CONNECTICUT
LAW REVIEW

VOLUME 49 SEPTEMBER 2017 NUMBER 5

Keynote

Judicial Engagement with Surveillance Technology

JAMES ORENSTEIN

Judicial Engagement with Surveillance Technology

Keynote

JAMES ORENSTEIN*

Good morning, and thank you for this opportunity to share some thoughts with you. Of course, I am speaking only for myself, and not for the federal judiciary or anyone else.

Before we turn to new surveillance technologies, let's take a moment to consider what a couple of relics—the land-line telephone and the pager—can teach us about the development of technology-related law.

In 1928, roughly fifty years after the telephone's invention, the Supreme Court held in *Olmstead* that the Constitution did not prohibit warrantless wiretapping because even a liberal construction of the Fourth Amendment could not "justify enlarg[ing its] language . . . beyond the . . . meaning of houses, persons, papers, and effects . . . ."[1]

It was a decision that the Court later deemed to be ill advised in two important ways. The first time, of course, was in 1967, when the Court overruled the decision in *Katz*.[2] What *Olmstead* got wrong, as the Court then decided, was that the Fourth Amendment protects not places, but the people who live in them.[3] And as Justice Harlan explained, we must measure that protection against the standard of the reasonable expectation of privacy.[4]

Another forty years later, the Court found a more fundamental flaw in *Olmstead*. In the *Quon* case in 2010, the Court was asked to consider the extent to which a public employee was entitled to Fourth Amendment protection for the communications he received on his government-issued pager.[5]

For those of you so impolite as to be too young to know what that is, the pager was a mobile device you strapped to your belt that had an alphanumeric readout of maybe twenty characters. It could be used to

---

* United States Magistrate Judge, Eastern District of New York. I am grateful to Christine Scott-Hayward for comments on an earlier draft of these remarks.

[1] Olmstead v. United States, 277 U.S. 438, 465 (1928).

[2] Katz v. United States, 389 U.S. 347, 353 (1967).

[3] *Id.* at 351.

[4] *See id.* at 361 (Harlan, J. concurring).

[5] City of Ontario v. Quon, 560 U.S. 746, 750 (2010).

receive a short message such as a callback number, or perhaps a code such as 911 to indicate urgency, or in later versions perhaps a short phrase.

They had limited utility, and tended to be worn only by those who, in the days before widespread cell phone usage, needed to be reachable on short notice when away from their homes and offices: doctors, drug dealers, and, in the fall of 2001, a police sergeant in Ontario, California named Jeff Quon.[6]

The police department had given Quon a pager to use on police business, and like all early adopters of every new technology since the beginning of time, he somehow figured out a way to use his shiny new device for a version of what we would now call sexting.[7] When his enthusiastic innovation ran up the department's phone bill, it audited his pager messages, saw what he was doing, and disciplined him for using the pager for decidedly unauthorized purposes.[8] He sued for a violation of his civil rights, and that's where we come in.[9]

The Court ruled against Quon under the precise circumstances of that case,[10] but it declined to provide any guidance for lower courts about whether and how the Fourth Amendment applied more generally to text messages sent via employer-issued pagers, because they were worried about rushing into things. Citing *Olmstead*'s reversal in *Katz*, and noting that pagers had been supplanted by smartphones while the case was pending, the Court wrote:

> The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear . . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.[11]

In other words, to be admittedly tendentious about it, the Justices concluded that part of their predecessors' mistake in *Olmstead* was that a half century of telephone use was not enough time for them to figure out how that new technology would affect our society.

Recognizing that they were at the dawn of a new digital age, the Justices seemed to worry that it might take another forty years to correct a similar mistake if they failed to figure out how this new technology might become an essential part of the way a free society exchanges ideas. Some

---

[6] *Id.* at 750–51.
[7] *Id.* at 753.
[8] *Id.*
[9] *Id.* at 753–54.
[10] *Id.* at 764–65.
[11] *Id.*

things, the Court seemed to be saying, are too hard to figure out quickly and too important to hurry.

Such caution is certainly understandable: in the decades between *Olmstead* and *Katz*, the telephone had remained essentially unchallenged as the world's dominant communications technology. While it had become more efficient in any number of ways, the basic technological concept of two tin cans connected by a vibrating piece of string remained unchanged.

And as the twentieth century waned, much the same was true of the rest of the world's technology: if you wanted to look up some information, you pulled a book from a shelf. If you wanted to see where someone was going, you got up off your behind and followed them.

Sure, technology made communications more efficient and richer as the radio gave way to the television, and the calculator to the computer. But the pace of change in the basic way we lived our lives was gradual enough that the technological world in which I entered kindergarten was essentially the same as the one in which I graduated from law school.

For people who grew up in that world and went on to become judges, it could easily bolster an assumption that they had the luxury of sitting back to wait and see how technological advances would play out before jumping to conclusions about how to shape the law around them.

And recognizing the breadth of change confronting the Court in 2010 must have made it even easier to be cautious: there was so much new technology to consider, that it made sense not to take a headlong plunge.

But today, with no small amount of trepidation about critiquing controlling Supreme Court law, I'd like to discuss why I think that the judiciary can no longer afford such patience and caution.

The tenth anniversary of the advent of the iPhone a couple of weeks ago was just one of the many major technological milestones of this new century.[12] In the years since Jeff Quon got his pager, we have seen the rise of Google, Facebook, Amazon, and Twitter.

Using technology that was "nearly inconceivable just a few decades ago,"[13] we now have at our fingertips virtually the entirety of human knowledge, and we carry in our pockets at all times a collection of information that amounts to what Chief Justice Roberts called in *Riley* "[t]he sum of an individual's private life."[14]

The increasing pace of technological change is matched by correspondingly accelerated changes in our society. We not only have more information, but we have the power to process and manipulate it at

---

[12] *See* Chance Miller, *Apple Commemorates 10 Year iPhone Anniversary, Tim Cook Says 'The Best is Yet to Come'*, 9TO5MAC (Jan. 8, 2017, 4:48 PM), https://9to5mac.com/2017/01/08/apple-10th-anniversary-iphone/ (describing the evolution of the iPhone in anticipation of its 10-year anniversary).

[13] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[14] *Id.* at 2489.

blinding speed and in previously unimaginable ways—not just to connect with others, but to track those connections; and not just to spread knowledge, but to spread harm.

So why does that counsel for a departure from the understandably cautious approach of *Quon*? Because with the quantum leap in both technology and our use of it, we no longer have the safety net, as we did just a decade ago, of a set of rules that were written for a world bearing even a passing resemblance to our own.

The basic statutory tools that Congress has given us to assess technology-driven surveillance methods were written in 1986, 1994, and to a minor extent in 2001—before any of the technologies we'll be discussing today were invented.[15] And there's no prospect of any new guidance coming from Congress any time soon.

As the world we live in drifts ever farther from the world in which our laws were written, we simply don't have the luxury of waiting to see how new technology will shape our society's views over a span of decades: cops and criminals alike will all be using these new technologies, and one way or another courts will have to pass on whether those uses are lawful.

To be sure, the Supreme Court can for a while put off making broad constitutional pronouncements. It did that just last term when it declined to review one of several recent circuit court decisions examining whether the government needs a warrant to get historical location tracking records.[16]

But those of us in the trenches can't choose not to decide an issue that's ripe for review. And when it comes to new forms of surveillance, the applicability of the Fourth Amendment is plainly one of the issues that must be decided.

Nor is it just lower court judges like me for whom the need to engage with new technologies is urgent.

The longer the appellate courts wait to tackle these issues, the longer law enforcement and private enterprise are hampered in their respective endeavors by the uncertainty of what is and isn't allowed—and the longer

---

[15] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994); 18 U.S.C. § 2510 (2012); 47 U.S.C § 1001 (2012); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107–56, § 214, 115 Stat. 286, 287 (2001) (amending 18 U.S.C. §§ 3121, 3123, 3124, 3127).

[16] *Davis v. United States*, 136 S. Ct. 479–80 (2015) (denying certiorari to review *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015)); *see also United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (petitions for certiorari pending); *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013). Several months after I made the remarks, the Supreme Court agreed to review a decision that no warrant is required for law enforcement to secure historical location records. *See United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, *Carpenter v. United States*, No. 16-402, 2017 WL 2407484 (U.S. June 5, 2017). As of the date of this writing, *Carpenter* remains under review.

those of us at the bottom of the food chain struggle to give what often turn out to be conflicting answers.

While that uncertainty can of course help refine the issues for the Supreme Court to resolve, I'm not sure that in this context the tradeoff makes sense, in part because the uncertainty surrounding these issues can feed on itself to amplify the cost of indecision.

To give just one example, consider the issues surrounding technology-based location tracking. The lower courts have been addressing the issue since 2005, and have reached a wide array of results both as to the statutory standard for allowing the government to conduct such surveillance, and the Fourth Amendment implications.[17] But the Supreme Court has thus far declined to take up the issue.[18]

An opportunity arose in 2011 when the Court agreed to review a circuit court decision that the warrantless use of a tracking device violated the Fourth Amendment.[19] The Court instead decided the case based on the physical trespass involved in planting the tracker.[20]

But while the Court's opinion avoided the issue, a majority of the Justices did not: five of them signed on to concurring opinions that called into question the continuing viability of the doctrine critical to the technology issue: the third-party doctrine.[21]

In this context, as most of you know, third-party doctrine holds that if

---

[17] *See* Carpenter, 819 F.3d at 883-84 (holding that cellphone location tracking does not implicate the Fourth Amendment, distinguishing "between the content of a communication and the information necessary to convey it"); United States v. Graham, 824 F.3d at 424 (holding "that the Government's acquisition of historical CSLI from Defendants' cell phone provider did not violate the Fourth Amendment") (en banc; vacating and disagreeing with previous panel opinion that the warrantless seizure of cell site location information violated the defendant's Fourth Amendment rights); *see also* In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) (holding, on statutory grounds, that the government can obtain cell site location information upon a showing short of probable cause under the Stored Communications Act, but that the court has discretion require a showing of probable cause); In re Application of U.S. for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (holding that the government can obtain cell site location information without a showing of probable cause pursuant to the pen register statute and the Stored Communications Act); In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005) (holding that government must show probable cause to secure access to cell site location information).

[18] *See* cases cited in n.16, *supra*. As noted above, several months after delivering this address, the Supreme Court agreed to review the issue in *Carpenter*.

[19] United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010), *aff'd on other grounds sub nom* United States v. Jones, 565 U.S. 400, 403–4 (2012).

[20] *See Jones*, 565 U.S. at 404–05 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

[21] *Id.* at 417 (Sotomayor, J., concurring); *id.* at 424 (Alito, J., concurring) (joined by Justices Ginsberg, Breyer, and Kagan).

you share your location with a communications provider it's reasonable under the Fourth Amendment for the government to secure that information without a warrant.[22] It's a doctrine that every circuit court to address location tracking has relied on to decide that no warrant is required.[23]

When that doctrine was developed in the 1970s to permit the installation of pen registers on a showing short of probable cause,[24] it reflected a very limited trade-off of privacy for more effective law enforcement. And those who wanted a greater level of privacy had effective ways to engage with society that required a relatively modest sacrifice of convenience.

But applying that same doctrine to location tracking, or to other forms of surveillance based on our online activities,[25] has much greater consequences. Because technology has become such a pervasive part of how we live our lives, continued application of the third-party doctrine essentially tells us that the price of admission to modern society is a huge slice of the protections we formerly enjoyed under the Warrant Clause.[26]

Many people seem unprepared to make that trade, which is prompting technology providers to offer products and services that reduce the amount of information they have available when government agents come calling, such as smart phones the manufacturer can't unlock and messaging

---

[22] *Id.* at 417–18, 424 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)). Unlike the circuit court cases cited above, see footnote 16, *supra*, all of which involved applications for access to historical records of the subject's location generated by the subject's mobile telephone, the issue in *Jones* arose as a result of law enforcement agents' surreptitious installation of a tracking device on the subject's car. Thus, while all of the cases potentially raised the question of whether electronic surveillance of a person's location constitutes a search within the meaning of the Fourth Amendment, that question could not be mooted in *Jones* by application of the third-party doctrine—because there could be no argument that the government had obtained information about Jones's location from any third party to whom Jones had made it available.

[23] *See* United States v. Guerrero, 768 F.3d 351, 361 (5th Cir. 2014) (holding the district court properly admitted the historical cell-site location data at trial under the third-party doctrine); Davis, 785 F.3d at 511; Graham, 824 F.3d at 427 ("Applying the third-party doctrine to the facts of this case, we hold that defendants did not have a reasonable expectation of privacy in the historical [cell-site location information]."); Carpenter, 819 F.3d at 886–87.

[24] *Smith*, 442 U.S. at 741–42.

[25] United States v. Caira, 833 F.3d 803 (7th Cir. 2016) (finding no reasonable expectation of privacy by applying the third-party doctrine to the defendant's Internet Protocol addresses).

[26] S*ee* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) ("Perhaps . . . some people may find the 'tradeoff' of privacy for convenience worthwhile . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."); In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected. In light of drastic developments in technology, the Fourth Amendment doctrine must evolve to preserve cell-phone user's reasonable expectation of privacy in cumulative cell-site-location records.").

platforms with end-to-end encryption that frustrate lawful interception orders.[27] And that in turn produces novel litigation such as the case I had last year in which the government sought to rely on the All Writs Act of 1789 to secure an order requiring Apple to break the security it markets as a feature to its customers.[28]

So as a practical matter, the cautious approach articulated in *Quon* seems ill-suited to the rapid advance and adoption of technology in our lives. Or perhaps more to the point, the increasing pace of technological advance has come with an increased pace of social change that makes it not only possible, but also critically important, for judges to assess the role this new technology plays in our lives.

Courts can of course continue to reflexively apply the third-party doctrine as if we are still living in the 1970s, and to tell people who do not want to expose their entire lives to surveillance not to interact with the world—but to what end?

If we insist that existing law is sufficient to our needs, if we jam new technology into the framework of old laws and doctrines, we end up with incoherent results. It produces such anomalies as decisions that the government can force you to unlock your smart phone by means of a subpoena if you used your fingerprint to lock it, but cannot force you to do so if you used a password instead.[29]

Such reflexive reliance on outdated doctrines is an abdication of our responsibility. In applying the law to new technology, judges must instead actively engage with that technology—both by taking the time to understand the technology itself, and by doing our best to understand the role it plays in our society right now.

We really have no choice. When the government argues that it is entitled under an existing statute like the Stored Communications Act to deploy a particular surveillance technology, we simply cannot know whether to agree or disagree without knowing exactly what the technology does, and how that mechanism fits into the existing statutory scheme.

For example, how does a Stingray work? We know the basic idea: it is

---

[27] *See* Malathi Nayak, *Finjan Sets Sights on Mobile Security Products, Licensing*, BLOOMBERG BNA (Feb. 21, 2017), https://www.bna.com/finjan-sets-sights-n57982084094/ (describing Finjan Mobile's five pending U.S. patent applications including for "technology that lets users securely access file servers through mobile devices" and "encryption-based technology" and licensees including Microsoft Corp.); Andy Greenberg, *You Can All Finally Encrypt Facebook Messenger, So Do It*, Wired (Oct. 4, 2016), https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/ (describing the rollout of end-t-end encryption on the WhatsApp and Facebook messaging platforms).

[28] In re Apple, Inc., 149 F. Supp. 3d 341, 350–51 (E.D.N.Y. 2016).

[29] *See*, *e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010) (passcode is testimonial, therefore requiring government to confer act-of-production immunity before compelling disclosure); Com. v. Baust, 89 Va. Cir. 267 (2014) (holding that a fingerprint, unlike a passcode, is not testimonial, and therefore may be compelled without a grant of immunity).

essentially a cell tower that does not put calls through. To find a suspect by locating his phone, the device plays the tech equivalent of Marco Polo: it says "Marco" by sending out a signal identifying itself as a cell tower, and every phone nearby says "Polo" by sending back a unique identifier.[30] The Stingray then sifts through all of the responses, and if they include the signature of the phone it is seeking, it starts tracking its location.[31]

At that point, we are on relatively solid ground: once we decide the appropriate legal standard for real-time location tracking—which has generated some controversy, but seems to have settled into a practice of the government showing probable cause[32]—we can determine whether to authorize the Stingray's tracking function in a given case.

But that's only the start of the inquiry. What is going on while the Stingray is playing Marco Polo? When it sends out its signal, triggering a response by all the nearby phones, is it interfering with the calls those phones might be making? Would that be an unreasonable seizure within the meaning of the Fourth Amendment?

And what about all those "Polo" responses from the phones we are not interested in, but that we have to sift through to find the target phone: is the device recording those responses, and if so, for how long is the recording kept? Does that "Polo" response include data that would constitute "dialing, routing, addressing, or signaling information" within the meaning of the pen register statute?[33]

---

[30] I am indebted to Prof. Christopher Sogohian for this analogy. *See*, *e.g.*, Police Use Stingray Tool To Intercept Cellphone Signals, *All Things Considered* (Nat'l Public Radio, June 22, 2015) (transcript available at http://www.npr.org/2015/06/22/416538036/police-use-stingray-tool-to-intercept-cell-phone-signals).

[31] *See* United States v. Lambis, 197 F. Supp. 3d 606, 609 (2016); In the Matter of the Application of the of Am. for an Order Relating to Telephones Used by Suppressed, 2015 WL 6871289, at *1-3 (N.D. Ill. Nov. 9, 2015); *see also* Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology at 2, https://www.justice.gov/opa/file/767321/download (U.S. Dep't of Justice, Sept. 3, 2015) (hereinafter, "DOJ Guidance"); Justice Department Announces Enhanced Policy for Use Of Cell-Site Simulators, DOJ 15-1084, 2015 WL 5159600 (U.S. Dep't of Justice, Sept. 3, 2015); Jason Norman, *Taking the Sting Out of the Stingray: The Dangers of Cell-Site Simulator Use and the Role of the Federal Communications Commission in Protecting Privacy & Security*, 68 FED. COMM. L.J. 139, 142 (2016); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 144–47 (2014).

[32] United States v. Lambus, No. 15-CR-382, 2017 WL 1745495, at *20, *25 (E.D.N.Y. May 4, 2017); *see*, *e.g.*, *Lambis*, 197 F. Supp. 3d at 609; In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) (denying request to use cell site simulator pursuant to pen register statute); DOJ Guidance, *supra* note 31, at 3 (requiring federal prosecutors, as a matter of policy, to seek both a search warrant and a pen register order to authorize use of a cell site simulator). *But see id*. (asserting that "the [Justice] Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute").

[33] 18 U.S.C. § 3127(3) (2012)**;** *see* DOJ Guidance, *supra* note 31, at 2 (requiring cell site simulators used by the Justice Department to be "configured as pen registers").

The answers to these questions determine whether granting the government's request would require me not only to authorize the location tracking of the target's phone, but also the installation of a pen register on the phone of every person in range of the device.[34]

Without such a detailed understanding of the technology, a judge simply cannot make an informed decision about how to apply existing laws to technology that no one had in mind when they were written.

Judicial engagement also requires a willingness to try to understand and respect the way people live their lives today. The concept of a reasonable expectation of privacy that is the touchstone of our Fourth Amendment jurisprudence has two distinct components: a person's subjective expectation, and the objective reasonableness of that expectation—that is, whether it is an expectation that society is prepared to accept as reasonable.[35]

An exploration of that standard is well beyond the scope of this talk, but no matter which of several models might be used to describe that objective element, it would have to take into account an understanding of what our society is like today—not what it was like in an earlier age.

---

[34] The Justice Department's policy statement on the matter requires prosecutors to seek an order authorizing the installation of a pen register. *See* DOJ Guidance, *supra* note 31, at 3. In doing so, the guidance memorandum implicitly assumes that the authority to be sought is to install a pen register on the target phone; however, the policy statement is wholly silent as to whether and how such authority should or could be obtained with respect to other phones whose identifying information the cell site simulator would, however briefly, collect and record.

[35] *See* Ashcroft v. al-Kidd, 563 U.S. 731, 736 (2011) ("Fourth Amendment reasonableness is predominantly an objective inquiry.") (citing Indianapolis v. Edmond, 531 U.S. 32, 47 (2006)); Brigham City, Utah v. Stuart, 547 U.S. 398, 404 (2006) ("An action is reasonable under the Fourth Amendment, regardless of the individual officer's state of mind, as long as the circumstances, viewed *objectively,* justify [the] action.") (Internal quotations and citation omitted). In 2005, when courts first addressed the standard for granting law enforcement authorization to conduct prospective location tracking of a subject's mobile telephone, Federal Rule of Criminal Procedure 41 (governing the issuance of search and seizure warrants) made no mention of tracking devices (a broad term statutorily defined in 18 U.S.C § 3117 (2012)). As a result, the courts were divided as to whether, instead of making the showing of probable cause required under Rule 41, law enforcement agents seeking to conduct location tracking of a subject's telephone might need only satisfy the lesser standards of either the pen register statute, 18 U.S.C. § 3123 (2012) (requiring only the applicant's certification of relevance to a criminal investigation), or the Stored Communications Act, 18 U.S.C. § 2703(d) (2012) (requiring a showing of "specific and articulable facts" showing relevance and materiality to a criminal investigation). *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (requiring a showing of probable cause); *In re Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (requiring a showing of specific and articulable facts). As of December 1, 2006, however, Rule 41 was amended to include procedures for issuing a tracking device warrant. *See* FED. R. CRIM. P. 41(f) & advisory committee notes to 2006 amendments. Although that amendment did not explicitly state that electronic surveillance of a subject's telephone could only be authorized under the new procedures set forth in Rule 41, the Justice Department has apparently decided since the amendment's promulgation to stop litigating the issue.

For that reason, where a new surveillance method is not regulated by a specific statute, judges considering whether using the technique requires a warrant must do their best to assess how people view the role of different technologies in our lives.

I don't mean to suggest that that's easy to do to, or that there is any single answer out there waiting to be discovered. As a society we might conclude, for example, that it *is* reasonable to expect that the government needs a warrant to get location tracking records from your cell-phone carrier, but that it is *not* reasonable to expect that the government needs a warrant to get that same kind of information if you provide it to Uber when you need a ride.

But how do we take the measure of such objective societal preferences? One very useful tool in that context is the kind of empirical research conducted by a team of scholars—including, I am proud to say, my former law clerk, Professor Christine Scott-Hayward at Cal State—into the specific kinds of privacy interests that people in our society think should or should not be protected.[36]

That kind of empirical research isn't the whole answer, but it should be an important part of how we determine how best to align our laws to our values in the digital age.

Consider again those circuit court cases on whether the Fourth Amendment requires a warrant to get historical location records.[37]

The problem isn't simply that by applying existing third-party doctrine the courts applied the societal expectations of privacy of the 1970s to modern technological reality. It's also that the gap between those two things grows greater by the day.

As Verizon's General Counsel recently observed, all four of those cases involved calls or texts made in 2010 or 2011.[38] But since then, the number of devices in use, and the amount and precision of location information they generate, has increased so exponentially that we must ask: "[A]t what point does the volume and precision of the … information conveyed . . . [by] mobile devices differ so materially from the dialed numbers of 1970[] . . . phones that our expectation of privacy in that

---

[36] *See* Christine S. Scott-Hayward, Henry F. Fradella, & Ryan G. Fischer, "*Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*," 43 AM. J. CRIM. L. 19, 52, 56 (2015) (finding that participants in a survey of 1,198 people generally "displayed a strong desire for privacy when it came to their online transactions and communications").

[37] *See* footnote 16.

[38] *See* Craig Silliman, *Technology and Shifting Privacy Expectations (Perspective),* BLOOMBERG LAW: BIGLAW BUSINESS (Oct. 7, 2016), https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective ("[I]n all four cases, the location information was gathered by law enforcement from wireless carriers back in 2010 and early 2011 based on telephone calls (and, in one case, text messages). None of the four cases involved location information generated when a device was used to access data . . . .").

information changes, as well?"[39]

What I am suggesting is merely that in the face of a growing gap between the technologies our existing laws were designed to regulate and those being deployed today, judges have to get down in the weeds more than used to be necessary, to learn more both about technology itself and about its place in our society. We can't wait for those answers to reveal themselves over time.

What I am decidedly *not* suggesting is that judges should have a bias against authorizing new forms of technology-based surveillance.

But I am suggesting that we can't take it for granted that just because a technology exists, there must be some way for a court to authorize its use in the service of law enforcement. Federal courts have limited power, and before we take it upon ourselves to authorize an investigative technique, we need to figure out what gives us the authority to do so.

If the government wants to rely on a statute to authorize a new surveillance technology, show me that Congress has actually made that decision. That's a showing that becomes ever more difficult as technology advances beyond anything the drafters of existing statutes could have contemplated.

If a specific statute doesn't apply and warrantless use of the technology is unreasonable, show me that there's probable cause to issue a warrant—and that the kind of warrant you want is within the scope of Rule 41.[40]

If the government can't do either of those things, it can try to persuade me that the All Writs Act is sufficient authority[41]—though as I imagine we'll discuss in the first panel, I don't necessarily see that statute as a backstop to make sure that the government can always accomplish its investigative goals.[42]

The engagement with technology I'm suggesting, the willingness to reconsider old doctrines in light of changing societal expectations, and the focus on just where we get the authority to do as the government asks—all of that will sometimes frustrate an important investigation, as it did in *Riley* in 2014, when the Supreme Court recognized that the search incident to arrest doctrine could no longer justify warrantless searches of

---

[39] *Id.*

[40] *See* FED. R. CRIM. P. 41(c)(1)-(4) (defining the kinds of property that are subject to search and seizure with a warrant).

[41] *See* 28 U.S.C. § 1651(a) (2012) (noting that all courts can issue all writs "necessary or appropriate in the aid of their respective jurisdictions and agreeable to the usages and principles of law[]").

[42] *See, e.g.*, In re Apple, Inc., 149 F. Supp. 3d 341, 372, 375–76 (E.D.N.Y. 2016) (finding that the All Writs Act is not sufficient authority to "override individual autonomy" in all circumstances).

smartphones.[43]

It may even cripple a whole swath of investigations until Congress steps in to strike a new balance between privacy and law-enforcement interests. That may be a very long wait, but that can't deter us.

I do not say that because I lack sympathy for the difficult job that law-enforcement agencies have in fulfilling their critical mission or an appreciation of the societal cost of hampering an investigation.

Having spent over a decade as a prosecutor, it's actually quite the opposite, and some of my rulings on surveillance technology have unquestionably run contrary to my policy preferences. Rather, I say it because I have more concern for our democratic institutions.

If Congress cedes the field, the judiciary is left with two choices, neither of them particularly consonant with a robust democracy.

We can continue to rely on outdated doctrines, but that essentially leaves it to the executive branch to balance its law-enforcement needs against our privacy interests.

Law enforcement can be trusted to do many things, and to do them well—but their mission requires intrusion into the lives of people about whom they know little or nothing. It is asking too much to ask them to fulfill that mission while also serving as the exclusive guardians of our privacy.

Another option is for the judiciary to strike what it believes to be a more appropriate balance between competing legitimate interests. Judges will try to be fair, but we haven't the perspective or the institutional accountability to be striking the balance between law enforcement and privacy.

I say instead that judges have a responsibility to incentivize legislators to do their job. We shouldn't look for opportunities to say no to law enforcement, but we should insist that Congress give law enforcement and judges alike the tools to do our jobs.

And if Congress fails to do so, judges should shed light on the problem by giving a public account of their reasons for saying no to law enforcement—even in the context of ex parte warrant applications—so that the public can see the consequences of legislative inaction and demand better from those most accountable to them.

A bias against granting law enforcement the authority they seek to deploy new forms of surveillance technology is every bit as pernicious as a bias in favor of granting such requests simply to avoid frustrating an investigation. Either choice necessarily short-changes an important value—security or privacy.

---

[43] Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (holding that because modern cell phones contain a substantial amount of personal information, the police must obtain a warrant before searching a cell phone seized incident to an arrest).

The point is to avoid going on auto-pilot. Even in the age of the self-driving car, courts must keep someone at the wheel, because the people who wrote our outdated statutes couldn't see the dangers approaching on the road we're now traveling down so very quickly.

Thank you very much.