GUIDE TO UNDERSTANDING USER INTERFACE DESIGN RULES (1st ed. 2010).

support, either in the form of dedicated technologists or, at the very least, hybrid-trained lawyers with some experience in technology. Civil liberties groups will need to continue their trend of hiring in-house technologists. It is not a coincidence that many of the amici briefs cited by the Court were authored by groups focused on digital civil rights and are well-known for hiring and associating with trained technologists.[296]

Finally, this shift should encourage legal scholars who write about the Fourth Amendment and technology to place a premium on getting the technological details right. The only law review article cited in either majority opinion was authored by Orin Kerr, who not only is a preeminent scholar but also one with formal technological training and experience;[297] and many of the majority's arguments owe a debt to other uncited articles, also written by trained or technologically sophisticated legal scholars.[298]

E. Time and Technological Change

The unprecedented, rapidly changing nature of technology also causes the Court to relax its rules about restricting its attention to the record evidence before it. Traditionally, appellate courts including the Supreme Court refuse to peek outside the record developed in the trial court. Some of this reticence comes from Article III of the Constitution, which limits federal courts to consider only "cases or controversies."[299] But it also reflects an institutional modesty that recognizes that appellate courts are distant from the facts.

Tech exceptionalism puts pressure on this understanding. The premise of tech exceptionalism is that technology changes today at unprecedented rates. An appellate court that looks only to the past is using the outdated examples in the record to set rules for the present and future, which might already differ in important ways. In *Carpenter* and *Riley*, the Court refuses to resign itself to this fate. Instead, it relaxes, just a little, its practices, by peeking a little at the present and the future.

This leads to three new principles of judicial fact-finding: refresh what has changed during the pendency of litigation and appeal; relax

---

[296] Riley, 134 S. Ct. at 2489 (citing Brief for Center for Democracy & Technology); *id.* at 2490 (citing Brief for Electronic Privacy Information Center). Carpenter, 138 S. Ct. at 2219 (citing Brief for Electronic Frontier Foundation et al.).

[297] Riley, 134 S. Ct. at 2489 (citing Orin Kerr, *Foreward: Account for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404-05 (2013))

[298] Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PENN. J. CON. L. 933 (2016); Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 YALE L.J. ONLINE 335 (2014); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3.

[299] U.S. CONST. Art. III. § 2.

the rules of judicial notice; and understand that the future is ascertainable.

First, the Court in these opinions shows a willingness to refresh the record, a little, at each stage of appeal. It takes several years to proceed from an arrest, through appeals, to review by the Supreme Court.[300] Given the rate of change of technology, the passage of time means the Court is always reviewing a historical relic in cases like these. The Court has responded by seeing fit to peek at the present, availing itself of the kind of unusual sources of information listed above, including amici.

Second, the Court also seems willing to relax its ordinary attitudes about taking judicial notice. In *Riley*, the Court cited the iPhone User Guide for the proposition that "modern cell phones can be programmed to lock automatically after some period of inactivity,"[301] a citation criticized by observers.[302] This extra-record "fact" was introduced to the Court through an amici brief filed by the United States in support of the State of California.[303] Although the Court does not explicitly acknowledge that it is taking judicial notice of this technological fact, this seems to be what it has done.[304]

Finally, the Court is not afraid to look past the facts of the technology at issue before it, to the present and likely near-future technology that we will soon encounter. The Court implies that the future is ascertainable; it is something we can talk about and predict with some certainty. In *Carpenter*, the Court assessed how cell-site technology had changed in the intervening seven years.[305] In *Riley*, the Court noted how the flip phone at issue had already "faded in popularity".[306]

---

[300] In *Riley*, the defendants in the two cases reviewed were arrested in August 2009 and September 2007. Riley v. California, Petition for Writ of Certiorari, *available at* http://sblog.s3.amazonaws.com/wp-content/uploads/2013/09/Riley-cert-petition-final1.pdf; United States v. Wurie, 728 F.3d 1 (1st Cir. 2013). The Supreme Court decided the cases on June 25, 2014, almost five and seven years after the arrests, respectively. Riley, 134 S. Ct. at 2473. In *Carpenter*, the defendant was arrested in April 2011, United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), seven years before the Supreme Court's decision. Carpenter, 138 S. Ct. at 2206.

[301] Riley, 134 S. Ct. at 2487.

[302] H. Adam Shapiro, *Court Continues to Misunderstand How We Use Technology*, DANZINGER, SHAPIRO & LEAVITT BLOG (June 25, 2014) https://www.ds-l.com/blog/2014/06/the-supreme-court-continued-it.html.

[303] Brief for the United States as Amici Curiae Supporting Respondent, Riley v. California, 134 S. Ct. 2473 (2014) at 11 (No. 13-132) (2014 WL 1389032).

[304] *See* Fed. R. Evid. 201 (allowing federal court to take judicial notice of facts that "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned").

[305] Carpenter, 138 S. Ct. at 2219 (noting how more cell towers and better technology had brought the accuracy of CSLI closer to GPS).

[306] Riley, 134 S. Ct. at 2484.

This sets up a rather stark contrast to what Justice Kennedy said (and did) in *City of Ontario v. Quon*, a 2010 opinion that held that a government employer's review of an employee's text messages on a work pager was reasonable, declining to rule on whether it amounted to a search.[307] Justice Kennedy cautioned that the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[308] *Carpenter* prefers the *Kyllo* attitude toward predicting the future: we "must take account of more sophisticated systems that are already in use or in development."[309] Chief Justice Roberts could not disagree more fundamentally.

F. Refusing to Look Backwards

The Court decided to look to the future in the face of many urging it to look to the past in novel ways. Scholars urged the court to base its Fourth Amendment decisions on a close examination of, in turn, survey evidence, history, or sources of positive law. The Court ignored all of this advice, much to the consternation of the scholars involved.

1. The Surveyors

The objective prong of the REP test asks whether an expectation of privacy is "one that society is prepared to recognize as reasonable."[310] Some have read the prong to hitch the Fourth Amendment's protections to public sentiment.[311] Police power respected the bounds of Constitutional privacy so long as it did not stray too far from what ordinary people or average people expect.[312] The REP test should produce results that follow, at least to some extent, what people actually expect, or so these observers have argued.[313]

For those who would connect REP to the attitudes of ordinary people, the next step was to survey Americans, gathering opinions about various police practices, including many fact patterns that have already been the subject of Supreme Court case law. This originated with landmark work in the late 1990's by Chris Slobogin and Joseph

---

[307] 560 U.S. 746, 760 (2010).
[308] *Id.* at 759.
[309] Carpenter, 138 S. Ct. 2206, 2218-19 *quoting* Kyllo v. United States, 533 U.S. 27, 36.
[310] Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).
[311] Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205 (2015) [hereinafter Kugler & Strahilevitz, *Actual Expectations*].
[312] Smith v. Maryland, 442 U.S. 735, 740 (1979).
[313] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311, at 224-25.

Schumacher.[314] Through its surveys, the pair concluded that public sentiment about the invasiveness of police practice disagreed in many instances with the Court's Fourth Amendment doctrine.[315] For example, the survey respondents judged "perusing bank records" to be the thirty-eighth most invasive activity out of fifty surveyed, roughly the same as "hospital surgery on shoulder",[316] contradicting the relative holdings of *Miller* and *Winston v. Lee*.[317]

The turn to survey work has been revived and invigorated in recent years.[318] A chief advocate is Lior Strahilevitz, working with Matthew Kugler.[319] Strahilevitz and Kugler have written two articles reporting the results of two surveys they have conducted.[320] The authors spend much more time than Slobogin and Schumacher trying to lay out a doctrinal and normative case for why judges ought to look to surveys when assessing police practices.[321] They cite democratic legitimacy, doctrinal coherence and predictability, and the costs of creating legal rules that ordinary citizens don't understand or expect as the primary justifications.[322]

This work follows the broader trend in legal scholarship finding new roles and contexts for quantitative social science.[323] Although Strahilevitz himself is not directly associated with law and economics, he is part of the faculty of the University of Chicago, the cradle of the

---

[314] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727 (1993).
[315] *Id.* at 740.
[316] *Id.*
[317] *Compare* Miller v. United States, 425 U.S. 435 (1976) (obtaining bank records not a search) *with* Winston v. Lee, 470 U.S. 753, 759-63 (1985) (requiring probable cause plus additional factors for surgery in shoulder).
[318] Bernard Chao, et al., *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CAL. L. REV. (forthcoming 2018); Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. (forthcoming 2017) [hereinafter Kugler & Strahilevitz, *The Myth*]; Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016); Christine S. Scott-Hayward, et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19 (2015-2016); Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311; Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus,* 49 WAKE FOREST L. REV. 261 (2014).
[319] See Kugler & Strahilevitz, *The Myth*, *supra* note 318; Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311.
[320] Kugler & Strahilevitz, *The Myth*, *supra* note 318; Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311.
[321] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311, at 227.
[322] *Id.*
[323] Lee Epstein & Gary King, *The Rules of Inference*, 69 U. CHI. L. REV. 1, 3 (2002).

discipline. His arguments for incorporating surveys into the Fourth Amendment expressly relies on principles from law and economics.[324]

These scholars, joined by others who have published surveys about privacy attitudes, wrote an amicus brief urging the *Carpenter* Court to look to the evidence they had gathered.[325] The brief summarizes results showing that very few Americans are aware of the ability of cell phone companies to track the location of phones using CSLI, supporting an argument for requiring a warrant in the case.[326]

The majority opinion failed to cite any of the survey evidence in its opinion. The survey work did appear in some of the dissents, albeit in support of only minor arguments.[327]

Strahilevitz has been among the sharpest critics of the majority opinion's reasoning, if not its result.[328] He faults the opinion not just for failing to cite survey work but for more broadly refusing to engage legal scholarship.[329]

2. The Legal Historians

One notable legal historian who has focused on the Fourth Amendment in recent years is Laura Donohue who has advocated for what might be described as an expansive originalism for the Fourth Amendment.[330] In her carefully researched, book-length article, Donohue excavates English and colonial law as well as the story of the drafting of the Constitution and Bill of Rights to take on misimpressions of Fourth Amendment history.[331]

Professor Donohue also authored an amicus brief in *Carpenter*, on behalf of herself and other "scholars of the history and original

---

[324] *Id.* at 227 (advocating a normative framework for the Fourth Amendment that "enhance[s] social welfare" and does not spur people to "take excessive precautions to protect their information"); *id.* ("[W]e think there is a strong case to be made that misalignment between the law and social expectations is detrimental for both efficiency and fairness-related reasons.").

[325] Brief for Empirical Fourth Amendment Scholars as Amici Curiae Supporting Petitioner, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (2017 WL 3530963).

[326] *Id.* Part I (citing study showing that only 26.5% of American cell phone users expressed even a general awareness about location tracking by cell phone companies).

[327] Carpenter v. United States, 138 S. Ct. 2206, 2244 n.10 (2018) (Thomas, J., dissenting) (citing Strahilevitz and Tokson article, among others, to demonstrate scholarly disapproval of the *Katz* test); *Id.* at 2265 (Gorsuch, J., dissenting) (citing Slobogin and Schumacher article for proposition that "judicial judgments often fail to reflect public views").

[328] Strahilevitz, *Ten Thoughts*, *supra* note 3.

[329] *Id.*

[330] Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 (2016).

[331] *Id.*

meaning of the Fourth Amendment".[332] The historians argued that rummaging through CSLI fits the meaning of the word "search" at the time of the founding and analogized the search of CSLI as akin to the use of general warrants that motivated the Revolution and the drafters of the Bill of Rights.[333] They noted how the early, celebrated cases of *Wilkes v. Wood* and *Entick v. Carrington* involved opinions that focused on how searches created invasions into privacy and personal affairs.[334] Among the other signers of the historians' brief was William Cuddihy, author of a well-cited, exhaustive history of the Fourth Amendment.[335]

The majority opinion engages in almost no historical analysis, beyond an obligatory acknowledgement of the role the opposition to general warrants and writs of assistance played in sparking the American Revolution.[336] Justices Thomas and Gorsuch engaged the history much more deeply in their respective dissents. Only Justice Thomas cites the work of legal historians, including Donohue and Cuddihy, while using the history to conclude that no search had occurred in this case, the opposite conclusion the historians pressed in their brief.[337]

3. The Positive Law Proponents

Finally, much attention has been paid to a recent law review article by William Baude and James Stern.[338] The authors propose a dramatically simplified question to replace the REP: "have [officials] engaged in an investigative act that would be unlawful for a similarly situated private actor to perform"?[339] If yes, a search has occurred; if not, no search has occurred.[340] The sources of illegality would include property law—thus bearing some resemblance to Justice Scalia's rule in *Jones*—but would go beyond to include "any prohibitory legal provisions, whether legislative, judicial, or administrative in origin, and whether classified as criminal or civil in nature."[341]

---

[332] Brief for Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae Supporting Petitioner, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (2017 WL 3530961).
[333] *Id.* at 3.
[334] *Id.*
[335] WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING (2009).
[336] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).
[337] *Id.* at 2243 (Thomas, J., dissenting) (citing Cuddihy); *id.* at 2240 (citing Donohue); *id.* at 2241 (same); *id.* at 2243 (same).
[338] William Baude & James Stern, The Positive Law Model of the Fourth Amendment, 129 HARV. L. REV. 1821 (2016).
[339] *Id.* at 1825.
[340] The rule would extend to seizures as well. *Id.* at 1830.
[341] *Id.* at 1833.

The authors argue that confining the meaning of search to issues addressed in the positive law is better than the REP test because "[i]t is conceptually clear, theoretically sound, less subjective, more legal, and responsive both to social fact and technological change."[342] They connect the proposal to historical references to positive law in critiques of British search and seizure practice; the structural advantages of making Fourth Amendment law act similarly to Fifth Amendment takings jurisprudence; and the idea that judging the police by the same laws that govern us all contributes to the rule of law.[343] Finally, they point to practical advantages, touting that it betters the REP test by being clearer, equally adaptable, and more respectful of the role of the legislature.[344]

Neither Baude nor Stern signed an amicus brief, but their article was cited in the Petitioner's opening brief.[345] Although the majority opinion failed to cite the article, it was cited in the dissents by both Justices Thomas and Gorsuch.[346]

4. Looking Forwards Not Backwards

The majority's refusal to embrace surveys, legal history, or the positive law when applying the Fourth Amendment to new technology should be seen as an affirmative rejection by five justices of these proposals, not indifference nor an oversight. The reason, once again, is tech exceptionalism. Seen through this lens, approaches that look backward in time, like these three, do not serve a useful purpose, for the focus should turn to the present and future. This is not to say that history, surveys, and positive law will never again figure into Fourth Amendment cases involving advances in information technology. But for now, the Court has turned its back on them.

Most directly, history seems the wrong tool for reasoning about these questions. Given the significant differences between CSLI tracking and the location tracking of a few decades ago, it seems especially unhelpful to wonder what the Framers would have thought about CSLI.

In *Riley* and *Carpenter*, history is invoked, but briefly and in passing. History seems useful to the modern Fourth Amendment only held at a distance and as a source of very general analogy. "The fact that technology now allows an individual to carry [a cell phone's worth of] information in his hand does not make the information any less

---

[342] *Id.* at 1888.
[343] *Id.* at 1837–1850.
[344] *Id.* at 1850–55.
[345] Brief for petitioner at 22, 32, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (2017 WL 3575179).
[346] Carpenter v. United States, 138 S. Ct. 2206, 2242 (2018) (Thomas, J., dissenting); *id.* at 2268 (Gorsuch, J., dissenting).

worthy of the protection for which the Founders fought."[347] The suggestion is that searching a cell phone is akin to "the reviled 'general warrants' and 'writs of assistance' of the colonial era."[348]

The Fourth Amendment is "informed by historical understandings 'of what was deemed an unreasonable search and seizure [when the Fourth Amendment] was adopted."[349] It is meant to "secure 'the privacies of life' against 'arbitrary power'" and "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance'".[350] These quoted passages are the sum total of the Court's attention to history in these two landmark opinions, a far cry from what the historians had hoped to see.

The problem with survey results in an era of tech exceptionalism is that lay attitudes about rapidly changing technology are likely to be rapidly changing, unstable, and uninformed. It's one thing to look at survey results to ask whether Americans think the police ought to be able to hide a recording device on a confidential informant. Average Americans have had nearly a century to understand voice recording and millennia to have developed fixed opinions about misplaced confidences.[351] This seems like the kind of technology-aided surveillance that a court might rely on a survey to assess. But asking average Americans to opine about cell-site location information or facial recognition or smart meters is simply not likely to produce informed opinions.[352] At best, it will reflect still developing attitudes about misunderstood and changing technologies. To be fair, Strahilevitz suggests something similar in his work.[353] Why we would hitch our Constitutionally bestowed civil liberties to the quicksand of the median American's technology literacy defies common sense.

The situation for the positive law is even worse. It compounds the confusion the general public has about the social meaning of rapidly changing technology with the vagaries of the sclerotic legislative and judicial processes.[354] This is especially true when

---

[347] *Riley*, 134 S. Ct. at 2495.
[348] *Id.* at 2494.
[349] *Carpenter*, 138 S. Ct. at 2214.
[350] *Id.* at 2214.
[351] *E.g.*, CUDDIHY, *supra* note 335, at 333 (discussing use of informants for securing warrants in the colonies).
[352] Freiwald, *First Principles*, *supra* note 71, at *25.
[353] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311, at 234–35 ("We do think that the case for placing real weight on survey responses is strongest when laypeople are being surveyed on issues that are familiar to them. For that reason, our surveys ask people about the sorts of technologies that they are likely to have encountered in the world . . . .").
[354] Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 326–27 (2015–2016) (critiquing the positive law model by pointing to many reasons legislatures might not have yet regulated a new technology, including "regulatory lag").

considering statutory privacy law. Many have decried the state of privacy legislation at the national and state levels today as failing properly to account for the harms that can be wrought by new technology.[355] The situation has become much worse in recent years, as technology companies have discovered Washington and today represent an industry that spends some of the most lobbying Congress.[356]

To put it succinctly, applying the Fourth Amendment to information technology requires the Court to look forward; all three of the proposed approaches look backward instead.

IV. *CARPENTER* AS A REPLACEMENT FOR *KATZ*

The conventional wisdom suggests that *Carpenter* is an application or expansion of the *Katz* REP test. We might think of it instead as an outright replacement for REP, at least for cases involving complex modern technology.

Carpenter settles long-standing disputes about both prongs of the *Katz* test. It affirms the conclusion that *"Katz* has only one step,"[357] providing no analysis whatsoever into the defendant's subjective expectation of privacy. For the objective prong, *Carpenter* means that the Court has at long last answered the fundamental question about REP: does the objective prong merely describe the expectations of ordinary Americans or does it ask judges to propound a normative vision for the kind of society the Constitution seeks to protect? *Carpenter* selects the normative over the descriptive: given tech exceptionalism, the role for courts is to protect the balance of power between the state (in the form of the police) and the people, refusing to let technological change eviscerate individual privacy and security from the state.

These changes do more than apply or extend *Katz*, they reinvent and supplant that venerable opinion. The REP test has been replaced by *Carpenter's* multi-factor test and the rule of technological equivalence. Time will reveal that the *Katz* era has ended. This is a welcome development; the *Carpenter* era will be seen as more predictable, Constitutionally supported, and responsive to the rate of change of technology than the REP test it has replaced.

---

[355] Ohm, *Sensitive Information*, *supra* note 79, at 1127.

[356] *Id.* at 329 (discussing role of private interest groups in debates surrounding legislation regulating privacy in data); *See also* OPENSECRETS.ORG, 2017 TOP INDUSTRIES, https://www.opensecrets.org/lobby/top.php?showYear=2017&indexType=I (last visited Aug. 24, 2018).

[357] Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113 (2015) [hereinafter Kerr, *One Step*].

A. The Subjective Prong: *Katz* has Only One Step

Carpenter supports what Orin Kerr has argued: "the subjective prong [of the REP test] has become a phantom doctrine."[358] As initially expressed in Justice Harlan's concurrence, the REP test was a two-pronged inquiry: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[359]

Scholars have offered at least three different interpretations for the subjective prong, none of which appear in *Carpenter*. Most often, Courts seem to treat the subjective test as an inquiry into what the person actually intended in her mind.[360] Did this person actually believe her actions or communications were shielded from public view? The problem with this formulation is that it never seems to matter. Almost never is the Court confronted with a situation in which this version of the subjective prong fails but the objective prong does not.

Kerr argues that the subjective prong could instead have been read, long ago, to place more emphasis on Justice Harlan's use of the word "exhibited."[361] By this reading, the subjective prong asks whether the defendant had "voluntarily exposed" information to the public. Critically, this version of the test would not require courts to probe the inner mind of the person asserting privacy. Rather, it would look to the objective measures the person took to block the government's view.[362]

A third way of interpreting the subjective prong is offered by Lior Strahilevitz and Matthew Kugler.[363] They argue that courts should consult survey evidence in the subjective prong, "us[ing] the sentiments of the median American citizen as a proxy for the defendant's subjective expectation of privacy."[364]

We do not know how the *Carpenter* Court interpreted the subjective prong, because the majority's opinion gives it almost no attention. The opinion never mentions the word "subjective." Its recitation of the REP test barely nods at this as a separate requirement: An REP is "[w]hen an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable . . . ."[365] In applying the test, the Court makes no attempt to analyze subjective and objective expectations separately.

---

[358] *Id.* at 133.
[359] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[360] Kerr, *One Step*, *supra* note 357, at 130-31.
[361] Kerr, *One Step*, *supra* note 357, at 126.
[362] *Id.*
[363] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 311, at 240-44.
[364] *Id.* at 241.
[365] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

Carpenter did not put a nail in the coffin of the subjective prong, because it was interred six feet under long ago.[366] The subjective prong has become an unmarked grave, one courts trample from above, not even acknowledging the presence of the decomposed remains underfoot.

B. The Objective Prong: Victory of the Normative Fourth Amendment

By recognizing tech exceptionalism, the *Carpenter* court restores—at least for the time being—the normative vision of the Fourth Amendment, taking sides in a very old debate: is the objective prong of the REP test—which asks, is society prepared to accept an expectation of privacy as reasonable—a descriptive or normative inquiry?[367] Is it the judge's role to examine what the reasonable individual or median member of society expects, or is it the judge's charge to imagine how its rulings can help set our society onto a particular path?[368]

Justice Harlan, who first conceived of the reasonable expectation of privacy test, made his opinion about this question quite clear only four years after *Katz*, albeit in dissent:

> Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.[369]

Too often, the Court has strayed from this path, thinking of its role in interpreting REP as merely descriptive.[370]

---

[366] Kerr, *One Step*, *supra* note 357, at 114 (attributing abandonment of subjective prong to cases from the 1970s and 1980s).

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

[368] Kerr, *Four Models*, *supra* note 81, at 507-24.

[369] United States v. White, 401 U.S. 745, 786 (1971) (White, J., dissenting).

[370] *E.g.* Bond v. United States, 529 U.S. 334, 338 (2000) ("When a bus passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled."); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."); Smith v. Maryland, 442 U.S. 735, 744 (1979) ("When he used his phone,

Carpenter advances the idea that, at least when technology changes rapidly, the proper role for the court is the normative one Justice Harlan advocated. We should not "saddle" society with merely what it has come to expect.[371]

Technology exceptionalism once again settles this question. The proper accounting of the way technology has disrupted individual privacy, distorted society, and rebalanced the power between the state and its citizens thrusts the judiciary into a more aggressive role interpreting the Fourth Amendment than it has assumed in the past.

This, once again, is at the heart of Orin Kerr's equilibrium adjustment theory and Bankston and Soltani's theory of government efficiency gain.[372] The Constitution is premised on an ordinary rate of change in the balance of power between the state and the people. The Fourth Amendment is our national thermostat, recalibrating what the police can and cannot do. In periods of ordinary technological change—which describes the first two hundred years or so of our national experience—we could afford a merely descriptive Fourth Amendment, trusting our institutions to respond to change. But when faced with moments of disruptive technological restructuring of power and institutions, the normative Fourth Amendment—and the court's central role in protecting it—becomes an imperative.

C. The Argument for Moving Beyond *Katz*

Once we recognize that *Carpenter* has moved beyond *Katz* in important ways, we should ask whether this is a desirable result. I contend that the future sketched out by *Carpenter* is to be preferred than the world *Katz* has given us.

First, *Carpenter's* multi-factor test will lead to more predictability than *Katz*. The REP test has always been open-textured and ambiguous. What is a reasonable expectation of privacy? Is the objective prong to be analyzed descriptively or normatively?

Ambiguous at birth, the subsequent decades have done very little to lend *Katz* concreteness or predictability. Orin Kerr persuasively argues that the Court chooses from among a menu of four different approaches—private facts, probabilistic, positive law, and

---

petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

[371] *Accord* Kerr, *Four Models*, *supra* note 81, at 543–44.

[372] Bankston and Soltani, *supra* note 133; Kerr, *Equilibrium-Adjustment*, *supra* note 136.

policy—to assess REP.[373] But it is hard to discern a pattern to when the Court chooses each.[374]

In contrast, the multi-factor test is relatively easy to apply. As the examples in Part I demonstrate, there will be disagreement about how to apply, say, the "depth, breadth, and comprehensive reach" factor to different databases. But the spectrum of disagreement will be narrow and cabined compared to wide ranging across Kerr's four models that *Katz* has created.[375] *Carpenter* sweeps away the cacophony of the four models, selecting a normative over descriptive methodology with four concrete factors.

Second, the approach is, if anything, more closely connected to the text and history of the Constitution. To be clear, neither *Katz* nor *Carpenter* purports to adhere closely to the text and history. But *Katz* suffered by focusing on a principle—privacy—that is nowhere to be seen on the literal text of the amendment.

In contrast, *Carpenter's* test and reasoning resonate much more directly with the history. The Court treats the Fourth Amendment as primarily a restriction on government power, not just a protection of privacy.[376] The factors hone in on the features of data that fuel the government's power. "Comprehensive reach" allows the government to conduct surveillance on the entire populace; "breadth" allows it to peer back in time; "depth" and "deeply revealing nature" raise the prospect of meaningful harm.

In addition, the location information in *Carpenter* and the smart phone in *Riley* are arguably intrinsic aspects of individual personality, connecting them to the "persons" recited in the text of the opinion.

Third, the technological exceptionalism at the heart of the new test impels courts to consider deeply the specific features of technology, and society's embrace of technology, that was usually lacking from the conventional REP test. This will prevent the kind of indifference to progress that plagued the third-party doctrine from its birth.

CONCLUSION

Based on the new rule it announces, Carpenter is already on par with some of the most consequential Fourth Amendment cases of all time. But when one looks beyond the core rule to some of the other

---

[373] Kerr, *Four Models*, *supra* note 81, at 506.

[374] *Id.* at 524 ("The hard cases tend to be those in which the different models point judges to different conclusions. In those cases, courts must choose which model applies to that particular case.").

[375] *Id.*

[376] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("[T]he Amendment seeks to secure 'the privacies of life' against 'arbitrary power' . . . . "[A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'").

revolutions wrought in the opinion, one is left to conclude that Carpenter represents a fundamental shift, not merely an incremental adaptation. *Carpenter* turns the third-party doctrine inside-out, eroding the requirement of government action as a core underpinning of the Fourth Amendment; it applies even when the government acts directly to collect information about many individuals in massive databases; it implicitly suggests three new rules of technological equivalence; it embraces a technological exceptionalism that permits a break from judicial precedent; and it begins the overdue project of replacing the *Katz* REP test.

On December 19, 1967, the day after the Court decided *Katz*, it probably was not yet clear what the Court had done.[377] The decision was rightly seen as important, the culmination of almost forty years of scholarly commentary against the narrow trespass theory reasoning of *Olmstead v. United States*.[378] What might have been seen at first as merely an important decision only later was rightfully recognized for the many revolutions it created.

What *Katz* did to *Olmstead*, *Carpenter* will do to *Katz,* transforming the Fourth Amendment into something fundamentally new. The Fourth Amendment has become the vessel for a civil right that, for the first time, responds flexibly and rapidly to the insistent challenges of new technology on privacy.

---

[377] Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 5 (2009).

[378] 277 U.S. 438 (1928). Winn, *supra* note 377, at 2 ("The Olmstead decision was very divisive, and the government's use of wiretaps continued to be controversial.").