



2016

After Snowden: Regulating Technology-Aided Surveillance in the Digital Age


David Cole

Georgetown University Law Center, cole@law.georgetown.edu

This paper can be downloaded free of charge from:
<https://scholarship.law.georgetown.edu/facpub/1905>

44 Cap. U. L. Rev. 677 (2016)

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Internet Law Commons](#), [National Security Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

AFTER SNOWDEN: REGULATING TECHNOLOGY-AIDED SURVEILLANCE IN THE DIGITAL AGE

DAVID D. COLE*

Imagine a state that compels its citizens to inform it at all times of where they are, who they are with, what they are doing, who they are talking to, how they spend their time and money, and even what they are interested in. None of us would want to live there. Human rights groups would condemn the state for denying the most basic elements of human dignity and freedom. Student groups would call for boycotts to show solidarity. We would pity the offending state's citizens for their inability to enjoy the rights and privileges we know to be essential to a liberal democracy.

The reality, of course, is that this is our state—with one minor wrinkle. The United States does not directly compel us to share all of the above intimate information with it. Instead, it relies on private sector companies to collect it all, and then it takes it from them at will.¹ We “consent” to share all of this private information with the companies that connect us to the intensely hyperlinked world in which we now live through our smart phones, tablets, and personal computers.² Our cell phones constantly apprise the phone company of where we are, as well as with whom we are talking or texting.³ When we send emails, we share the addressing information, subject line, and content with the internet service provider.⁴ When we search the web or read something online, we reveal our interests

Copyright © 2016, David D. Cole.

* Hon. George J. Mitchell Professor in Law and Public Policy, Georgetown Law. I delivered a version of this essay at the John E. Sullivan Lecture at Capital University Law School in 2014. Parts of this essay are also developed and adapted from David Cole, *Is Privacy Obsolete?*, NATION (Apr. 6, 2015), <http://www.thenation.com/article/privacy-20-surveillance-digital-age>, and David Cole, *Must Counterterrorism Cancel Democracy?*, N.Y. REV. BOOKS (Jan. 8, 2015), <http://www.nybooks.com/articles/2015/01/08/must-counterterrorism-cancel-democracy>.

¹ See, e.g., Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

² See *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

³ See Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

⁴ See, e.g., *What Data Does Google Collect?*, GOOGLE, <https://privacy.google.com/data-we-collect.html> (last visited Mar. 27, 2016).

to the company that runs the search engine.⁵ When we purchase anything with a credit card, we pass on that information to the credit card company.⁶ In short, we share virtually everything about our lives—much of it intensely personal—with some private company. It is recorded in an easily collected, stored, and analyzed digital form. We do so “consensually,” at least in theory, because we could choose to live without using the forms of communication that dominate modern existence. But to do so would require cutting oneself off from most of the world as well. That is a high price for privacy.

We do not affirmatively consent to share this information with the government. But a rule announced back in the analog age by the Supreme Court of the United States holds that what we share with third parties is no longer private, at least when the government obtains information from the third party.⁷ Thus, if the Federal Bureau of Investigation (FBI) wants to find out who we have been calling and where we have been, it can approach the phone company and demand our phone data and location records. If it wants to know what websites we have been visiting, it can demand those records from our internet service provider. If it wants to know what we have been thinking about, it can obtain our search history from Google. Under the Court’s third-party disclosure rule, we have no privacy interest in any of this information. As a constitutional matter, the government can obtain it without any basis for suspecting us of wrongdoing and without a judicial warrant.⁸

The third party disclosure rule is just one way in which privacy protections are threatened in the digital age. The border search exception⁹

⁵ *Id.*

⁶ See Charles Duhigg, *What Does Your Credit Card Company Know About You?*, N.Y. TIMES MAG. (May 12, 2009), <http://www.nytimes.com/2009/05/17/magazine/17credit-t.html>.

⁷ See *United States v. Miller*, 425 U.S. 435, 443 (1976).

This Court held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id.

⁸ See *id.* As discussed below, some courts have questioned the applicability of the third-party disclosure rule in the digital era, in particular to cell phone location data. See *infra* note 10; *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015), *reh’g en banc granted*, 624 Fed. App’x 75 (4th Cir. 2015).

⁹ See *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

(continued)

has long held that the government may search an individual and her possessions when she is crossing the border, without a warrant, probable cause, or any individualized suspicion.¹⁰ But most of us routinely carry some form of personal computer—a laptop, tablet, or smart phone—with us when we travel, including internationally. And, as the Court observed in *Riley v. California*,¹¹ those computers generally contain more personal information than could be gleaned from an exhaustive search of one’s home.¹² They record with precision and unerring accuracy who you have been communicating with, what you have been reading, what information you have searched for, and where you have been.¹³ Should the state be permitted to search computers for such information, without any basis for suspicion, simply because one is crossing a border?

If the U.S. government had its way, every arrestee who happened to be carrying a cellphone would also have surrendered all the information on his phone to the police. The government maintained that the search incident to lawful arrest exception—which provides that the police may, without any further suspicion or warrant, search the person of an arrestee and any containers in his immediate control—authorizes police to search arrestees’ cell phones and smart phones.¹⁴ The Court, however, unanimously rejected that proposition, holding that because of the quantity

That searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration.

Id.

¹⁰ See *Ramsey*, 431 U.S. at 616; but see *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (declining to apply the extended border search exception to forensic search of laptop computer).

¹¹ 134 S. Ct. 2473 (2014).

¹² See *id.* at 2491.

[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Id.

¹³ See *id.* at 2490 (observing that “it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives”).

¹⁴ See *id.* at 2491.

and personal character of the information contained in cellphones, the police must obtain a warrant to search a cellphone of an arrestee.¹⁵

As Jennifer Daskal has powerfully shown, computer data can travel across borders without our awareness, is often difficult to associate with particular individuals while en route, and can be stored virtually anywhere in the world.¹⁶ These features have the potential to compromise privacy protections for such data in significant ways.¹⁷ If the Fourth Amendment is deemed not to protect against searches directed at foreign nationals living abroad—as a broad reading of the Court’s decision in *United States v. Verdugo-Urquidez*¹⁸ might suggest—then many of our communications are, as a practical matter, vulnerable to searches without constitutional limitation of any kind.¹⁹ In that case, the Court declined to extend the Fourth Amendment’s warrant requirement to U.S. officials’ search of a Mexican national’s home in Mexico.²⁰ Relying on that precedent, the U.S. government maintains that as long as the National Security Agency (NSA) targets a foreign national living abroad, it need not satisfy Fourth Amendment standards, even if it “incidentally” collects communications with U.S. citizens and residents by doing so.²¹

As a result of the digital revolution, the face of privacy has changed, and will continue to change, dramatically. We are in danger of losing much of the privacy we once had, which has immense consequences not only for our personal lives but also for the character of our country. The aim of this essay is to describe the danger, respond to some of the most common arguments that we need not worry about the problem, and point to signs that all three branches of the federal government have begun to recognize that the digital age poses new challenges that require new rules to ensure the protection of privacy.

The significance of digital technology developments to both surveillance and privacy cannot be overstated. Before the advent of computerized records and the internet, much of the information now routinely collected was either unavailable or available only at prohibitive

¹⁵ See *id.* at 2485.

¹⁶ Jennifer Daskal, *The Un-territoriality of Data*, 125 YALE L.J. 326, 329 (2015).

¹⁷ *Id.*

¹⁸ 494 U.S. 259 (1990).

¹⁹ See *id.* at 274–75; *id.* at 279 (Brennan, J., dissenting) (observing the Court “h[eld] that although foreign nationals must abide by our laws even when in their own countries, our Government need not abide by the Fourth Amendment when it investigates them for violations of our laws”).

²⁰ *Id.* at 263.

²¹ Brief for the Petitioners at 7, *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013) (No. 11–1025).

cost. For example, if the government wanted to know where you were every moment of the day, it could in theory assign an investigator to tail you around the clock.²² But that is both expensive and exceedingly difficult to accomplish without detection. Moreover, even such round-the-clock surveillance could not see what you were doing inside buildings and behind walls. Now, we all carry with us at virtually all times a cell phone or smart phone, devices that routinely track our location, record many of our communications and thoughts, and transmit that information to phone companies and internet service providers.²³

In the past, if the government wanted to know what you were reading or thinking about, it had limited options. It could search your home to see what was there, but that required probable cause and a warrant,²⁴ and even then it would only stumble across those materials that you kept on hand. There would be no real way of knowing what you were thinking about, short of asking you directly. If there were any likelihood that an answer might be incriminating, you could assert the Fifth Amendment privilege against compelled self-incrimination.²⁵ Now the government can, without probable cause or a warrant, obtain your web browsing history from Google, which likely knows more about what you have been thinking than you yourself might be aware. I can forget what I was researching three days, much less three months, ago; Google, in contrast, never forgets.

In addition to perfect recall, computers also have the capacity to store and analyze massive amounts of information about any one of us, or—as NSA contractor Edward Snowden’s 2013 disclosures revealed—about all of us. Among other things, Snowden’s leak informed Americans that, for more than seven years, the NSA had been collecting phone “metadata”—the phone numbers we call and the time and duration of our conversations—on virtually all of us.²⁶ It did so under the ostensible

²² See *United States v. Jones*, 132 S. Ct. 945, 961 (2012) (Alito, J., concurring).

²³ According to Pew Research, as of 2013, 91% of Americans owned some kind of cell phone. Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RES. CTR. (June 6, 2013), <http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults>. And in 2015, nearly two-thirds of Americans owned smart phones. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (April 1, 2015), <http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015>.

²⁴ See, e.g., *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978) (“The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.”).

²⁵ See U.S. CONST. amend. V (“No person . . . shall be compelled in any criminal case to be a witness against himself . . .”).

²⁶ See Dan Roberts & Spencer Ackerman, *NSA Mass Phone Surveillance Revealed by Edward Snowden Ruled Illegal*, GUARDIAN (May 7, 2015, 11:39 AM), [\(continued\)](#)

authority of a provision of the USA PATRIOT Act that authorized the FBI to obtain only those business records “relevant” to a specific terrorist investigation.²⁷ But the NSA argued—and the Foreign Intelligence Surveillance Court (FISA Court or FISC) agreed in secret, one-sided proceedings—that it should be able to collect everyone’s records without any connection to terrorism, on the theory that anyone’s records might at some future point become relevant to a terrorist investigation.²⁸ On that expansive theory of relevance, it is not clear what information would not be subject to bulk collection by our security agencies.

The NSA’s international surveillance is even more intrusive. Snowden revealed that the NSA, often acting in concert with Britain’s General Communications Headquarters (GCHQ), has intercepted and collected not just metadata, but the actual contents of all manner of electronic communications from millions of foreign nationals, including texts, phone calls, emails, contact lists, and internet browsing.²⁹ Under section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, the NSA can collect the contents of electronic communications of any person it believes is a foreign national living abroad, as long as it does so for foreign intelligence purposes.³⁰ It need not have individualized suspicion that the target is engaged in any terrorism, espionage, or wrongdoing of any kind.³¹ Under another authority, Executive Order 12,333, the NSA collects foreign communications data without any statutory or constitutional limit whatsoever.³² Until recently, the NSA was constrained in how aggressively it could monitor the world by its limited resources and capabilities. Today, however, it has the capacity to collect, store, and analyze massive quantities of information—and it seems to have had the attitude that if it *can* collect and analyze information, it *should* do so. Modern technology affords the government newfound ways to monitor all of us. And as long as it does so with information gathered from third

<http://www.theguardian.com/us-news/2015/may/07/nsa-phone-records-program-illegal-court>.

²⁷ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 215, 115 Stat. 272 (2001).

²⁸ See *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (rejecting government’s expansive interpretation of section 215, and finding the NSA metadata program unauthorized by statute).

²⁹ Nick Hopkins, *UK Gathering Secret Intelligence via Covert NSA Operation*, GUARDIAN (June 7, 2013, 9:27 AM), <http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>.

³⁰ FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436 (2008).

³¹ See *id.*

³² Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

parties, at borders, or from foreign nationals living abroad, the government contends that the Constitution imposes no limits on its ability to do so.³³

These advances in technological capacity also increase exponentially the government's ability to construct intimate portraits of any particular individual's life by collecting all sorts of disparate data about the individual, and then combining and analyzing the data for revealing patterns. A single phone call, credit card transaction, or location might not tell very much about someone's private life. But, for example, if the phone call was to an abortion provider, the location showed that the individual shortly thereafter visited the provider, and the credit card showed a sizeable fee paid, one could easily infer that an unwanted pregnancy had been terminated.

Defenders of the new surveillance make several arguments for why we need not be concerned. None of them pass muster. With respect to the domestic NSA phone metadata program, they insist that the government collects only metadata about the calls and not their content. But the collection of metadata alone can have major consequences. Metadata could reveal, for example, whether one is calling a rape crisis, suicide, or drug treatment hotline; or a mistress, bookie, or specific political organization or party. As Stewart Baker, former general counsel of the NSA, has said, "Metadata absolutely tells you everything about somebody's life. . . . If you have enough metadata, you don't really need content."³⁴ When I quoted Baker's remark at a public debate with General Michael Hayden, former director of the NSA, Hayden concurred readily, and raised him one. Hayden boasted, "We kill people based on metadata."³⁵

In some ways, metadata is more threatening to privacy than content because it is more easily analyzed by computer. To derive useful information from the content of phone calls, a human being has to take the time to listen to them. (This may become less true as voice recognition technology improves.) But computer algorithms can be used to draw critical conclusions from metadata about individuals' private lives without having to listen to the content of their conversations. Accordingly, the

³³ See PRIVACY & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 119 (July 2, 2014), <https://www.pclomb.gov/library/702-Report.pdf>.

³⁴ See Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. BOOKS, (Nov. 21, 2013) (quoting Stewart Baker), <http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public>.

³⁵ See David Cole, 'We Kill People Based on Metadata', N.Y. REV. BOOKS (May 10, 2014, 10:12 AM), <http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata>.

government is able to engage in dragnet surveillance³⁶ with metadata at a much lower cost than if it had to review content.

Some NSA defenders suggest that as long as there are enough back-end limits on how the information can be used, we ought not to be concerned about government collecting and storing the information in the first place. Thus, the government has stressed that the NSA's phone database could only be accessed by a limited number of NSA analysts, only for counterterrorism purposes, and only if they had reasonable suspicion that a particular phone number was associated with a terrorist organization or individual.³⁷

Back-end use limitations are an important element of the reasonableness of searches and seizures and an important tool in protecting privacy. Particularly in an age when the private sector already collects vast quantities of data about our private lives,³⁸ it is essential that we pay more attention to how that information is used. Europeans, for example, insist on strict limits on how private companies use the private data they collect, and they restrict how information, once it has been collected, can be used, sold, or transferred to others.³⁹ Until now, with a few exceptions, Fourth Amendment doctrine has focused on the act of collection and has had relatively little to say about how that information is actually maintained, collated, and used by the state. Thus, to search a home, the police must generally have probable cause and a warrant.⁴⁰ But once they seize items from the house pursuant to the warrant, they do not need additional authorization to consider it in combination with other information they may have, or to comb through the seized materials again.

There are exceptions. Under the administrative search doctrine, for example, the constitutionality of drug testing of students engaged in extracurricular activities turns in part on the limited use to which the

³⁶ "Dragnet" is defined as "a system in which the [authorities] look for criminals using systematic and thorough methods." *Dragnet*, BLACK'S LAW DICTIONARY (10th ed. 2014).

³⁷ See OFF. OF THE PRESS SEC'Y, REMARKS BY THE PRESIDENT ON REVIEW OF SIGNALS INTELLIGENCE (Jan. 17, 2014), <https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> [hereinafter SIGNALS INTELLIGENCE].

³⁸ See Marie O'Reilly, *As Private Sector Embraces Big Data, Public Sector Falls Behind*, IPI GLOBAL OBSERVATORY (May 8, 2013), <http://theglobalobservatory.org/2013/05/as-private-sector-embraces-big-data-public-sector-falls-behind>. When millions of customers around the world purchase goods at Walmart, the retailer collects data about their consumer behavior. *Id.* "The private sector has embraced big data analytics." *Id.*

³⁹ Council Directive 95/46, 1995 O.J. (L 281) 31 (EC); Case C-362/14, *Schrems v. Data Prot. Comm'r* (Oct. 16, 2015), <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130d5bbf805dca432456ea788e756c7ad?text=&docid=169195&pageInd ex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=94600>.

⁴⁰ *Vale v. Louisiana*, 399 U.S. 30, 33–34 (1970).

students' urine is put in the testing process.⁴¹ Similarly, in concluding that the taking of DNA samples from arrestees is reasonable under the Fourth Amendment, the Court stressed that the DNA was used for identification purposes only, and not to gather any of the other information that can be gleaned from genetic material.⁴² These decisions suggest that at least where private information is collected from individuals on a showing of less than probable cause, the reasonableness of the program under the Fourth Amendment may well turn on the limits imposed on how the government uses and analyzes the information.

In most instances, however, back-end use limitations are not sufficient to satisfy Fourth Amendment concerns, because the invasion of privacy is said to occur at the time of the initial search or seizure. Collection of data itself has privacy costs, irrespective of how the information is subsequently used. No court would accept the NSA collecting 24/7 videotape footage from every American's bedroom, no matter what back-end limits were imposed on access to and use of the information.

Moreover, once a database exists, what is to stop mission creep? If a database can be searched for terrorists today, why not for serial murderers and rapists tomorrow? And if data may be searched for rape and murder, why not assaults, robberies, and illegal drug transactions? Thus, although use limitations are important, they should not be treated as sufficient to satisfy Fourth Amendment standards where the government obtains private information that has the potential to reveal intimate details about individuals.

Some commentators suggest that privacy is dead in the digital age, and we should simply get used to it.⁴³ They point to young people's social media practices as evidence that privacy is no longer a serious value, given how readily individuals share the most intimate details of their lives on relatively open-access websites and platforms.⁴⁴ But that greatly overstates the case. In significant part to safeguard their privacy, most people—including most young people—still lock the doors to their houses, close the doors to their bedrooms, and password-protect their computers and phones. There remains a difference for most people between what they will share with an intimate friend, family member, doctor, or therapist, and what they

⁴¹ See *Bd. of Educ. v. Earls*, 536 U.S. 822, 825, 834 (2002).

⁴² See *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013).

⁴³ Scott McNealy, former CEO of Sun Microsystems said, "You have zero privacy anyway . . . Get over it." Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999), <http://archive.wired.com/politics/law/news/1999/01/17538>.

⁴⁴ See Theodore F. Claypoole, *Privacy and Social Media*, A.B.A. BUS. L. TODAY, http://www.americanbar.org/publications/blt/2014/01/03a_claypoole.html (last visited Feb. 25, 2016).

will post on a social media platform. Although some have chosen to bare many details of their lives, others choose to retain their privacy.⁴⁵

Finally, it is commonly said that if you have nothing to hide, you have nothing to fear. But that argument misunderstands the importance of privacy. Privacy is valuable not only to criminals, but to all of us. Most of us insist on and value the privacy of the home, even if we never intend to engage in any criminal activity there. The sense that one is being watched inflicts a chilling effect on a wide range of wholly lawful activity. Intimacy and political freedom demand privacy, even for those who have done nothing wrong.⁴⁶ A society without privacy would make it easier for the police to capture criminals and terrorists. We have nonetheless recognized that the democratic and individual values of privacy justify its protection, even though criminals will also be able to exploit it. Indeed, it is in significant part because privacy is valuable for the law-abiding that we protect it for law-breaking.

The law has always had to adapt to new technologies to preserve privacy. We can, and I believe, will, adjust the rules to preserve privacy—but only if the technologies of surveillance are not hidden in the shadows. Somewhat paradoxically, transparency is critical to effective privacy reform. Before Snowden's disclosure of the NSA domestic metadata program, for example, all three branches had approved it. President Obama maintained the program, which he inherited from his predecessor, George W. Bush. Congress reauthorized section 215 of the USA PATRIOT Act⁴⁷ seven times, even after the executive branch informed it of the NSA phone metadata program—albeit in limited classified briefings that hampered members' abilities to understand fully what was going on.⁴⁸ And the FISC repeatedly authorized the program, without even writing an opinion setting forth its reasoning.⁴⁹ Indeed, when the program was

⁴⁵ Facebook is currently the largest social media website. Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 893–94 (2013). It allows users to select their own privacy settings and who they want to see certain things. *Id.* This allows users to control the information they share with the outside world. *Id.*

⁴⁶ See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 199 (1890) (stating that privacy has value and every individual has the right to decide what he or she will and will not disclose to the public).

⁴⁷ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 215, 115 Stat. 272 (2001).

⁴⁸ David Cole, *Reining in the NSA*, N.Y. REV. BOOKS, (June 2, 2015, 3:40 PM), <http://www.nybooks.com/daily/2015/06/02/nsa-surveillance-congress-sunset>.

⁴⁹ See David Cole, *Can Privacy Be Saved?*, N.Y. REV. BOOKS (March 6, 2014), <http://www.nybooks.com/articles/2014/03/06/can-privacy-be-saved>.

disclosed, government officials often defended the program by asserting that all three branches of the government had blessed it.⁵⁰

Yet all of that changed once Snowden disclosed the program. President Obama appointed an expert review panel and subsequently endorsed several of its suggested reforms.⁵¹ He agreed, for example, that the NSA should be required to obtain judicial approval before searching its telephone database, that those searches should be more limited in scope, and that a public advocate should participate in hearings before the FISC.⁵² Another executive branch body, the Privacy and Civil Liberties Oversight Board, launched an investigation and determined that the domestic telephone metadata program was illegal because, contrary to the FISC's conclusions, it was not authorized by section 215 of the USA PATRIOT Act.⁵³

The courts, which had repeatedly authorized the NSA's domestic phone metadata program while it was secret, also changed their approach once it became public. A federal district court in Washington, D.C., declared that the program was likely unconstitutional.⁵⁴ The U.S. Circuit Court of Appeals for the Second Circuit ruled that the program was illegal from its outset, as section 215 does not encompass collecting every American's phone data in bulk.⁵⁵ Even the FISC itself, which had routinely rubber-stamped the official collection of metadata while it was secret, changed its ways. Whereas it had approved the program on multiple occasions without even writing an opinion, after the program was disclosed, it wrote an opinion providing its rationale.⁵⁶ And while the

⁵⁰ J. Kirk Wiebe, *Who Broke the Law, Snowden or the NSA?*, CNN (Dec. 18, 2013, 12:21 PM), <http://www.cnn.com/2013/12/17/opinion/wiebe-snowden-amnesty>. See also David Cole, *Must Counterterrorism Cancel Democracy?*, N.Y. REV. BOOKS (Jan. 8, 2015), <http://www.nybooks.com/articles/2015/01/08/must-counterterrorism-cancel-democracy>.

⁵¹ Mike Levine, *White House Picks Panel to Review NSA Programs*, ABC NEWS (Aug. 21, 2013, 9:50 PM), <http://abcnews.go.com/m/blogEntry?id=20030899&ref=http%3A%2F%2Ft.co%2FBZwibdjVsl>. See also THE PRESIDENT'S REV. GRP. ON INTELLIGENCE AND COMM. TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 24–42 (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

⁵² SIGNALS INTELLIGENCE, *supra* note 37.

⁵³ PRIVACY AND C.L. OVERSIGHT BD., 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 10 (2014), <https://fas.org/irp/offdocs/pcllob-215.pdf>.

⁵⁴ See *Klayman v. Obama*, 957 F. Supp. 2d 1, 41 (D.D.C. 2013).

⁵⁵ See *Clapper*, 785 F.3d at 812.

⁵⁶ *In re Application of the F.B.I. for an Order Requiring Production of Tangible Things From [Redacted]*, 2013 WL 5741573, at *9.

FISC had previously kept virtually all its opinions secret, it has, since Snowden, released many to the public.⁵⁷

Congress, which had repeatedly reauthorized the USA PATRIOT Act provision that the NSA relied on to conduct its domestic phone data program, also changed course once the program became public.⁵⁸ In June 2015, it enacted the USA FREEDOM Act,⁵⁹ which, among other changes, ended the NSA's bulk collection of metadata, allowed privacy advocates to participate in FISC hearings, required public disclosure of that court's opinions, and imposed new disclosure requirements on the NSA.⁶⁰

More broadly, both Congress and the courts have recognized that the law needs to adapt to advances in technology. Congress has amended the FISA on several occasions to reflect changes in technology.⁶¹ The Supreme Court of the United States altered Fourth Amendment doctrine to address the advent of telephone wiretapping in *Katz v. United States*,⁶² required the police to obtain a warrant before using a thermal imaging device to detect heat emanating from a home in *Kyllo v. United States*,⁶³ held in *United States v. Jones* that the Fourth Amendment is implicated by the use of a global positioning system (GPS) device to track a car's movements in public for a month,⁶⁴ and, in *Riley v. California*,⁶⁵ required a warrant to search the cellphone of an arrestee. In all of these cases, the Court rejected government arguments that the rules should not change in light of new technologies and that the government should be able to exploit

⁵⁷ See, e.g., *In re Application of F.B.I.*, Misc. No. 15-01, 2015 WL 5637562 (FISA Ct. June 29, 2015); *In re Application of F.B.I.*, No. BR 14-96, 2014 WL 5463290 (FISA Ct. June 19, 2014); *In re Application of F.B.I.*, No. BR 14-01, 2014 WL 5463097 (FISA Ct. Mar. 20, 2014).

⁵⁸ Steven Nelson, *Senate Passes Freedom Act, Ending Patriot Act Provision Lapse*, U.S. NEWS (June 2, 2015, 6:34 PM), <http://www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse>. See also USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (enacted to "reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes").

⁵⁹ 129 Stat. at 268.

⁶⁰ See generally *id.*

⁶¹ See David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act 7-8* (Brookings Inst., Geo. U. L. Ctr. & Hoover Inst., Working Paper, 2007), http://www.brookings.edu/~media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris.

⁶² 389 U.S. 347, 353 (1967).

⁶³ 533 U.S. 27, 40 (2001).

⁶⁴ 132 S. Ct. 945, 949 (2012).

⁶⁵ 134 S. Ct. 2473, 2493 (2014).

those technologies without Fourth Amendment constraints.⁶⁶ In each case, the Court adjusted Fourth Amendment doctrine to ensure the continuing protection of privacy.⁶⁷

Although the Court has not yet addressed whether the “third-party disclosure” rule needs updating in the digital era, Justice Sotomayor has already stated that she thinks it might need to be,⁶⁸ and the opinions in *Jones* and *Riley* suggest that the Court recognizes that we are indeed in a brave new world. In 2015, a panel of the U.S. Court of Appeals for the Fourth Circuit rejected application of the third-party disclosure rule to the collection of historic cell phone location data.⁶⁹ In *Graham*, the panel held that “the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user’s historical [cell-site location information] for an extended period of time,” and that the government must obtain a warrant for such data.⁷⁰ The court relied on the reasoning of Justice Alito in the GPS monitoring case, concluding that the collection of data revealing an individual’s location over an extended period of time intrudes upon a reasonable expectation of privacy.⁷¹ The Fourth Circuit has granted rehearing en banc, and a decision is pending. Other courts have found that the third party disclosure rule should apply to location data, although often over dissents.⁷² Thus, the Court is almost certain to take up the issue in the near future. If privacy is to be preserved, some modification of the third party disclosure rule is necessary, perhaps guided by the approach Justice Alito took in his concurrence in *Jones*, which recognizes that when technology enables the government to monitor citizens in ways that disclose information that they previously had a reasonable expectation would remain private, the Fourth Amendment should treat that investigative method as a search.⁷³

⁶⁶ *Riley*, 134 S. Ct. at 2491; *Jones*, 132 S. Ct. at 951–52; *Kyllo*, 533 U.S. at 37; *Katz*, 389 U.S. at 352.

⁶⁷ *Riley*, 134 S. Ct. at 2495; *Jones*, 132 S. Ct. at 949; *Kyllo*, 533 U.S. at 40; *Katz*, 389 U.S. at 359.

⁶⁸ See *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

⁶⁹ *United States v. Graham*, 796 F.3d 332, 344 (4th Cir. 2015), *reh’g en banc granted*, 624 Fed. App’x 75 (4th Cir. 2015).

⁷⁰ *Id.* at 344–45.

⁷¹ *Id.* at 347.

⁷² See, e.g., *United States v. Davis*, 785 F.3d 498, 507–09 (11th Cir. 2015) (en banc) (holding, over dissents, that cell phone location data is covered by the third party rule); *United States v. Carpenter*, 819 F.3d 880, 887–89 (6th Cir. 2016) (finding that cell phone location data is covered by the third party rule).

⁷³ *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

We need not await for the Court's protection, however. Congress and the state legislatures can also enact rules that protect privacy from the threats that new technology poses. Justice Alito has urged Congress to take up the issue.⁷⁴ In the past, Congress responded to the Court's decisions denying constitutional protection to certain types of information by enacting new statutory privacy protections.⁷⁵ Thus, although the Court interpreted the Fourth Amendment to place no limit on the government's ability to obtain records from one's bank or credit card company, Congress has enacted law restricting access to that information.⁷⁶ Although there are risks to leaving privacy protection to the legislative process—in particular the likelihood that law enforcement interests will trump privacy concerns in the drafting process—legislation is nonetheless a possible avenue for protection, particularly where, as in the NSA domestic phone metadata program, the interest in protecting privacy is widely shared.⁷⁷

The states can and should play a part as well. Many of the new surveillance technologies are available and used at the state and federal level.⁷⁸ The vast majority of criminal law enforcement is carried out by the states.⁷⁹ State legislatures and state courts are therefore appropriate venues for confronting the issue of how to preserve privacy in the digital age. State protections cannot fall below the floor established by the federal Constitution, but the states are free to provide greater protection—and many do.⁸⁰

Finally, Americans ought to confront the threats to privacy posed by the private sector. We certainly have more to fear from the state than from Google; only the state can launch a criminal investigation or prosecution, and governments have an unfortunate, but demonstrable, tendency to target dissenters.⁸¹ But it is also possible and advisable to impose privacy limits on what the private sector can do with the information it gathers from and

⁷⁴ See *Jones*, 132 S. Ct. at 962–63 (Alito, J., concurring).

⁷⁵ See Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2012).

⁷⁶ See *id.*

⁷⁷ On the risks of relying on Congress, see David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 232–33 (2015) (detailing how the Justice Department succeeded in watering down legislative restrictions on access to pen register data after *Smith v. Maryland*, 442 U.S. 735 (1979)).

⁷⁸ David Cole, *Is Privacy Obsolete?*, NATION (Mar. 23, 2015), <http://www.thenation.com/article/privacy-20-surveillance-digital-age>.

⁷⁹ See Jerold Israel, Yale Kamisar, Wayne LaFave, Nancy King & Eve Primus, CONSTITUTIONAL PROCEDURE AND THE CONSTITUTION: LEADING SUPREME COURT CASES AND INTRODUCTORY TEXT 2 (2015 ed.) (noting that state systems account for 99% of the criminal docket in the United States).

⁸⁰ See Cole, *supra* note 78.

⁸¹ See FED. R. CRIM. P. 18.

about us. As noted above, European law restricts not only what the government can do with private data but also what the private sector can do.⁸² If the government has started outsourcing much of its surveillance to private companies, we would do well to limit what those companies can do with our data in the first place.

Privacy has never been more vulnerable than it is today. The digital era has brought us unimagined conveniences, but it has simultaneously created previously unthinkable risks. Some have pointed to these developments to argue that privacy is dead. But that's a premature diagnosis. Like Mark Twain's death, reports of privacy's demise are, for the moment, greatly exaggerated. But, privacy may be on life support. Unless we insist on new rules to govern and regulate the use of new technologies of surveillance, not only our privacy will be lost but all that depends on privacy as well, including democracy itself.

⁸² See *supra* note 39 and accompanying text.

