2013

The Dangers of Surveillance

Neil M. Richards
Washington University in St. Louis School of Law, nrichards@wustl.edu

THE DANGERS OF SURVEILLANCE

Neil M. Richards[*]

From the Fourth Amendment to George Orwell's *Nineteen Eighty-Four*, and from the Electronic Communications Privacy Act to films like *Minority Report* and *The Lives of Others*, our law and culture are full of warnings about state scrutiny of our lives. These warnings are commonplace, but they are rarely very specific. Other than the vague threat of an Orwellian dystopia, as a society we don't really know why surveillance is bad and why we should be wary of it. To the extent that the answer has something to do with "privacy," we lack an understanding of what "privacy" means in this context and why it matters. We've been able to live with this state of affairs largely because the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states.

But these warnings are no longer science fiction. The digital technologies that have revolutionized our daily lives have also created minutely detailed records of those lives. In an age of terror, our government has shown a keen willingness to acquire this data and use it for unknown purposes. We know that governments have been buying and borrowing private-sector databases,[1] and we recently learned that the National Security Agency (NSA) has been building a massive data and supercomputing center in Utah, apparently with the goal of intercepting and storing much of the world's Internet communications for decryption and analysis.[2]

Although we have laws that protect us against government surveillance, secret government programs cannot be challenged until they are discovered. And even when they are, our law of surveillance provides only minimal protections. Courts frequently dismiss challenges to such programs for lack of standing, under the theory that mere surveillance creates no harms. The Supreme Court recently reversed the only major case to hold to the contrary, in *Clapper v. Amnesty International*

[*] Professor of Law, Washington University School of Law. For helpful comments on prior drafts, I thank Jim Bohman, John Inazu, Jonathan King, Wendy Niece Richards, and participants in the Washington University Political Theory Workshop. Special thanks are also due to my co-participants at the *Harvard Law Review* Symposium on Privacy and Technology — Professors Julie Cohen, Paul Schwartz, Dan Solove, and Lior Strahilevitz — and my generous commentators, Danielle Citron, David Gray, and Orin Kerr. Thanks also to my research assistants, Matthew Cin and Ananth Iyengar, and my faculty assistant, Rachel Mance.

[1] *See, e.g.*, ROBERT O'HARROW, JR., NO PLACE TO HIDE 1–4 (2005).

[2] James Bamford, *The Black Box*, WIRED, Apr. 2012, at 78, 80.

USA,[3] finding that the respondents' claim that their communications were likely being monitored was "too speculative."[4]

But the important point is that our society lacks an understanding of why (and when) government surveillance is harmful. Existing attempts to identify the dangers of surveillance are often unconvincing, and they generally fail to speak in terms that are likely to influence the law. In this Article, I try to explain the harms of government surveillance. Drawing on law, history, literature, and the work of scholars in the emerging interdisciplinary field of "surveillance studies," I offer an account of what those harms are and why they matter. I will move beyond the vagueness of current theories of surveillance to articulate a more coherent understanding and a more workable approach.

At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy."[5] A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.

At a practical level, I propose a set of four principles that should guide the future development of surveillance law, allowing for a more appropriate balance between the costs and benefits of government surveillance. First, we must recognize that *surveillance transcends the public/private divide*. Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers. Second, we must recognize that *secret surveillance is illegitimate* and prohibit the creation of any domestic-surveillance programs whose existence is secret. Third, we should recognize that *total surveillance is illegitimate* and reject the

---

[3] 133 S. Ct. 1138 (2013).

[4] *Id.* at 1147.

[5] *See generally* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008) [hereinafter Richards, *Intellectual Privacy*].

idea that it is acceptable for the government to record all Internet activity without authorization. Government surveillance of the Internet is a power with the potential for massive abuse. Like its precursor of telephone wiretapping, it must be subjected to meaningful judicial process be-fore it is authorized. We should carefully scrutinize any surveillance that threatens our intellectual privacy. Fourth, we must recognize that *surveillance is harmful*. Surveillance menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination; accord-ingly, we must recognize surveillance as a harm in constitutional standing doctrine. Explaining the harms of surveillance in a doctrinally sensitive way is essential if we want to avoid sacrificing our vital civil liberties.

I develop this argument in four steps. In Part I, I show the scope of the problem of modern "surveillance societies," in which individuals are increasingly monitored by an overlapping and entangled assemblage of government and corporate watchers. I then develop an account of why this kind of watching is problematic. Part II shows how surveillance menaces our intellectual privacy and threatens the development of individual beliefs in ways that are inconsistent with the basic commitments of democratic societies. Part III explores how surveillance distorts the power relationships between the watcher and the watched, enhancing the watcher's ability to blackmail, coerce, and discriminate against the people under its scrutiny. Part IV explores the four principles that I argue should guide the development of surveillance law, to protect us from the substantial harms of surveillance.

I. THE AGE OF SURVEILLANCE

We are living in an age of surveillance. The same digital technologies that have revolutionized our daily lives over the past three decades have also created ever more detailed records about those lives. In addition, new technologies, from surveillance cameras and web bugs to thermal scanners and GPS transponders, have increased the ability to track, observe, and monitor. The scope and variety of the types of surveillance that are possible today are unprecedented in human history. This fact alone should give us pause.

But not only have the technologies of surveillance multiplied; so too have the entities that wish to surveil. Autocratic regimes have long been the villains in the stories we tell about surveillance, but they are no longer the only governments that have stepped up their surveillance activities. Democratically elected governments in the West have deepened their commitment to surveillance of the public as well. Since 2001 this monitoring has often been done in the name of counterterrorism, but it has also been justified as protecting cybersecurity, intellectual property, children from predators, and a seemingly ever-growing list of other concerns. Some of the most well-known and

valuable publicly traded corporations have also got in on the act, often with the consent (in varying degrees) of their customers. Surveillance, it seems, is not just good politics, but also good business.

What, then, is surveillance? Scholars working throughout the English-speaking academy have produced a thick descriptive literature examining the nature, causes, and implications of the age of surveillance.[6] Working under the umbrella term of "surveillance studies," these scholars represent both the social sciences and humanities, with sociologists making many of the most significant contributions.[7]

Reviewing the vast surveillance studies literature, Professor David Lyon concludes that surveillance is primarily about power, but it is also about personhood.[8] Lyon offers a definition of surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[9] Four aspects of this definition are noteworthy, as they expand our understanding of what surveillance is and what its purposes are. First, it is *focused* on learning information about individuals. Second, surveillance is *systematic*; it is intentional rather than random or arbitrary. Third, surveillance is *routine* — a part of the ordinary administrative apparatus that characterizes modern societies.[10] Fourth, surveillance can have a wide variety of *purposes* — rarely totalitarian domination, but more typically subtler forms of influence or control.[11]

A. The Scope of Surveillance

Even a cursory overview of the kinds of surveillance that are being performed today reveals the scope of the surveillance problem. At the level of state surveillance, it should be no surprise that autocratic regimes have been among the worst offenders. For example, China has used Internet activity to detect and censor dissidents,[12] and states resisting the Arab Spring uprisings have also keenly sought social media data in order to stem the tide of the revolts.[13] Some activists also suspect that the Vietnamese government may have used computer viruses

---

[6] For three recent introductions to this vast literature, see, for example, DAVID LYON, SURVEILLANCE STUDIES (2007); SURVEILLANCE AND DEMOCRACY (Kevin D. Haggerty & Minas Samatas eds., 2010); and THE SURVEILLANCE STUDIES READER (Sean P. Hier & Joshua Greenberg eds., 2007).

[7] *See* LYON, *supra* note 6, at 18–22.

[8] *See id.* at 23.

[9] *Id.* at 14.

[10] *Id.*

[11] *See id.* at 15–16.

[12] REBECCA MACKINNON, CONSENT OF THE NETWORKED 36–40 (2012).

[13] *Id.*; Anupam Chander, Essay, *Jasmine Revolutions*, 97 CORNELL L. REV. 1505, 1516–17, 1525–28 (2012).

to monitor the Internet activity and private data of dissidents protesting government mining policies.[14]

Surveillance is not just for communists and dictators. Democratic states have also invested heavily in surveillance technologies in the aftermath of the September 11 attacks in America, the London subway bombings of 2005, and other atrocities. Britain is one of the most heavily surveilled countries in the world, with a network of public and private surveillance cameras, traffic enforcement cameras, and broad government powers to examine Internet traffic.[15] In the United States, the NSA has engaged in a program of warrantless wiretapping of telephone conversations. Although many of the details of the wiretapping and other surveillance programs remain shrouded in secrecy, it is clear that the investment in surveillance infrastructure remains significant. And as noted above, a 2012 investigative report by *Wired* magazine revealed that the NSA is building a massive supercomputing facility in the Utah desert, possibly with the goal of capturing and archiving much of the world's Internet traffic, with a view to decrypting and searching it as decryption technologies inevitably advance.[16]

Surveillance is not just for governments either. Private companies big and small generate vast fortunes from the collection, use, and sale of personal data. At the broadest level, we are building an Internet that is on its face free to use, but is in reality funded by billions of transactions where advertisements are individually targeted at Internet users based upon detailed profiles of their reading and consumer habits.[17] Such "behavioral advertising" is a multibillion-dollar business, and is the foundation on which the successes of companies like Google and Facebook have been built.[18] One recent study concludes that this form of surveillance is so ingrained into the fabric of the Internet "that a small number of companies have a window into most of our movements online."[19] Other technologies engage in similar forms of private surveillance. "Social reading" applications embedded into Facebook and other platforms enable the disclosure of one's reading habits,

---

[14] EVGENY MOROZOV, THE NET DELUSION 143–45 (2011).

[15] Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 362 (2009). *See generally* KIRSTIE BALL ET AL., A REPORT ON THE SURVEILLANCE SOCIETY: FOR THE INFORMATION COMMISSIONER BY THE SURVEILLANCE STUDIES NETWORK (David Murakami Wood ed., 2006), *available at* http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf; *How We Are Being Watched*, BBC NEWS (Nov. 3, 2006, 2:21 AM), http://news.bbc.co.uk/2/hi/uk_news/6110866.stm.

[16] *See generally* Bamford, *supra* note 2.

[17] *See* SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING 26–30 (2011).

[18] *See* DAVID KIRKPATRICK, THE FACEBOOK EFFECT 260–66 (2010); STEVEN LEVY, IN THE PLEX 262–63, 336–37 (2011).

[19] Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 279 (2012).

while electronic readers like the Kindle and the Nook track reader behavior down to the specific page of the specific book on which a user's attention is currently lingering.[20]

In recent years, industry, media, and scholars have increasingly focused their attention on the concept of "Big Data," an unwieldy term often used to describe the creation and analysis of massive data sets.[21] Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and analyzed to produce new inferences and findings. As social scientists danah boyd and Kate Crawford put it, "Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."[22] Big Data holds much potential for good in areas as diverse as medical research, the "smart" electrical grid, and traffic management.[23]

But Big Data also raises many potential problems in areas such as privacy and consumer power. For example, the retail superstore Target uses Big Data analytics to infer which of its customers are pregnant based upon their purchases of other products and upon personally identifying data from other sources.[24] As the *New York Times Magazine* reports, new parents are highly desirable customers not just because they buy many new products, but because their normally stable purchasing habits are "up for grabs" in the chaotic exhaustion that accompanies the birth of a child.[25] Target uses Big Data to snare new parents because, as one of its data analysts concedes, "[w]e knew that if we could identify them in their second trimester, there's a good chance we could capture them for years . . . . As soon as we get them buying diapers from us, they're going to start buying everything else too."[26] Big Data analytics enabled Target to discover that expectant parents display a change in buying habits (for example, buying unscented lotion and magnesium supplements) that mark them as expectant, allowing this kind of (appropriately enough) "targeted" market-

---

[20] Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 698–99 (2013) [hereinafter Richards, *The Perils of Social Reading*].

[21] danah boyd & Kate Crawford, Six Provocations for Big Data 6 (Sept. 21, 2011) (unpublished manuscript) (on file with the Harvard Law School Library).

[22] *Id.*

[23] *See generally* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. (forthcoming 2013).

[24] Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 16, 2012 (magazine), § 6, at 30, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[25] *Id.*

[26] *Id.*; *see also* Tom Simonite, *What Facebook Knows*, MIT TECH. REV. (June 13, 2012), http://www.technologyreview.com/featured-story/428150/what-facebook-knows/?mod=related.

ing. Big Data surveillance and analysis thus affect the commercial power of consumers, identifying their times of relative weakness and allowing more effective marketing to nudge them in the directions that watchful companies desire.

The incentives for the collection and distribution of private data are on the rise. The past fifteen years have seen the rise of an Internet in which personal computers and smartphones have been the dominant personal technologies. But the next fifteen will likely herald the "Internet of Things," in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control.[27] Many of us already carry GPS tracking devices in our pockets, not by government command, but in the form of powerful multifunction smartphones. Sociologists Zygmunt Bauman and David Lyon have identified the spread of surveillance beyond nonconsensual state watching to a sometimes-private surveillance in which the subjects increasingly consent and participate — a phenomenon that they call "liquid surveillance."[28] Professor Scott Peppet foresees the "unraveling" of privacy,[29] as economic incentives lead consumers to agree to surveillance devices like Progressive Insurance's "MyRate" program, which offers reduced insurance rates in exchange for the installation of a device that monitors driving speed, time, and habits.[30] Peppet argues that this unraveling of privacy creates a novel challenge to privacy law, which has long focused on unconsented surveillance rather than on surveillance as part of an economic transaction.[31]

It might seem curious to think of information gathering by private entities as "surveillance." Notions of surveillance have traditionally been concerned with the watchful gaze of government actors like police and prison officials rather than companies and individuals. But in a postmodern age of "liquid surveillance," the two phenomena are deeply intertwined. Government and nongovernment surveillance support each other in a complex manner that is often impossible to disentangle. At the outset, the technologies of surveillance — software, RFID chips, GPS trackers, cameras, and other cheap sensors —

---

[27] Clive Thompson, *Sensors Everywhere*, WIRED, Dec. 2012, at 72, *available at* http://www.wired.com/opinion/2012/12/20-12-st_thompson/. For a critique of the "Internet of Things," see ROB VAN KRANENBURG, THE INTERNET OF THINGS (2008), *available at* http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf.

[28] ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE 2–3 (2013).

[29] Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1156 (2011).

[30] *Id.* at 1153–56.

[31] *Id.*

are being used almost interchangeably by government and nongovernment watchers.[32] Private industry is also marketing new surveillance technologies to the state. Though it sounds perhaps like a plot from a paranoid science fiction novel, the *Guardian* reports that the Disney Corporation has been developing facial recognition technologies for its theme parks and selling the technology to the U.S. military.[33] Nor do the fruits of surveillance respect the public/private divide. Since the September 11 attacks, governments have been eager to acquire the massive consumer and Internet-activity databases that private businesses have compiled for security and other purposes, either by subpoena[34] or outright purchase.[35] Information can also flow in the other direction; the U.S. government recently admitted that it was giving information to insurance companies that it had collected from automated license-plate readers at border crossings.[36]

Similarly, while government regulation might be one way to limit or shape the growth of the data industry in socially beneficial ways, governments also have an interest in making privately collected data amenable to public-sector surveillance. In the United States, for example, the Communications Assistance for Law Enforcement Act of 1994[37] requires telecommunications providers to build their networks in ways that make government surveillance and interception of electronic communications possible.[38] A European analogue, the EC Data Retention Directive Regulations of 2009, requires Internet service providers to retain details of all Internet access, email, and Internet telephony by users for twelve months, so that they can be made available to government investigators for cases of antiterrorism, intellectual property, child protection, or for other purposes.[39] This surveillant symbiosis between companies and governments means that no analysis of surveillance can be strictly limited to just the government or the market in isolation. Surveillance must instead be understood in its aggregated and complex social context.

---

[32] *See* LYON, *supra* note 6, at 111–12.

[33] Naomi Wolf, *The New Totalitarianism of Surveillance Technology*, GUARDIAN (Aug. 15, 2012, 4:12 PM), http://www.guardian.co.uk/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology.

[34] *See* Gonzales v. Google, Inc., 234 F.R.D. 674, 688 (N.D. Cal. 2006).

[35] *See* O'HARROW, *supra* note 1, at 64, 98–103.

[36] Cyrus Farivar, *License Plates Scanned at Border, Data Shared with Car Insurance Group*, ARS TECHNICA (Aug. 22, 2012, 4:36 PM), http://arstechnica.com/tech-policy/2012/08/license-plates-scanned-at-border-data-shared-with-car-insurance-group/.

[37] 47 U.S.C. §§ 1001–1010 (2006).

[38] *Id.* § 1002.

[39] The United Kingdom version of this regulation is The Data Retention (EC Directive) Regulations, 2009, S.I. 2009/859 (U.K.), *available at* http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents.

B. Surveillance Law's Limited Protections

American law governing surveillance is piecemeal, spanning constitutional protections such as the Fourth Amendment, statutes like the Electronic Communications Privacy Act of 1986[40] (ECPA), and private law rules such as the intrusion-into-seclusion tort.[41] But the general principle under which American law operates is that surveillance is legal unless forbidden. Perhaps out of a fear that surveillance might be used to suppress dissent, American law contains some limited protections against government surveillance of purely political activity. For example, government investigators in antiterrorism cases possess a powerful tool known as the National Security Letter (NSL). NSLs are statutory authorizations by which the FBI can obtain information about people from their telephone companies, Internet service providers, banks, credit agencies, and other institutions with which those people have a relationship. NSLs are covert and come with a gag order that prohibits the recipient of the letter from disclosing its existence, even to the person whose secrets have been told to the government. NSLs can currently be obtained under four federal statutes: the Right to Financial Privacy Act of 1978[42] (RFPA), the ECPA,[43] the Fair Credit Reporting Act[44] (FCRA), and the National Security Act of 1947.[45] Taken together, these provisions allow the FBI to access a wide variety of information about people, including historical and transactional information relating to telephone calls and emails, financial information, and consumer credit information.[46] This information can be obtained by crossing a very low threshold — the FBI must merely certify in writing that the request is "relevant to an authorized investigation to protect against international terrorism or clandestine

---

40 Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

41 *See generally* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

42 12 U.S.C. §§ 3401–3422 (2006 & Supp. V 2011) (allowing access to personal financial records held by a wide variety of entities, including casinos, insurance companies, automobile dealerships, credit unions, real estate companies, and travel agencies).

43 18 U.S.C. § 2709 (allowing access to telephone and email information including billing and call history, email, subscriber information, and screen names).

44 15 U.S.C. §§ 1681–1681x (2006 & Supp. V 2011); *see also id.* § 1681u (allowing access to credit history information and the header information on credit reports, including name, address, and employment history); *id.* § 1681v (allowing access to a consumer's full credit report and "all other information in a consumer's file").

45 50 U.S.C. §§ 401–442b (2006 & Supp. V 2011); *see also id.* § 436 (allowing the issuance of NSLs in connection with investigations of improper disclosure of classified information by government employees).

46 *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 10 (2007).

intelligence activities."[47] Communications and bank records sought under the ECPA and the RFPA are protected by the additional requirement that the FBI certify that "such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[48]

Despite these protections, courts lack the tools to enforce them. This problem predates the current NSL framework. For example, in 1967, the President ordered the U.S. Army to engage in surveillance of domestic dissident groups, fearing civil disorder in the aftermath of the assassination of Martin Luther King, Jr.[49] The program expanded over time to become a large-scale military surveillance program of the domestic political activities of American citizens.[50] In *Laird v. Tatum*,[51] the Supreme Court held that it lacked jurisdiction over the claims that the surveillance violated the First Amendment rights of the subjects of the program, because the subjects claimed only that they felt deterred from exercising their First Amendment rights or that the government could misuse the information it collected in the future.[52] The Court could thus declare that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[53]

More recent surveillance cases have followed the lead of the *Laird* Court. Challenges to the NSA's wiretapping program have foundered because plaintiffs have failed to convince federal courts that secret surveillance has caused them any legally cognizable injury. In *ACLU v. NSA*,[54] the Sixth Circuit dismissed any suggestion that First Amendment values were threatened when the government listened to private conversations. As that court put it: "The First Amendment protects public speech and the free exchange of ideas, while the Fourth Amendment protects citizens from unwanted intrusion into their personal lives and effects."[55] The court concluded that the plaintiffs had

---

[47] This precise language is quoted from the ECPA, 18 U.S.C. § 2709(b)(1)–(2), but the other NSL provisions are substantially similar. *See* 12 U.S.C. § 3414(a)(5)(A) (RFPA); 15 U.S.C. §§ 1681u(b), 1681v(a) (FCRA); 50 U.S.C. § 436(a)(3) (National Security Act).

[48] 18 U.S.C. § 2709(b)(1)–(2) (ECPA); 12 U.S.C. § 3414(a)(5)(A) (RFPA). The original FCRA NSL provision allowing access to the headers of credit reports only, 15 U.S.C. § 1681u(b), contains such a First Amendment limitation, but since the Patriot Act added § 1681v, which allows for the full credit report to be obtained without meeting the First Amendment requirement, it is unclear what practical effect the limitation in § 1681u(b) will have.

[49] *See* Laird v. Tatum, 408 U.S. 1, 4–5 (1972).

[50] *See id.* at 6–7.

[51] 408 U.S. 1.

[52] *Id.* at 13.

[53] *Id.* at 13–14.

[54] 493 F.3d 644 (6th Cir. 2007).

[55] *Id.* at 657 n.15 (citations omitted).

no standing to assert First or Fourth Amendment violations, as they could not prove that the secret government surveillance program had targeted them.[56] Similarly, in *Al-Haramain Islamic Foundation, Inc. v. Bush*,[57] the government successfully invoked the state-secrets doctrine to stop the plaintiffs from finding out whether they were the subjects of secret surveillance under the program.[58] This ruling created a brutal paradox for the plaintiffs: they could not prove whether their telephone calls had been listened to, and thus they could not establish standing to sue for the violation of their civil liberties.[59] Despite the fact that the judges in the case knew whether surveillance had taken place, they believed that the state-secrets doctrine barred them from ruling on that fact.[60] And the Court's most recent decision in *Clapper* affirmed this approach to standing to challenge surveillance. Plaintiffs can only challenge secret government surveillance they can prove, but the government isn't telling. Plaintiffs (and perhaps civil liberties) are out of luck.

So far so bad. Or maybe not. Putting the oppression of totalitarian states to one side, public and private surveillance can have beneficial effects. All other things being equal, greater security from crime and terrorism is a good thing.[61] So too are the conveniences of modern communications, email, and the power of a search engine in our pockets valuable advances that improve our quality of life. And a sensible system of automated traffic regulation can save money and direct scarce police resources to serious criminals rather than ordinary motorists.

As a society, we are thus of two minds about surveillance. On the one hand, it is creepy, Orwellian, and corrosive of civil liberties. On the other hand, it keeps us and our children safe. It makes our lives more convenient and gives us the benefit of a putatively free Internet. Moreover, some influential thinkers argue that data surveillance does not affect privacy at all. As Judge Posner puts it:

> The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their vol-ume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting,

---

[56] *Id.* at 673–74.

[57] 507 F.3d 1190 (9th Cir. 2007).

[58] *Id.* at 1204.

[59] *See id.* at 1205.

[60] *See id.* at 1204–05.

[61] *See* RICHARD A. POSNER, NOT A SUICIDE PACT 130 (2006) (arguing that adherence to civil liberties like the right to privacy must be flexible where it conflicts with government antiterrorism efforts).

> far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.[62]

Surveillance is thus confusing. We like its benefits, though we are fearful (and sometimes dismissive) of its costs. This confusion points to a larger problem: civil liberties advocates lack a compelling account of when and why (if at all) surveillance is harmful. As a society, we have an intuitive understanding that public- and private-sector surveillance is potentially bad, but we do not have an articulate explanation of why it is bad. Some of our intuitions stem from literature, such as George Orwell's chilling portrait of Big Brother in *Nineteen Eighty-Four*.[63] But few critics of government surveillance such as the NSA wiretapping program and the British data-retention regulations would suggest that these programs are directly analogous to the evil regime depicted in Orwell's dystopia. Moreover, the Orwell metaphor seems wholly inapplicable to databases used to personalize targeted advertising on the web, the efforts of insurance companies to promote safe driving, and the practices of online booksellers to sell more books by monitoring consumers' shopping habits in ways that used to be impossible.[64]

We need an account of when and why surveillance is problematic to help us see when we should regulate and when we should not. The following Parts seek to provide an account of some of the dangers of surveillance and the ways in which laws could mitigate them. I want to advance two lines of critique to the notion that surveillance does not create a legally cognizable injury: first, that surveillance by government and private actors threatens intellectual privacy and chills the exercise of vital civil liberties; and second, that surveillance affects the power balance between individuals and those who are watching, increasing the risk of persuasion, blackmail, and other harmful uses of sensitive information by others.

II. SURVEILLANCE AND INTELLECTUAL PRIVACY

The most salient harm of surveillance is that it threatens a value I have elsewhere called "intellectual privacy."[65] Intellectual-privacy

---

[62] Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html.

[63] GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Irving Howe ed., Harcourt Brace Jovanovich, Inc. 1982) (1949).

[64] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 29–36 (2004) (critiquing the usefulness of Orwell's metaphor as a tool in understanding the private database industry). *But see* Neil M. Richards, Essay, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1133 (2006) (suggesting that the Orwell metaphor retains some validity as a tool to understand electronic surveillance).

[65] Richards, *Intellectual Privacy*, *supra* note 5, at 389; Richards, *The Perils of Social Reading*, *supra* note 20, at 691.

theory suggests that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy — protection from surveillance or interference — is necessary to promote this kind of intellectual freedom. It rests on the idea that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse.[66] I want to be clear at the outset that intellectual-privacy theory protects "intellectual" activities, broadly defined — the processes of thinking and making sense of the world with our minds. Intellectual privacy has its limits — it is a subset of all things that we might call "privacy," albeit a very important subset. But importantly, intellectual privacy is not just for intellectuals; it is an essential kind of privacy for us all.

At the core of the theory of intellectual privacy are two claims, one normative and one empirical. The normative claim is that the foundation of Anglo-American civil liberties is our commitment to free and unfettered thought and belief — that free citizens should be able to make up their own minds about ideas big and small, political and trivial. This claim requires at a minimum protecting individuals' rights to think and read, as well as the social practice of private consultation with confidantes. It may also require some protection of broader social rights, whether we call them rights of association or assembly.[67] Protection of these individual rights and social practices allows individuals to develop both intellectual diversity and eccentric individuality. They reflect the conviction that big ideas like truth, value, and culture should be generated from the bottom up rather than from the top down.[68]

These commitments to the freedoms of thought, belief, and private speech lie at the foundation of traditional First Amendment theory, though they have been underappreciated elements of that tradition. But as I have argued elsewhere, a careful examination reveals that a commitment to freedom of thought is present in virtually every major text in First Amendment theory.[69] In particular, freedom of thought lies at the core of the modern American tradition of First Amendment libertarianism, which began with the opinions of Justices Holmes and

---

[66] Richards, *Intellectual Privacy*, *supra* note 5, at 403–04.

[67] *See, e.g.*, Ashutosh Bhagwat, *Associational Speech*, 120 YALE L.J. 978, 998 (2011) ("An association is a coming together of individuals for a common cause or based on common values or goals."). *See generally* JOHN D. INAZU, LIBERTY'S REFUGE (2012) (arguing for the protection of political- and religious-group autonomy under the alternative rubric of the right of assembly).

[68] *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (2012).

[69] *See* Richards, *Intellectual Privacy*, *supra* note 5, at 408–12 (exploring this point in greater detail). For a similar argument, see generally Seana Valentine Shiffrin, *A Thinker-Based Approach to Freedom of Speech*, 27 CONST. COMMENT. 283 (2011).

Brandeis in the decade following the end of the First World War. Dissenting from the majority position of the Supreme Court, the two friends developed theories that justified special protection for speech and ideas under the First Amendment. The two men advanced slightly different reasons why speech should be protected — Justice Holmes justified protection in terms of the search for truth, while Justice Brandeis privileged democratic self-government — but each theory enshrined protection for free thought at its core. For example, Justice Holmes's dissent in *Abrams v. United States*[70] is a forceful statement of the idea that democratic institutions depend on minds' being able to freely and fearlessly engage in the search for political truth. As he put it poetically:

> [W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.[71]

Justice Brandeis also placed the freedom of thought at the foundation of his justification for special protection for free speech. In *Whitney v. California*,[72] he wrote:

> Those who won our independence believed that *the final end of the State was to make men free to develop their faculties*; and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty. *They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth . . . .*[73]

Thus, in each of the traditional American justifications for freedom of speech,[74] a commitment to freedom of thought — to intellectual freedom — rests at the core of the tradition.

---

[70] 250 U.S. 616 (1919).

[71] *Id.* at 630 (Holmes, J., dissenting).

[72] 274 U.S. 357 (1927).

[73] *Id.* at 375 (Brandeis, J., concurring) (emphasis added).

[74] Although most courts justify free speech in terms of truth-seeking or democratic self-governance, some scholars have argued that free speech is better justified in terms of the autonomy or self-development of the individual. *See, e.g.*, C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964, 990–92 (1978); Martin H. Redish, *The Value of Free Speech*, 130 U. PA. L. REV. 591, 593–94 (1982); David A. J. Richards, *Free Speech and Obscenity Law: Toward a Moral Theory of the First Amendment*, 123 U. PA. L. REV. 45, 62 (1974); Thomas Scanlon, *A Theory of Freedom of Expression*, 1 PHIL. & PUB. AFF. 204, 210–19 (1972). Free thought is a logically necessary precondition for autonomous speech, though this point is underdeveloped in the relevant literature. For an analysis of the relationship between free thought and autonomous speech, see Richards, *Intellectual Privacy*, *supra* note 5, at 406 & n.113, and see generally Shiffrin, *supra* note 69.

The second claim at the core of the theory of intellectual privacy is an empirical one — that surveillance inclines us to the mainstream and the boring. It is a claim that when we are watched while engaging in intellectual activities, broadly defined — thinking, reading, web-surfing, or private communication — we are deterred from engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality.

Three different kinds of arguments highlight the ways in which surveillance can restrain intellectual activities. The first set of arguments relies on cultural and literary works exploring the idea that surveillance deters eccentric or deviant behavior. Many such works owe a debt to Jeremy Bentham's idea of the Panopticon, a prison designed around a central surveillance tower from which a warden could see into all of the cells. In the Panopticon, prisoners had to conform their activities to those desired by the prison staff because they had no idea when they were being watched. As Bentham describes this system, "[t]o be incessantly under the eyes of an Inspector is to lose in fact the power of doing ill, and almost the very wish."[75] Of course, the most famous cultural exploration of the conforming effects of surveillance is Orwell's harrowing depiction in *Nineteen Eighty-Four* of the totalitarian state personified by Big Brother.[76] Orwell's fictional state sought to prohibit not just verbal dissent from the state but even the thinking of such ideas, an act punished as "thoughtcrime" and deterred by constant state surveillance.[77] Some scholars have documented how the modern surveillance environment differs from both the classic Panopticon and a fully realized Big Brother in important ways.[78] Nevertheless, Orwell's insight about the effects of surveillance on thought and behavior remains valid — the fear of being watched causes people to act and think differently from the way they might otherwise.

Our cultural intuitions about the effects of surveillance are supported by a second set of arguments that comes from the empirical work of scholars in the interdisciplinary field of surveillance studies. Moving beyond the classic metaphors of the Panopticon and Big Brother, these scholars have tried to understand modern forms of surveillance by governments, companies, and individuals in all of their

---

[75] Jeremy Bentham, *Panopticon*, *in* 3 OPINIONS OF DIFFERENT AUTHORS UPON THE PUNISHMENT OF DEATH 321, 328 (Basil Montagu ed., 1816).

[76] ORWELL, *supra* note 63, at 4.

[77] *Id.* at 14.

[78] *See, e.g.*, Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605, 606–08 (2000); SOLOVE, *supra* note 64, at 33–35.

complexities.[79] The scope of this burgeoning literature has been wide-ranging and provides many examples of the normalizing effects of surveillance in a wide variety of contexts. In his pioneering work in the 1980s, for example, Professor Anthony Giddens argues that surveillance continually seeks the supervision of social actors and carries with it a permanent risk that supervision could lead to domination.[80] More recent scholars have explored the risks that surveillance poses to democratic self-governance.[81] One such risk is that of self-censorship, in terms of speech, action, or even belief. Studies of communist states give social-scientific accounts of many of the cultural intuitions about these self-censoring effects of surveillance,[82] but so too do studies of modern forms of surveillance in democratic societies. For example, one study of the EU Data Retention Directive notes that "[u]nder pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations."[83] As I explore below, the scope of surveillance studies is much broader than merely the study of panoptic state surveillance; scholars working in this field have examined the full scope of modern forms of watching, including data surveillance by private actors. But above all, surveillance scholars continually reaffirm that, while surveillance by government and others can have many purposes, a recurrent purpose of surveillance is to control behavior.[84]

A third and final set of arguments for intellectual privacy comes from First Amendment doctrine. A basic principle of free speech law as it has developed over the past century is that free speech is so important that its protection should err on the side of caution. Given the uncertainty of litigation, the Supreme Court has created a series of procedural devices to attempt to ensure that errors in the adjudication of free speech cases tend to allow unlawful speech rather than engage in mistaken censorship. These doctrines form what Professor Lee Bollinger calls the "First Pillar" of First Amendment law — the "[e]xtraordinary [p]rotection against [c]ensorship."[85] Such doctrines take various forms, such as those of prior restraint, overbreadth, and vagueness, but they are often characterized under the idea of the "chilling effect." This idea maintains that rules that might deter potentially valuable expression should be treated with a high level of suspi-

---

[79] *See generally* LYON, *supra* note 6.

[80] *See generally* ANTHONY GIDDENS, THE NATION-STATE AND VIOLENCE (1985).

[81] *See generally, e.g.*, SURVEILLANCE AND DEMOCRACY, *supra* note 6.

[82] *See, e.g.*, Maria Los, *A Trans-Systemic Surveillance: The Legacy of Communist Surveillance in the Digital Age*, *in* SURVEILLANCE AND DEMOCRACY, *supra* note 6, at 173, 174–75.

[83] Lilian Mitrou, *The Impact of Communications Data Retention on Fundamental Rights and Democracy — The Case of the EU Data Retention Directive*, *in* SURVEILLANCE AND DEMOCRACY, *supra* note 6, at 127, 138.

[84] *See, e.g.*, LYON, *supra* note 6, at 15; BALL ET AL., *supra* note 15, at 4.

[85] LEE C. BOLLINGER, UNINHIBITED, ROBUST, AND WIDE-OPEN 12 (2010).

cion by courts. As the Supreme Court put it in perhaps its most important free speech decision of the twentieth century, *New York Times Co. v. Sullivan*,[86] the importance of uninhibited public debate means that, although "erroneous statement is inevitable in free debate, . . . it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need . . . to survive.'"[87] As Professor Frederick Schauer explains, "the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech."[88] Although the chilling-effect doctrine has been criticized on grounds that it overprotects free speech and makes empirically unsupported judgments,[89] such criticisms miss the point. The doctrines encapsulated by the chilling effect reflect the substantive value judgment that First Amendment values are too important to require scrupulous proof to vindicate them, and that it is (constitutionally speaking) a better bargain to allow more speech, even if society must endure some of that speech's undesirable consequences.

Intellectual-privacy theory explains why we should extend chilling-effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.[90] Professor Timothy Macklem argues that "[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive."[91] A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling-effect doctrine's normative commitment to err on the side of First Amendment values even if proof is imperfect.

---

[86] 376 U.S. 254 (1964).

[87] *Id.* at 271–72 (second omission in original) (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

[88] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 688 (1978).

[89] *See generally, e.g.*, Leslie Kendrick, *Speech, Intent and the Chilling Effect*, 54 WM. & MARY L. REV. (forthcoming 2013).

[90] *See* COHEN, *supra* note 68, at 223–25; Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912, 1918 (2013).

[91] TIMOTHY MACKLEM, INDEPENDENCE OF MIND 36 (2006).

Intellectual-privacy theory therefore suggests a solution to the confusion that has plagued courts and others in dealing with whether surveillance programs create legally cognizable injuries. Despite often displaying an intuitive understanding that surveillance might be potentially harmful, courts have struggled to understand why. This absence of clarity has led to courts misunderstanding and diminishing privacy interests that conflict with other values. When faced with balancing a vague and poorly articulated privacy right against state interests such as the prevention of terrorist attacks, surveillance tends to win. Courts also make the mistake that the *ACLU v. NSA* court made and cast surveillance as solely a Fourth Amendment issue of crime prevention, rather than as one that also threatens intellectual freedom and First Amendment values of the highest order.[92] Other decisions mirror the mistake of the *Al-Haramain* court in concluding that preventing secret surveillance is less important than inconveniencing the executive branch.[93] Additionally, some courts can make the mistake that the *Clapper* Court made, refusing to recognize as justiciable harms the costly measures that people must adopt to shield their communications from government surveillance.[94]

Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society. My argument is not that intellectual surveillance should never be possible, but that when the state seeks to learn what people are reading, thinking, and saying privately, such scrutiny is a serious threat to civil liberties. Accordingly, meaningful legal process (that is, at least a warrant supported by probable cause) must be followed before the government can perform the digital equivalent of reading our diaries.

But we must also remember that in modern societies, surveillance fails to respect the line between public and private actors. Intellectual privacy should be preserved against private actors as well as against the state. Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained in our actions by peer pressure at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which (as noted above) has shown a

---

92 *See* ACLU v. NSA, 493 F.3d 644, 657 (6th Cir. 2007).

93 *See* Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1201–05 (9th Cir. 2007).

94 *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150–53 (2013).

voracious interest in all kinds of personal information, particularly records related to the operation of the mind and political beliefs.[95] Put simply, the problem of intellectual privacy transcends the public/private divide, and justifies additional legal protections on intellectual privacy and the right to read freely.[96] Constitutional law and standing doctrine alone will not solve the threat of surveillance to intellectual freedom and privacy, but they are a good place to start.

III. SURVEILLANCE AND POWER

The mechanics of intellectual privacy discussed so far depend upon knowing, or at least fearing, that someone might be watching us. If we have a sense of privacy, even one that turns out to be an illusion, we are less likely to change our behavior under the panoptic gaze. Truly secret and unexpected surveillance, from this perspective, might appear not to violate our intellectual privacy at all. If we have no inkling that we are being watched, if we really do not care that we are being watched, or if we fear no consequences of being watched, it could be argued that our intellectual freedom is unaffected. It can thus be argued that if the NSA Wiretapping Program had never leaked, it would have posed no threat to intellectual privacy.

There are two problems with this account. First, no program of widespread surveillance is likely to remain secret forever. At some point, such a program will inevitably come to light, either by being leaked (as happened with the NSA program and the Army surveillance in *Laird*), or by actions taken pursuant to the program (such as prosecutions or disclosures). The injury suffered by those thus punished would serve as an example to the rest of us, and the mechanisms of intellectual privacy would come into effect at that point.

Second, surveillance (even secret surveillance) can create additional harms that are separate from the ones suggested by intellectual-privacy theory. Scholars working in surveillance studies have explored the phenomenon of surveillance in all of its contemporary complexity, going beyond the Panopticon to consider private surveillance, the relationships between watchers and watched, and the wide variety of dangers that modern surveillance societies raise.[97] Recall in this regard that Lyon's definition of surveillance notes that surveillance has a purpose,[98] but in the modern era this purpose is rarely totalitarian domination. All the same, most forms of surveillance seek some form

---

[95] *See* Richards, *Intellectual Privacy*, *supra* note 5, at 427–28 (providing examples).

[96] *See generally* Richards, *The Perils of Social Reading*, *supra* note 20.

[97] *See, e.g.*, Kevin D. Haggerty & Minas Samatas, *Introduction*, *in* SURVEILLANCE AND DEMOCRACY, *supra* note 6, at 1, 3–4.

[98] *See* LYON, *supra* note 6, at 14.

of subtler influence or control over others. Even when surveillance is not Orwellian, it is usually about influencing or being able to respond to someone else's behavior. And while surveillance can sometimes have benign goals (like traffic safety, or parents using baby monitors or GPS trackers to keep tabs on their children), it is invariably tied to a particular purpose. Critically, the gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance.[99] It might sound trite to say that "information is power," but the power of personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion.

A. Blackmail

Information collected surreptitiously can be used to blackmail or discredit opponents by revealing embarrassing secrets. American political history over the past hundred years furnishes numerous examples of this phenomenon, but perhaps the most compelling is the treatment of Martin Luther King, Jr., by the FBI. Concerned that Dr. King was a threat to public order, the FBI listened to his private telephone conversations in order to seek information with which to blackmail him. As the official government investigation into the Dr. King wiretaps concluded in 1976:

> The FBI collected information about Dr. King's plans and activities through an extensive surveillance program, employing nearly every intelligence-gathering technique at the Bureau's disposal. Wiretaps, which were initially approved by Attorney General Robert F. Kennedy, were maintained on Dr. King's home telephone from October 1963 until mid-1965; the SCLC headquarter's [sic] telephones were covered by wiretaps for an even longer period. Phones in the homes and offices of some of Dr. King's close advisers were also wiretapped. The FBI has acknowledged 16 occasions on which microphones were hidden in Dr. King's hotel and motel rooms in an "attempt" to obtain information about the "private activities of King and his advisers" for use to "completely discredit" them.[100]

Imagine a dissident like Dr. King living in today's information age. A government (or political opponent) that wanted him silenced might be able to obtain not just access to his telephone conversations, but also to his reading habits and emails. This critic could be blackmailed outright, or he could be discredited by disclosure of the information as an example to others. Perhaps he has not been having an affair, but has some other secret. Maybe he is gay, or has a medical condition, or

---

[99] *See id.*

[100] S. REP. NO. 94-755, at 81 (1976) (quoting Memorandum from Frederick Baumgardner to William Sullivan (Jan. 28, 1964)).

visits embarrassing web sites, or has cheated on his expenses or his taxes. All of us have secrets we would prefer not be made public. Surveillance allows those secrets greater opportunities to come out, and it gives the watchers power that can be used nefariously.

The risk of the improper use of surveillance records persists over time. Most of the former communist states in Eastern Europe have passed laws strictly regulating access to the surveillance files of the communist secret police. The primary purpose of such laws is to prevent the blackmail of political candidates who may have been surveilled under the former regime.[101] The experience of these laws reveals, moreover, that the risk of such blackmail is one that the law cannot completely prevent after the fact. Professor Maria Los explains that "[s]ecret surveillance files are routinely turned into a weapon in political struggles, seriously undermining democratic processes and freedoms."[102]

More recently, the world observed some of the potential of electronic blackmail during the revolutions in the Arab world. Many observers have argued that the turmoil in Tunisia, Libya, and Syria shows the liberating potential of digital technologies.[103] But the crisis also illustrates the potential of modern surveillance technologies, which have been deployed by authoritarian governments across the Middle East. The Libyan government of Colonel Moammar Gadhafi, for example, attempted to capture Internet and phone communications with the assistance of Western technology companies for later review. As one journalist remarked about the availability of such "'massive intercept' technology" to governments around the world, "[t]oday you can run an approximation of *1984* out of a couple of rooms filled with server racks."[104] Using these technologies, the Libyan government obtained information about dissidents that it was able to use to blackmail them into silence. And while the Gadhafi regime did not hesitate to use violence against its critics, it found blackmail and harassment to be even easier tools to use.[105] The fact that the Gadhafi regime ultimately collapsed does not diminish surveillance's blackmail threat.

Even in democratic societies, the blackmail threat of surveillance is a real one. Surveillance (especially secret surveillance) often detects crimes or embarrassing activity beyond or unrelated to its original purposes. The surveillance of Dr. King, for instance, produced evidence of his marital infidelity. In another infamous case, FISA-authorized surveillance of a terrorist suspect produced chilling evi-

---

101 Los, *supra* note 82, at 176–77.

102 *Id.* at 180.

103 *See, e.g.*, Chander, *supra* note 13, at 1508.

104 Matthieu Aikins, *Jamming Tripoli*, WIRED, June 2012, at 146, 176.

105 *Id.*

dence of the suspect's murder of his own daughter for dating the wrong boy.[106] Whether these discoveries are important, incidental, or irrelevant, all of them give greater power to the watcher. Unscrupulous government officials could engage in blackmail, whether motivated by political or pecuniary considerations. But even faithful government agents who discover illegal activity would now possess the weapon of selective prosecution, which could be used to influence the subject, and would be able to wield the threat of mere disclosure of legal but embarrassing activity. Putting the seriousness of the crime to one side, it is important to realize that wide-ranging secret surveillance gives coercive power to the watcher.

B. Persuasion

Surveillance also gives the watcher increased power to persuade. Persuasion is a more subtle exercise of the power differential that can be used to blackmail, but it can be even more effective. Consider again Target's use of Big Data to lure pregnant customers into its stores. Even if the customers have told no one that they are expecting, Big Data analytics can look for correlations between pregnancy and other changes in consumer behavior, for instance, purchasing more vitamins or scent-free lotions. Once an inference of pregnancy is established, Target's marketers can offer coupons to the pregnant woman in order to capture her business, knowing that she is at a point in her life when her buying habits are temporarily in flux before they will lock in for a period of some years. It is entirely possible that such actions by a retailer like Target could occur without the knowledge of the pregnant consumer. Indeed, the science of targeted online or "behavioral" advertising seeks to do exactly that: to market products to consumers based upon detailed profiles collected about their behavior. The effective sales technique of behavioral "retargeting" allows marketers to go one step further and literally follow targeted consumers around the web, delivering the same targeted advertisement to them with enough frequency that they are likely eventually to succumb and make a purchase in a moment of weakness.[107]

Governments also use the power of surveillance to control behavior. For example, one of the justifications for massive closed-circuit television (CCTV) networks in modern urban areas is that they allow police greater ability to watch and influence what happens on city streets.[108] Certainly, the presence of cameras or police can persuade citizens to obey the law, but it can have other effects as well. The surveillance-

---

[106] United States v. Isa, 923 F.2d 1300, 1302 (8th Cir. 1991).
[107] ELI PARISER, THE FILTER BUBBLE 44 (2011).
[108] *See* LYON, *supra* note 6, at 107–08.

studies literature has documented the use of government CCTV assemblages to direct public behavior toward commerce and away from other activities ranging from crime to protest.[109] In Britain, where the science of surveillance-based control is at its most advanced, CCTV operates in connection with court-ordered injunctions, known as Anti-Social Behavior Orders, to move groups of teens out of the commercial cores of cities using surveillance and the power of the state to ensure that commerce continues efficiently.[110] Government use of persuasive surveillance is still in its relative infancy, but since the technologies of surveillance and Big Data analytics are available to the state as well as to private companies, we can imagine the government becoming increasingly able to engage in Target-style persuasion in the future.

The bottom line about surveillance and persuasion is that surveillance gives the watcher information about the watched. That information gives the watcher increased power over the watched that can be used to persuade, influence, or otherwise control them, even if they do not know they are being watched or persuaded. Sometimes this power is arguably a good thing, for example when police are engaged in riot control. But we should not forget that surveillance represents a persuasive power shift whether the watcher is a government agent or a corporate marketer, and whether the target is a rioter or law-abiding citizen. The legal system has rules dealing with power imbalances between consumers and businesses, such as the doctrine of unconscionability and much of consumer protection law. There are also rules protecting citizens from state coercion, such as the unconstitutional conditions doctrine and the First Amendment's protections of freedom of thought and conscience. In our age of surveillance, where technological change has given the watcher enhanced powers of persuasion, it may well be time to think about updating those doctrines to restore the balance.

C. Sorting/Discrimination

Many kinds of surveillance are routinely used to sort people into categories. Some of these forms of sorting are insidious. Consider, for example, the use of census records by the American, Canadian, and German governments during the Second World War to identify citizens to relocate to the Japanese internment camps in North America and the concentration camps in Europe.[111] Others seem innocuous or even benign. The vast preference engines that power the "free" Internet are

---

[109] *See, e.g.*, ROY COLEMAN, RECLAIMING THE STREETS 226–28 (2004); LYON, *supra* note 6, at 107–08; Roy Coleman, *Surveillance in the City: Primary Definition and Urban Spatial Order*, *in* THE SURVEILLANCE STUDIES READER, *supra* note 6, at 231, 234–35.

[110] *See* COLEMAN, *supra* note 109, at 111.

[111] LYON, *supra* note 6, at 30, 32.

used to profile Internet users for marketing purposes. Companies like Google amass vast detailed profiles of our web-surfing habits, our interests, and our buying habits.[112] Data brokers like Acxiom and LexisNexis create even more detailed consumer profiles by combining various kinds of data and sell the data to a wide variety of sources, including direct marketers, background-check companies, and companies consumers may already have a relationship with, such as car dealers or Target.[113] Commercial data of this kind can be used to offer discounts or selective promotions to more or less desirable customers.

The sorting power of surveillance is a major theme among surveillance scholars. In the 1990s, sociologist Oscar Gandy described the "panoptic sort": the use of consumer databases to profile consumers, sort them into categories, and then discriminate among the categories, allocating opportunities on the basis of the classification.[114] More recently, Lyon and other scholars have built on Gandy's work to show the ways in which software is increasingly used to sort citizens and consumers by governments seeking profiles of criminal risk and by companies seeking profiles of commercial opportunity.[115]

From one perspective, the use of the fruits of data surveillance in this way might look like ordinary marketing. But consider the power that data-driven marketing gives companies in relation to their customers. The power of sorting can bleed imperceptibly into the power of discrimination. A coupon for a frequent shopper might seem innocuous, but consider the power to offer shorter airport security lines (and less onerous procedures) to rich frequent fliers, or to discriminate against customers or citizens on the basis of wealth, geography, gender, race, or ethnicity. The power to treat people differently is a dangerous one, as our many legal rules in the areas of fair credit, civil rights, and constitutional law recognize. Surveillance, especially when fuelled by Big Data, puts pressure on those laws and threatens to upend the basic power balance on which our consumer protection and constitutional laws operate. As Professor Danielle Citron argues, algorithmic decisionmaking based on data raises issues of "technological due process."[116] The sorting power of surveillance only raises the stakes of these issues. After all, what sociologists call "sorting" has many other

---

[112] LEVY, *supra* note 18, at 336–37, 341.

[113] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 917–18 (2008).

[114] OSCAR H. GANDY, JR., THE PANOPTIC SORT 15 (1993).

[115] *See generally* JOHN GILLIOM, OVERSEERS OF THE POOR (2006); DAVID LYON, SURVEILLANCE AFTER SEPTEMBER 11 (2003); THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY (Kevin D. Haggerty & Richard V. Ericson eds., 2006); SURVEILLANCE AS SOCIAL SORTING (David Lyon ed., 2003).

[116] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258 (2008).

names in the law, with "profiling" and "discrimination" being just two of them.

IV. LIMITING SURVEILLANCE

These insights into the ways in which surveillance is harmful point toward identifying remedies that can be built into law, technologies, and social norms to deter the most dangerous forms of surveillance. In this section, I outline four principles that we should use to guide the treatment of surveillance. My purpose is not to propose neat doctrinal fixes to existing law; as I have shown already, the age of surveillance raises massive challenges that will require us to think creatively about how to capture its benefits without sacrificing important civil liberties. Instead, my purpose is to identify some of the values that the law of surveillance ought to protect and the principles that should guide its evolution.

A. Surveillance Transcends the Public/Private Divide

One of the most significant changes that the age of surveillance has brought about is the increasing difficulty of separating surveillance by governments from that by commercial entities. Public- and private-sector surveillance are intertwined — they use the same technologies and techniques, they operate through a variety of public/private partnerships, and their digital fruits can easily cross the public/private divide. It is probably in this respect that our existing models for understanding surveillance — such as Big Brother and the Panopticon — are the most out of date. Even if we are primarily worried about state surveillance, perhaps because we fear the state's powers of criminal enforcement, our solutions to the problem of surveillance can no longer be confined to regulation of government actors. Any solutions to the problem of surveillance must thus take into account private surveillance as well as public.

In this respect, Professor Orin Kerr is correct when he argues that federal statutory law has advantages over the Fourth Amendment in guarding against surveillance in the digital age.[117] Not only is statutory law easier to change, but it also can be applied to bind both government and nongovernment actors. A good model in this context is the federal ECPA and its state-law equivalents. These laws prohibit wiretapping by private actors and require the government to obtain a warrant under a standard higher than probable cause before it can engage in wiretapping.[118] ECPA has many defects, both in terms of the

---

[117] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806–08 (2004).

[118] 18 U.S.C. § 2516 (2006).

level of protection it offers and in its often-bewildering complexity, but in transcending the public/private divide, it represents a good model for dealing with surveillance.

Additional legal protections will be needed to cope with developments in surveillance practices. Because the government can sidestep many legal restrictions on the collection of data by buying it from private databases, we should place additional restrictions on this growing form of state surveillance. Such regulations could operate in both directions. In relation to government, we could place restrictions both on the government's ability to buy private databases and on its ability to share personal information with the private sector. Privacy law already has numerous models for this latter category, ranging from the Driver's Privacy Protection Act of 1994,[119] which limits the government's ability to sell drivers' license records to industry, to the Privacy Act of 1974,[120] which prevents the government from disclosing many kinds of records about individuals that it has in its possession. In relation to private actors, we can place special obligations of confidentiality upon the holders of personal information related to intellectual privacy, treating them as information fiduciaries. Our law has long had a tradition of confidentiality rules, placing nondisclosure obligations on lawyers, doctors, trustees, librarians, and other information custodians.[121] On the Internet, many companies already promise not to share personal information with governments unless compelled. It would be but a small step to make such promises the default, or even the mandatory practice, for certain kinds of particularly sensitive information.[122]

B. Secret Surveillance Is Illegitimate

Democratic societies should prohibit the creation of any domestic-surveillance programs whose existence is secret. In a democratic society, the people, and not the state apparatus, are sovereign. In American law, this tradition goes back to James Madison, and it lies at the very heart of both First Amendment theory and American constitutionalism itself.[123] These principles are reflected at the core of modern information law. For example, the Supreme Court has made clear that the

---

[119] 18 U.S.C. §§ 2721–2725 (2006).

[120] 5 U.S.C. § 552a (2006).

[121] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 134–40 (2007).

[122] Richards, *The Perils of Social Reading*, *supra* note 20, at 692.

[123] *Madison's Report on the Virginia Resolutions (1789–1800)*, *in* 4 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 546, 553–76 (Jonathan Elliot ed., Philadelphia, J.B. Lippincott Co. 2d ed. 1891).

federal Freedom of Information Act[124] protects at its core the "citizens' right to be informed about 'what their government is up to.'"[125] As Professor Henry Steele Commager put it aptly, "[t]he generation that made the nation thought secrecy in government [to be] one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to."[126]

The illegitimacy of secret surveillance also lies at the heart of information-privacy law, which remains guided by the "Fair Information Practices" drafted by the U.S. Department of Health, Education, and Welfare in 1973.[127] The Code of Fair Information Practices recommended by the Department has continued to influence information-privacy law throughout the world,[128] and the first of its five principles is the commitment that "there must be no personal-data record-keeping systems whose very existence is secret."[129]

Requiring the existence of domestic-surveillance programs to be disclosed solves a practical problem that has bedeviled courts trying to assess legal challenges to secret surveillance programs. How can plaintiffs prove injury if the government is not required to admit whether surveillance exists in the first place? A prohibition on secret surveillance programs solves this problem. When government programs are public — when we have no secret surveillance — courts will be able to assess their legality in the open. The NSA wiretapping program was hard to challenge because its details were shrouded in secrecy, denials, and unassessable invocations of national security interests.[130] At the same time, its shadowy nature created an even greater threat to intellectual privacy in particular because no one knew if her telephone calls were being listened to or not. Requiring disclosure of the existence and capabilities of domestic-surveillance programs to the general public makes them amenable to judicial and public scrutiny to ensure their compatibility with the rule of law. At the same time, the prohibition on secret surveillance *systems* does not require the government to notify *individual targets* of surveillance that they are being

---

124 5 U.S.C. § 552 (2006 & Supp. V 2011).

125 U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773 (1989) (quoting EPA v. Mink, 410 U.S. 73, 105 (1973)).

126 Henry Steele Commager, *The Defeat of America*, N.Y. REV. BOOKS, Oct. 5, 1972, at 7, 7 (reviewing RICHARD J. BARNET, ROOTS OF WAR (1972)).

127 U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

128 LAWRENCE LESSIG, CODE: VERSION 2.0, at 227 (2006); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 130 (2008).

129 U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 127, at 41; *see also id.* 29–30, 41–42.

130 *See In re* NSA Telecomm. Record Litig., 671 F.3d 881, 893 (9th Cir. 2011).

watched. But fundamentally, surveillance requires legal process and the involvement of the judiciary to ensure that surveillance is targeted, justified, and no more extensive than is necessary.

Thus, while covert domestic surveillance can be justified in discrete (and temporary) instances when there is advance judicial process, blanket surveillance of all Internet activity menaces our intellectual privacy and gives the government too much power to blackmail or discriminate against the subjects of surveillance. In a free society, all forms of surveillance must be ultimately accountable to a self-governing public, and for this reason, secret domestic-surveillance programs of any kind are illegitimate.

C. Total Surveillance Is Illegitimate

Democratic societies should also reject the idea that it is reasonable for the government to record all Internet and telephone activity with or without authorization. Government surveillance of the Internet is a power with the potential for massive abuse, as the (thankfully) failed attempts by the Gadhafi regime illustrated.[131] Like its precursor, telephone wiretapping, Internet surveillance must be subjected to meaningful judicial process before it is authorized. And such authorization must allow only discrete and limited forms of surveillance. Otherwise, there would be no constraint on the government's ability to record and archive all electronic communications and read them at its leisure. The magnitude of technological change should not blind us to the important values that our law has protected for decades: the importance of private communications, intellectual privacy, and unfettered intellectual exploration. Moreover, a world of total surveillance would be one in which the power dangers of surveillance are even more menacing. In such a world, watchers would have increased power to blackmail, selectively prosecute, coerce, persuade, and sort individuals. A world of total surveillance is not just science fiction. It is the world toward which we are slowly creeping, as software is coded, databases are combined, and each CCTV camera is successively added to the network.

Rather than jettisoning longstanding civil liberties in our brave new digital world, we should instead follow the example of federal wiretapping law, which for decades has rested on the premise that private communications should be exactly that, shielded from the government (and other private actors) except in cases of proven law-enforcement need for limited access to those communications. Such a regime is a far cry from the security-driven argument for total surveillance, even in an age of terror.

---

[131] *See generally* Aikins, *supra* note 104.

D. Surveillance Is Harmful

As Parts II and III of this Article demonstrate, many forms of surveillance — covert and overt, public and private — menace our intellectual privacy and the processes of belief formation on which a free society depends. They also create a power imbalance between the watcher and the watched that creates risks of blackmail, undue persuasion, and discrimination. Courts and legislatures should therefore scrutinize any surveillance that threatens these values. But because of its relationship to First Amendment values and political freedom, surveillance of intellectual records — Internet search histories, email, web traffic, and telephone communications — is particularly harmful. In practice, this means that surveillance by government that seeks access to intellectual records should be subjected to a high threshold before a warrant can issue. A good model for this rule is Title I of the ECPA, which provides for a more stringent procedure under federal wiretapping law before a warrant may issue to intercept the contents of a telephone or electronic communication.[132] The ECPA requires more than just the standard probable cause requirement that is the constitutional floor under Fourth Amendment law. In addition to probable cause, government agents seeking to tap a phone or electronic communication must also show three other elements: (1) that the warrant is sought for a limited time, (2) that the interception of the communication is necessary to obtain the information sought, and (3) that the wiretapping will be conducted in such a way as to minimize the interception of information not relevant to the warrant.[133] These "super-warrant" protections for communications should be expanded to cover the full range of intellectual records.

For private-sector surveillance, additional statutory procedures are necessary to ensure that intellectual records are handled with greater care by the entities that hold them. We already have piecemeal protections for intellectual privacy against private-sector surveillance, which could serve as useful models for the extension of intellectual-privacy protection more broadly.[134] For example, the ECPA prohibition against warrantless wiretapping applies to private actors as well.[135] The Act makes private acts of wiretapping illegal, providing severe criminal and civil liability — up to five years in prison[136] and fines or

---

[132] 18 U.S.C. § 2518 (2006).

[133] *See id.*; *see also* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1554 (2010).

[134] For an expanded treatment of this argument in the context of reading records, see generally Richards, *The Perils of Social Reading*, *supra* note 20.

[135] 18 U.S.C. § 2511 ("any person").

[136] *Id.* § 2511(4)(a).

tort liability of $10,000 for each violation of the Act.[137] Other good models for intellectual-privacy protection in the private sector include the confidentiality obligations placed on video-rental companies by the Video Privacy Protection Act of 1988,[138] on librarians by the vast number of library-records confidentiality laws, and on print and electronic booksellers in California under its Reader Privacy Act.[139]

Because surveillance of intellectual activities menaces self-government, our law must also recognize it as a harm in standing doctrine. One of the difficulties that courts have faced in dealing with surveillance in the past is an inability to articulate exactly why surveillance is harmful. This inability was the problem in *Laird* and also in the NSA wiretapping cases. Contrary to the trend of the law, *Amnesty International USA v. Clapper*[140] held that amendments to the Foreign Intelligence Surveillance Act that authorized the NSA wiretapping program actually *could* cause a legally cognizable injury to journalists, lawyers, and aid workers whose communications with overseas clients might be subjected to surveillance by the United States government.[141] But even that outlier case, which the Supreme Court reversed on appeal, failed to recognize that a reasonable fear of government surveillance threatens the privacy of the surveilled, causing them to act differently. The Second Circuit found standing but rested its conclusions instead upon injury to the professional duties of the doctors and lawyers who feared that the government was listening. The professional duties of the plaintiffs in *Clapper* are important, and the Second Circuit was correct to recognize injuries to those duties as harms under standing doctrine. But on its own terms, even the Second Circuit seemed to suggest that only professional elites have standing to challenge surveillance. Such a conclusion is underprotective of the rights of all people to be free from unlawful surveillance and to be able to challenge unlawful surveillance in court. As I have argued, intellectual privacy is not just for intellectuals. If the government is engaged in unwarranted surveillance of a person's intellectual activities, that person should have standing to challenge the legality of the surveillance. The surveillance may or may not turn out to be warranted in each particular case, but our society's fundamental commitments to due process, freedom of the mind, and the rule of law suggest that such dangerous surveillance should be subject to legal challenge.

Intellectual-privacy theory thus corrects the errors of *Clapper*, *Laird*, and the NSA cases. It would extend protection from surveil-

---

137 *Id.* § 2520(2)(B).
138 18 U.S.C. § 2710 (2006).
139 CAL. CIV. CODE § 1798.90.05 (West 2012).
140 638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013).
141 *Id.* at 121–22.

lance to all people, and not just to professional elites. It explains why surveillance of reading, thinking, and private communication harms the development of ideas and beliefs unfettered by the skewing effects of observation. Accordingly, a reasonable fear of government surveillance that affects the subject's intellectual activities (reading, thinking, and communicating) should be recognized as a harm sufficient to prove an injury in fact under standing doctrine. Such a change to our law would not be a radical one; in fact, it is precisely the way courts currently assess challenges to individual free speech rights under the First Amendment's chilling-effects doctrine. Since intellectual privacy protects, at heart, First Amendment values, it is appropriate to extend these existing and workable doctrinal tools to this related area of the law.

This is not to say that individual determinations of the chilling of intellectual activities will always be easy. Determining whether a chill to intellectual privacy is substantial would certainly present difficult cases at the margins. In our law, the devil is frequently in the details. But as the chilling-effects doctrine has demonstrated, courts have managed to balance threats to free speech against competing government interests. Moreover, because the general details of government surveillance programs should be public, courts and litigants will have more information with which to assess the effects of surveillance. And even when publication of the details of surveillance might threaten ongoing investigations, such details could be released either under seal to the litigants or shared with the court. Courts have a wide variety of tools to manage the flow of confidential information that litigation inevitably produces, and they would be well suited to such a task. Such tasks may be difficult and require judgment, but that is the job of courts. The alternative to grappling with the civil-liberties threats that surveillance poses is to ignore those threats altogether, to face the prospect of rendering widespread government surveillance unreviewable and uncheckable. Democratic societies can do better than that.

V. CONCLUSION

The challenge to our law posed by the Age of Surveillance is immense. The justifications for surveillance by public and private actors are significant, but so too are the costs that the rising tide of unfettered surveillance is creating. Surveillance can sometimes be necessary, even helpful. But unconstrained surveillance, especially of our intellectual activities, threatens a cognitive revolution that cuts at the core of the freedom of the mind that our political institutions presuppose. Therefore, surveillance must be constrained by legal and social rules. The technological, economic, and geopolitical changes of the past twenty years have whittled away at those rules, both formally on their substance (for example, the Patriot Act and the expansion of National Se-

curity Letter jurisdiction) and in practice (for example, the pressure that the technological social practices of the Internet have exerted on privacy). By thus recognizing the harms of surveillance and crafting our laws accordingly, we can obtain many of its benefits without sacrificing our vital civil liberties or upending the power balance between individuals on the one hand and companies and governments on the other.