THE YALE LAW JOURNAL FORUM
APRIL 27, 2016

The Fourth Amendment in the Information Age

Robert S. Litt

To badly mangle Marx, a specter is haunting Fourth Amendment law—the specter of technological change. In a number of recent cases, in a number of different contexts, courts have questioned whether existing Fourth Amendment doctrine, developed in an analog age, is able to deal effectively with digital technologies. Justice Sotomayor, for example, wrote in her concurrence in *United States v. Jones*,[1] a case involving a GPS tracking device placed on a car, that "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age."[2] And in *Riley v. California*,[3] the Chief Justice more colorfully rejected the government's argument that a search of a cell phone was equivalent to a search of a wallet:

> 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. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.[4]

I intend to discuss the application of the Fourth Amendment in the information age, and I want to start with two important caveats.

First, I am not proposing a comprehensive theory of Fourth Amendment law. Rather, I want to offer some tentative observations that might be explored in shaping a productive response to the challenges that modern technology

1. 132 S. Ct. 945 (2012).
2. *Id.* at 957 (Sotomayor, J., concurring).
3. 134 S. Ct. 2473 (2014).
4. *Id.* at 2488-89.

creates for existing legal doctrine. In particular, I would like to suggest that the concept of "reasonable expectation of privacy" as a kind of gatekeeper for Fourth Amendment analysis should be revisited.

Second, these thoughts are not informed by deep research into the intent of the Framers, or close analysis of case law or academic scholarship. Rather, they derive from almost forty years of experience in law enforcement and intelligence. But, despite Justice Oliver Wendell Holmes's adage about the life of the law, I hope that they have some foundation in logic as well.[5]

I want to approach this complicated issue by focusing on two intelligence activities that have been the subject of recent litigation, partly because they will help illuminate the Fourth Amendment issue, and partly because I know them well. The first is the formerly secret, but now well-known, bulk telephone metadata collection program conducted under the business records provision of the Foreign Intelligence Surveillance Act (FISA).[6] Although this program has now ended, it provides a good starting point for this discussion.

Telephone metadata is information *about* a telephone call such as the number calling, the number being called, the date, time and duration of the call, and so on—the same sort of information that those of us old enough to remember long-distance toll calls used to get each month on our itemized telephone bills. Metadata does not include the content of the calls or the identity of the callers.

For several years, and with judicial authorization, the NSA collected metadata in bulk about U.S. phone calls from telephone companies for counterterrorism purposes. The metadata was kept in secure databases. It could only be accessed by a few specially trained NSA analysts, and then only to identify telephone numbers in contact with so-called "seed" numbers as to which there was a reasonable and articulable suspicion of an association with terrorism—such as, for example, a number used by a suspected terrorist.[7] The standard of "reasonable articulable suspicion" is derived from *Terry v. Ohio*,[8] which held that police stops that did not amount to an arrest could be made on reasonable suspicion. Although this program was approved numerous times by

---

5. *See* OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (1881) ("The life of the law has not been logic: it has been experience.").

6. 50 U.S.C. § 1861 (2012).

7. *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, PRIVACY & C.L. OVERSIGHT BOARD 24-28 (Jan. 23, 2014), http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf [http://perma.cc/FLV8-YBPW].

8. 392 U.S. 1, 37 (1968). Since *Terry*, the Supreme Court has frequently invoked the "reasonable articulable suspicion" standard in the context of a *Terry* stop. *See, e.g.*, United States v. Place, 462 U.S. 696, 702 (1983).

judges of the Foreign Intelligence Surveillance Court, the Second Circuit has held that it was not authorized by FISA's business records provision.[9]

Here, however, I want to focus on the litigation in the District of Columbia in which Judge Leon enjoined the bulk collection of metadata on the ground that it violated the Fourth Amendment.[10] The plaintiffs' constitutional challenge in that case faced a substantial hurdle in the form of *Smith v. Maryland*,[11] a 1979 Supreme Court decision holding that obtaining telephone metadata is not a search for Fourth Amendment purposes because people lack a reasonable expectation of privacy in information they voluntarily expose to the telephone company. If the so-called "third-party doctrine" of *Smith* governed this case, then there was no search at all, and hence no violation of the Fourth Amendment.

In his lengthy and somewhat colorful opinion, Judge Leon tried to distinguish the bulk collection program from *Smith* because the metadata in the case before him was collected about millions of people rather than about a single individual; because it was collected on a rolling basis and covered several years' worth of metadata, rather than just a few days; and because, in the modern age, cellphones are ubiquitous and contain vast amounts of information. According to Judge Leon, metadata "that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[12] Judge Leon went on to hold that the electronic search of this metadata without a warrant likely violated the Fourth Amendment.[13]

I do not think that Judge Leon's efforts to distinguish *Smith* were successful. First, while Judge Leon is certainly right that metadata can be very revealing of personal activities, there is nothing new about that insight. Justice Stewart dissented from the decision in *Smith* itself in part because he recognized that metadata "easily could . . . reveal the most intimate details of a person's life."[14] The point of *Smith* was not that metadata is innocuous, but that you have chosen to reveal it to a third party. To use an analogy, if you give a document to a third party, you have lost your expectation of privacy in that document, whether it is a laundry ticket or a confession of mortal sin. Moreover, the fact that cell phones today contain a lot of information beyond metadata does not seem relevant when the government did not actually search or collect any of that other information.

---

9. ACLU v. Clapper, 785 F.3d 787, 792 (2d Cir. 2015).

10. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

11. 442 U.S. 735, 742-43 (1979).

12. *Klayman*, 957 F. Supp. 2d at 36.

13. *Id.* at 42.

14. *Smith*, 442 U.S. at 748.

It is also true that the government collected lots of metadata about lots of people under this program. But it is a well-established principle that one person cannot assert the Fourth Amendment rights of someone else. The Court has long held that "Fourth Amendment rights are personal rights which . . . may not be vicariously asserted."[15] *My* right to privacy is not violated when the government collects *your* metadata.

Finally, I find it hard to understand the alchemy by which information that you choose to disclose to a third party develops an expectation of privacy because you have chosen to disclose a lot of that information. That seems counter-intuitive to say the least. For all of these reasons, if you accept *Smith*'s holding that there was no expectation of privacy in the telephone metadata in that case because it had been voluntarily exposed to a third party, you can't conclude there was an expectation of privacy in the metadata in this case.

I am not alone in thinking that Judge Leon did not correctly apply existing Fourth Amendment doctrine. Every other judge to rule on the constitutionality of the bulk metadata program has disagreed with him. Most recently, his injunction was immediately stayed by the D.C. Circuit,[16] and in an opinion concurring in the denial of rehearing en banc, Judge Kavanaugh pointedly noted that *Smith* remained controlling.[17] Although I think Judge Leon's dismissal of *Smith* was wrong, it is nevertheless worth considering his analytic framework.

Judge Leon's decision, and the arguments of the parties, followed traditional Fourth Amendment doctrine. First, he considered whether or not there was a "search" for Fourth Amendment purposes, by determining whether plaintiffs had a reasonable expectation of privacy in the information obtained by the government, including whether any expectation of privacy was defeated by the fact that they had voluntarily disclosed the information to the telephone companies. After finding that plaintiffs had a reasonable expectation of privacy in the metadata, he went on to analyze whether the search of that data was "reasonable" under the Fourth Amendment, using the well-established rubric that warrantless searches are unreasonable unless they fall within one of a number of established exceptions. That's the way cases like this have been approached since *Katz v. United States,*[18] but I'm not sure that the framework is entirely satisfying in the context of digital data.

---

15. Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)).

16. Klayman v. Obama, No. 15-5307, 2015 WL 9010330, at *1 (D.C. Cir. Nov. 16, 2015).

17. Klayman v. Obama, 805 F.3d 1148, 1149 (D.C. Cir. 2015).

18. 389 U.S. 347 (1967).

To help illustrate why, let's turn to another factual scenario: the recent case of *Jewel v. National Security Agency*,[19] in which plaintiffs challenged the government's surveillance of internet communications under Section 702 of the Foreign Intelligence Surveillance Act.[20] Section 702 authorizes the government to collect foreign intelligence information, without an individualized warrant or probable cause, by targeting non-U.S. persons outside the United States. Persons inside the United States, or Americans anywhere in the world, can only be targeted with probable cause.

However, plaintiffs in *Jewel* claimed that the warrantless collection of Internet communications even of foreigners violated the Fourth Amendment rights of Americans, because it involved the search of communications of U.S. persons as well as the foreign targets.[21] According to the plaintiffs' motion for partial summary judgment, the government accomplishes one type of collection under Section 702—so-called "upstream" collection of emails—by first copying all internet traffic flowing across certain switches and storing it briefly; then electronically scanning the contents of the communications as well as the metadata to determine which communications contain certain "selectors" such as email addresses that have been determined to be likely to produce foreign intelligence; and finally pulling out those communications and ignoring the rest.[22] The plaintiffs allege that this process constitutes an unconstitutional search of everyone's email communications and that, just as the Supreme Court in *Katz* recognized that people have a reasonable expectation of privacy in telephone communications that could not be invaded without a warrant, this electronic scanning constitutes an invasion of people's reasonable expectation of privacy in Internet communications.[23]

The description set out above is drawn from the plaintiffs' allegations. I am not confirming or denying their accuracy, or indeed saying anything about the means by which the government collects Internet communications. In fact, the court in *Jewel* never reached the merits of the Fourth Amendment argument, holding that the plaintiffs lacked standing because they could not establish that *their* communications were actually searched in this manner.[24] Assume,

19. *See* Motion for Partial Summary Judgment, Jewel v. Nat'l Sec. Agency, No. 4:08-cv-04373-JSW (N.D. Cal. July 25, 2014), ECF No. 261. Similar allegations were raised in another case. Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., No. 1:15-CV-662, 2015 WL 6460364 (D. Md. Oct. 23, 2015), appeal pending, Dkt. No. 15-2560 (4th Cir. Dec. 18, 2015).

20. 50 U.S.C. § 1881.

21. Motion for Partial Summary Judgment at 1, *Jewel*, No. 4:08-cv-04373-JSW, ECF No. 261.

22. *Id.* at 6-9.

23. *Id.* at 17.

24. *See* Jewel v. Nat'l Sec. Agency, 810 F.3d 622, 625 (9th Cir. 2015) (discussing the district court's dismissal of the plaintiffs' Fourth Amendment internet surveillance claim for lack of standing, and dismissing the plaintiffs' appeal for lack of jurisdiction).

however, that the plaintiffs' description is accurate, and consider how the Fourth Amendment should apply to this hypothetical scenario.

The *Jewel* case involved the content of communications rather than metadata. It is significant that the government did not argue in *Jewel* that the plaintiffs had no reasonable expectation of privacy in the content of the communications even though that content was exposed to a third party, although the government did advance other arguments that there was no search for purposes of the Fourth Amendment. Yet, in important respects, this hypothetical Internet collection program looks like the real bulk metadata program. In both situations, the government is obtaining large quantities of digital data and scanning that data electronically using specific selectors such as telephone numbers and email addresses to look for specific relevant information that is found in only a small percentage of communications. In both cases, no human being ever sees the vast majority of information that never passes through that filter. Yet because our analytical framework makes application of Fourth Amendment protections turn upon whether there is a "reasonable expectation of privacy," and thus distinguishes metadata from content, one of these might be a search subject to the Fourth Amendment, and the other might not be.

This strikes me as both unrealistic and undesirable. I suggest that—at least in the context of government acquisition of digital data—we should think about eliminating the separate inquiry into whether there was a "reasonable expectation of privacy" as a gatekeeper for Fourth Amendment analysis. In an era in which huge amounts of data are flowing across the Internet; in which people expose previously unimagined quantities and kinds of information through social media; in which private companies monetize information derived from search requests and GPS location; and in which our cars, dishwashers, and even light bulbs are connected to the Internet, trying to parse out the information in which we do and do not have a reasonable expectation of privacy strikes me as a difficult and sterile task of line-drawing. Rather, we should simply accept that any acquisition of digital information by the Government implicates Fourth Amendment interests.

After all, the concept of a "reasonable expectation of privacy" as a talisman of Fourth Amendment protection is not found in the text of the Fourth Amendment itself, which says merely that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[25] It was only in 1967, in *Katz*, that the Supreme Court defined a search as the invasion of a "reasonable expectation of privacy."[26] *Katz* revisited *Olmstead v. United States*[27] after 40

25. U.S. CONST. amend. IV.

26. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

years; the accelerating pace of modern technological change suggests to me that fifty years is not too soon to revisit *Katz*. My proposal is that the law should focus on determining what is unreasonable rather than on what is a search.

Of course, this approach would mean that courts would assess the reasonableness of government activity in cases where today they simply find that the Fourth Amendment does not apply. But before the privacy advocates start popping the champagne corks, I want to make clear that I believe the inquiry into reasonableness should focus on actual harms, rather than theoretical ones. It should involve a realistic assessment of privacy rights and governmental needs, one that looks at not only the act of collection but also at the use that is made of the data and the processes that exist to regulate that use. Just as the changing technological environment should affect how we view the interests of individuals, it should affect how we evaluate the governmental interests at stake.

Let's return to the metadata program. Every bit of the data that the government collected in the bulk metadata program was data that the telephone companies collected and retained for their own purposes. In fact, the government got the data from the telephone companies, not individuals. Once the government got the data, it remained unseen and unknown unless it proved to be connected to a terrorist "seed" number, and, as noted above, only an infinitesimal fraction of the data was ever seen by any human being.[28] And while Congress last summer ordered the bulk collection program stopped, it authorized a mechanism allowing the government to get the exact same information—phone numbers in contact with potential terrorist phone numbers—directly from the telephone companies, based on the exact same showing of a reasonable articulable suspicion of a connection to terrorism.[29]

In the bulk collection program, digital data was moved from one set of computer servers owned by telephone companies to another set of computer servers owned by the government. No person in the government ever saw this data, except under circumstances that Congress, at least, appears to have agreed are reasonable. What is the actual harm to an individual for constitutional purposes if information about her telephone calls sits on two computers instead of one? Indeed, despite a great deal of overheated rhetoric about "mass surveillance," the criticism of the bulk metadata program invariably focused on speculation about what the government *could* do with bulk metadata, rather than what it *did* do, and on the chilling effect that hypothetical activity might produce. There's no question that one *could* use

---

27. 277 U.S. 438 (1928).

28. *See supra* note 22 and accompanying text.

29. USA FREEDOM Act, Pub. L. No. 114-32, 129 Stat. 268 (2015).

bulk telephone metadata to do a lot of big data analysis and find out a lot of personal information. But that's not what this program ever did.

Similarly, in the hypothetical Internet case, if the government electronically scans electronic communications, even the content of those communications, to identify those that it is lawfully entitled to collect, and no one ever sees a non-responsive communication, or even knows that it exists, where is the actual harm? Indeed, while I am no expert, I believe that this scanning is similar to what private companies and government agencies already do on their networks for the purposes of identifying and stopping malware.[30]

In both of these situations, while government computers may electronically touch information about you contained in a digital database, the government actually knows nothing more about you than it did before—unless and until it has a valid purpose for learning that information. Fourth Amendment analysis should be based on that reality, rather than on hypotheticals.

Of course, the nature of the information the government collects, and the privacy interests that attach to that data, will still have an important role to play in assessing reasonableness. To this extent, I agree with those who criticize the broad proposition that *any* information that is disclosed to third parties is outside the protection of the Fourth Amendment. Courts can appropriately take into account whether information is content or non-content information, whether it is publicly disclosed through social media or is stored in the equivalent of the cloud, or whether its exposure is "voluntary" only in the most technical sense because of the demands of modern technology. But we should not be viewing this analysis of privacy interests as an on/off switch to determine whether or not the Fourth Amendment applies, as today's third-party doctrine does, but as more of a rheostat to identify the degree of protection that would ensure that the collection and use of that data is reasonable.

So the flip-side of my argument is that even where there is a substantial privacy interest in digital data, we should not default immediately to the rule that a warrant is required unless we can fit the collection of such data into one of the twentieth-century exceptions to the warrant requirement. Instead, at least while the courts are feeling their way through the new legal challenges of the digital age, they should look at all such activity through the prism of a reasonableness inquiry that takes into account not only the nature of the data the government is collecting, but the use the government is going to make of

30. Memorandum from the Office of Legal Counsel to the President 3 (Jan. 9, 2009), http://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues.pdf [http://perma.cc/B9DL-AJEF] ("EINSTEIN 2.0 intrusion-detection sensors will observe in near-real time the packet header and packet content of all incoming and outgoing Internet traffic of Federal Systems . . . for the 'signatures' of malicious computer code used to gain access to or to exploit Federal Systems.").

that data. And just as the assessment of privacy interests should be concerned with real harms rather than theoretical ones, the assessment of government use must take account of the very real government interests at stake. Protection of the public is one of the most important functions of government, and the kinds of digital data we are talking about can be of immense benefit to both law enforcement and the national security community, not to mention the potential victims of terrorist attacks or other crimes—if we can be comfortable with the manner in which the government collects and uses that data.

Turning back to my two examples, I noted in my description of the bulk metadata program that the data was used only to help determine, under carefully controlled and supervised conditions, whether a U.S. telephone number had a connection with a number associated with terrorism. There has been a lot of debate about the utility of this program, with people arguing that the program, by itself, never stopped a terrorist attack. But that is the wrong way to assess the value of an intelligence program; you do not get rid of a fire insurance policy that has never paid off because your house has never burned down. The bulk metadata program was developed to fill a real gap that was identified after the 9/11 attacks as one of the factors contributing to our failure to prevent those attacks. And in light of the ongoing efforts of terrorists to recruit Westerners to conduct attacks, and recent horrific events in Paris and Brussels, it's not hard to see how the information obtained from this program—information about potential contacts between terrorists abroad and people in the US—could be useful. In other words, the bulk metadata program was narrowly focused on a legitimate counterterrorism purpose.

Similarly, Section 702, the Internet program, was specifically authorized by Congress to allow the collection of information for important foreign intelligence purposes, including counterterrorism, by targeting foreigners outside the United States,[31] and is one of our most valuable intelligence collection programs. Moreover, while I do not have the technical knowledge necessary to speak authoritatively on this point and my analysis is therefore purely hypothetical, I find it at least plausible that there would often be no effective way to collect targeted communications from the Internet without scanning other communications as well. So in both the telephone metadata and the Internet cases, one can make a strong case that the use of the data was reasonable.

Our legal framework already accepts the concept that restrictions on the use of data can be an important way to protect privacy interests. Congress has required that a variety of government activity authorized under the Foreign Intelligence Surveillance Act be conducted pursuant to so-called "minimization procedures," which are designed, among other things, to limit the retention

31. 50 U.S.C. § 1881(a) (2012).

and dissemination of private information acquired through surveillance.[32] Executive Order 12,333 imposes a similar requirement for all intelligence activities collecting information about United States persons.[33] Minimization procedures generally identify permitted uses of information the government collects, including sharing of information between agencies when appropriate, and provide rules and procedures to ensure that those limitations are adhered to. They are a form of use restriction that helps ensure that data collection is consistent with the protection of privacy.

And this is similar to how privacy is protected today in the private sector. A company's privacy policies typically tell you that the company will keep only certain kinds of information about you, and make use of that information only for certain specified purposes. In other words, your privacy is protected through use restrictions. Corporate privacy policies are not universally applauded, but the principal criticism is that they are frequently contracts of adhesion, not that use restrictions are inadequate to protect privacy. So, in assessing the reasonableness of the government's collection of data, courts should look at the back end—whether the retention, use, and dissemination are reasonable—as well as the front end—whether the collection itself is reasonable in light of its purpose.

Let me now address several questions that this approach raises. One objection is obvious: once the government gets hold of information, how can we be sure that it is only used appropriately? This concern is both justified and substantial. We care more about government collection of data than private collection because of the government's power to make use of data in ways that adversely affect us and could infringe upon our privacy and liberties. We must always be alert to the possibility of government overreach, and attentive to ways to prevent it. As President Obama said, "Given the unique power of the state, it is not enough for leaders to say: Trust us: we won't abuse the data we collect . . . . Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power, it depends on the law to constrain those in power."[34] Three related concepts can provide the necessary assurance: oversight, technology, and transparency.

Oversight—and accountability through the mechanisms of oversight—is a critical way to ensure compliance with reasonable restrictions on collection and use. At least in the area of intelligence, we have robust oversight, involving a variety of agencies and offices, congressional committees, and, in the case of

---

32. *E.g.*, 50 U.S.C. § 1801(h) (2012).

33. United States Intelligence Activities, Exec. Order No. 12,333, § 2.3, 3 C.F.R. 200, 211 (1981), *amended by* Exec. Order No. 13,284, 3 C.F.R. 161 (2003); Exec. Order No. 13,355, 3 C.F.R. 218 (2004); and Exec. Order No. 13,470, 3 C.F.R. 218 (2008).

34. Remarks on United States Signals Intelligence and Electronic Surveillance, 2014 DAILY COMP. PRES. DOC. 5 (Jan. 17, 2014).

activities under FISA, the courts. In addition, the independent Privacy and Civil Liberties Oversight Board provides both oversight and guidance on counterterrorism policies. This multi-level oversight should play a role in any assessment of the reasonableness of data collection. The more people who have eyes on a particular activity, the less likely it is to be abused, and the more likely it is that privacy protections will be observed.

Technology is a critical adjunct to oversight. When people talk about technology in the context of surveillance, they tend to talk either about the awful ways in which technology enables the government to spy on us, or about the ways in which we can use technology to protect ourselves from that awful government spying. But technology can play an important role as well in protecting privacy while enabling lawful collection of information by the government. I mentioned above that the bulk telephone metadata was kept in special secure databases, with access limited to only a few people with special training. Software also tracked every query that was made of the database so that the queries could be audited for compliance. I am no computer scientist, but I have to think that there are additional ways that we could use technology to buttress our oversight mechanisms. I've been told, for example, that there are systems that permit queries of data in such a fashion that the person making the query never sees the data but sees only the response, and that the holder of the data doesn't see the actual query or the response but is able to ascertain that the query is authorized. Surely our extraordinarily capable technologists can develop other techniques to provide assurance that data the government collects is being used only as appropriate.

The fact is, in the context of the activities I discussed above—the bulk metadata program and collection under Section 702 of FISA—the combination of oversight mechanisms and technology worked effectively. In all the information that has come out about these two programs, there has not been a single instance of intentional violation of the law or other deliberate abuse. There were unquestionably mistakes made, which is not surprising given the complexity of the systems involved, and they were discovered, reported, and remedied. But there is a difference between a mistake and an abuse: to quote Justice Holmes again, "[e]ven a dog distinguishes between being stumbled over and being kicked."[35]

Where we fell short was on the third leg of the stool, transparency. There would have been less damage to the Intelligence Community from the disclosures of the last couple of years had we been more forthcoming about our activities before those leaks. Obviously, intelligence activities have to be conducted with some degree of secrecy, and the same is true of some law enforcement activities. Specific methods and targets of surveillance have to be protected. But if we don't discuss what we are doing and how we are

35. HOLMES, *supra* note 5, at 3.

regulating it even in general terms, we cede the field to those who are hostile to intelligence activities.

Our actions in the last two and a half years, including the DNI's promulgation of principles of transparency to govern the Intelligence Community, demonstrate that we are internalizing this lesson. And the availability of public information about intelligence programs, along with the extent of oversight and the nature of technological controls, should factor into the analysis of whether those activities are reasonable. The more transparent we can be about collection activity and its oversight, the more confident the public can be that the appropriate limits on that activity will be respected. And the more the public understands and has confidence in what our law enforcement and intelligence agencies are actually doing, the less likely it is to be "chilled" by fears about what they *could* be doing.

A second question is how broadly I would extend my suggested framework. In these remarks I have suggested that it apply to "digital data." Generally speaking, this is information, of any nature, that is transmitted or stored electronically. My discussion of the Fourth Amendment is limited to digital data because it most starkly illustrates the problems technology poses for existing doctrine. However, I have not considered whether my suggestions could or should serve as the basis for a broader Fourth Amendment jurisprudence.

Third, the idea of balancing the invasion of privacy and the government's purpose looks very much like the existing test used by courts to determine whether a warrantless search is "reasonable" under the Fourth Amendment. As the Supreme Court said in *Maryland v. King*,[36] "[a]pplication of 'traditional standards of reasonableness' requires a court to weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'"[37] In particular, the courts have upheld much warrantless foreign intelligence collection activity under the doctrine of "special needs." To that extent, I am proposing nothing new.

What I have suggested, however, is that—at least in the area of government collection of digital data—we eliminate the preliminary analysis of whether someone has a reasonable expectation of privacy in the data and proceed directly to the issue of whether the collection is reasonable; that the privacy side of that analysis should be focused on concrete rather than theoretical invasions of privacy; and that courts in evaluating reasonableness should look at the entirety of the government's activity, including the "back end" use, retention restrictions, and the degree of transparency, not just the "front end" activity of collection.

---

36. 133 S. Ct. 1958 (2013).

37. *Id.* at 1970 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

This approach would present a challenge for our legal system. We would be abandoning a set of fixed rules and a body of case law that have guided law enforcement and the courts for half a century, in favor of a less predictable analysis. But it is time we stopped trying to hammer twenty-first century pegs into mid-twentieth-century holes. It may be that over time a new series of rules would emerge to provide more certainty. But it is equally likely that technology will continue to change so rapidly that the legal system will constantly be struggling to catch up. Application of the general standard of reasonableness to judge the legality of government collection of digital data is a better way to hit that constantly moving target than trying to define more specific rules that may promptly be overtaken by new technologies.

This leads me to one final important point, which is to emphasize that Congress, rather than the judiciary, is in the best position to articulate the rules that should apply to collection activities of the government. A decision by Congress to authorize certain activities under certain controls, made after discussion and debate, should be a strong factor in support of the reasonableness of those activities. Congress is going to have a number of opportunities to address these issues. For example, Section 702 expires at the end of 2017, and there are continued efforts to modernize the Stored Communications Act.[38] It may be too much to hope that in the current political environment, Congress could have a dispassionate and comprehensive discussion about such weighty issues, but the Executive Branch would welcome such a discussion.

These are important issues. They implicate, on the one hand, the privacy and civil liberties of Americans and of others around the world, and, on the other hand, the safety and security of Americans and of others around the world. It is important that we get them right. I hope that the thoughts expressed here can be viewed as a constructive contribution to this effort.

Robert S. Litt is General Counsel, Office of the Director of National Intelligence. *This Essay is adapted from a speech delivered to the American Bar Association's Standing Committee on Law and National Security on February 16, 2016. The views above are entirely the author's and do not reflect the position of the United States government, the Obama Administration, the Intelligence Community, or even the Office of General Counsel for the Office of the Director of National Intelligence.*

Preferred Citation: Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J. F. 8 (2016), http://www.yalelawjournal.org/forum/fourth-amendment-information-age.

38. 18 U.S.C. §§ 2701-2712 (2012).