A TWENTY-FIRST CENTURY FRAMEWORK FOR DIGITAL PRIVACY

WHITE PAPER SERIES

Secret Government Searches and Digital Civil Liberties

NEIL RICHARDS

NATIONAL CONSTITUTION CENTER

Secret Government Searches and Digital Civil Liberties

By Neil Richards*

Perhaps surprisingly, the most compelling moment in Oliver Stone's "Snowden" biopic is the sex scene. Halfway through this movie about government surveillance and whistleblowing, the audience is shown a graphic and seemingly gratuitous sexual encounter involving Edward Snowden (played by Joseph Gordon Levitt) and his girlfriend Lindsay Mills (played by Shailene Woodley). In the midst of their passion, Snowden's eyes rest on Lindsay's open laptop, the empty eye of its camera gazing towards them. In a flash, he recalls an earlier event in which NSA contractors hacked laptop cameras to secretly spy on surveillance subjects in real time. Edward and Lindsay's mood was ruined, to say the least, by the prospect of government agents secretly watching their intimate activities.

The scene evokes George Orwell's famous warning about telescreens, the omnipresent surveillance devices in Big Brother's Oceania, by which the Thought Police could secretly watch anyone at any time.[1] It also has grounding in reality. The use of millions of hacked webcams as monitoring devices was a program known as "Optic Nerve," which was part of the Snowden revelations.[2] Another program leaked by Snowden involved the surveillance of the pornography preferences of jihadi radicalizers (including at least one "U.S. person"), with the intention being the exposure of their sexual fantasies to discredit them in the Muslim world.[3] Snowden himself famously appeared on John Oliver's HBO show "Last Week Tonight," humorously but effectively reducing unchecked government surveillance to the basic proposition that secret surveillance allowed the government, among other things, to "get your dick pics."[4]

---

* Thomas & Karole Green Professor of Law, Washington University School of Law; Affiliate Scholar, The Center for Internet and Society at Stanford Law School; Affiliated Fellow, Yale Information Society Project. Many thanks to Danielle Citron and Woody Hartzog for their comments on earlier drafts.

[1] GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949) ("The telescreen received and transmitted simultaneously. Any sound Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever the wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.").

[2] Spencer Ackerman & James Ball, *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*, THE GUARDIAN (Feb. 28, 2014), https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

[3] Glenn Greenwald, Ryan Grim & Ryan Gallagher, *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'*, HUFFINGTON POST (Nov. 26, 2013), http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html; Max Ehrenfreund, *NSA reportedly monitored pornography viewed by suspected Islamists*, WASH. POST. (Nov. 27, 2013), https://www.washingtonpost.com/world/national-security/nsa-reportedly-monitored-pornography-viewed-by-suspected-islamists/2013/11/27/5f4eac64-5778-11e3-ba82-16ed03681809_story.html.

[4] Emily Dreyfuss, *On John Oliver, Edward Snowden Says Keep Taking Dick Pics*, WIRED (Apr. 6, 2016), https://www.wired.com/2015/04/john-oliver-edward-snowden-dick-pics/.

Sexual surveillance may get our attention, but in our digital networked society, in which many of our documents are stored in the cloud, secret government surveillance powers are vastly broader than the power to be an electronic Peeping Tom. Today, the U.S. government has a wide variety of means of secretly watching and searching the people who live in the United States, whether they are citizens, permanent residents, or visitors.

How did we get to a place where secret government surveillance seems both omnipresent and unavoidable? It may be hard to believe these days, but when the Internet first jumped into the public consciousness in the mid-1990s, it was touted as a realm of anarchy and personal empowerment, a tool of freedom rather than of oppression.[5] At the time, the specter of always-on secret surveillance was unthinkable for a variety of technical, political, and legal reasons. Such surveillance was *technologically* impossible in a pre-broadband world of modems and computers that were usually not connected to the network and in which the Cloud was a dream of technologists and science fiction writers. It was *practically* impossible, because of the high costs of in-person surveillance. It was *politically* impossible, too, with many politicians having first-hand memory of the totalitarian regimes of the Axis Powers. *Legally*, too, the law was settled that the government needed to get a warrant before it tapped a phone, searched papers, or intercepted an email.

How times have changed. These well-established technical and political roadblocks to widespread secret surveillance vanished rapidly in the early months of the twenty-first century. When Al Qaeda terrorists turned four commercial airlines into missiles and attacked New York and Washington, D.C. in September 2001, a stunned American President without a strong commitment to civil liberties began to authorize unprecedented levels of digital surveillance. From a technological perspective, the attacks occurred just after the mass adoption of the Internet, and just before the social media and smartphone phases of the digital revolution. These advances and adoptions, running on a stream of previously uncollected personal data, made it technically possible for the government to read a person's emails or documents stored in the cloud, or obtain a minutely-detailed transcript of their location logged from the GPS chip in their phone. At the same time, these new technologies started to blur the lines between public and private, destabilizing settled legal understandings of the boundaries between what was private and what was not. In this environment, law enforcement often took the position that in doing their job of promoting security, it was better to ask for forgiveness than permission in attacking the newly-available digital evidence.

Yet despite the growth of the surveillance-industrial complex,[6] there are hopeful signs. Apple and Microsoft, among other technology companies, have engaged in high-profile litigation with the federal government on behalf of their users' privacy, including litigation over the security of iPhones and the government's ability to place gag orders on its searches of Microsoft's cloud and email services.[7]

---

[5] EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (2012).

[6] Here I borrow Jay Stanley's helpful term. *See* Jay Stanley, *The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*, ACLU Report (2004), https://www.aclu.org/sites/default/files/FilesPDFs/surveillance_report.pdf.

[7] In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Calif. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016). Microsoft

The result of these changes is the rise of a phenomenon I shall call the "secret government search." This is, as the name suggests, a search by law enforcement of information relating to an individual. Secret government searches can be diverse—they can be physical or increasingly digital; they can be executed under a warrant, under no warrant, or under some intermediate authorization; they can be unknown to all, or served on a trusted digital service accompanied by an injunction forbidding notice to the target; and the target may get delayed notice of the search or no notice ever. Different kinds of secret government searches can raise different problems, and these problems may require different solutions. But at bottom, secret government searches share the essential characteristic of being government surveillance of which the target has no notice at the time of the search.

In this essay, I attempt to put the rise of secret government searches into context—historical, technological, and most importantly constitutional. My argument is straightforward—the current state of secret government searches is a dangerous anomaly in our democratic order. It is unprecedented as a technological and historical matter, and it is inconsistent with what I believe is the best reading of our constitutional traditions protecting freedom of thought, freedom of expression, and freedom from unreasonable searches and seizures. If we are to faithfully translate our hard-won civil liberties against the state from the physical realm to the digital, we need to do better to limit the ability of the government to peer into the lives of its citizens in ways that are not only secret but also relatively unconstrained. It is important to recognize, however, that this is not a question of civil liberties "in cyberspace," as if the digital realm is somehow a separate one. While the fiction of separate physical and virtual worlds may have been a useful one twenty years ago, in today's networked, mobile era of ubiquitous personal computers, the overwhelming majority of ordinary people use digital platforms and technologies to live their everyday lives. Recognition of this fact must also cause us to recognize that there is not really any such place as "cyberspace." On the contrary, there is only space, and humans in that space trying to live their lives—sometimes using digital tools, sometimes using pre-digital ones, and frequently using a combination of the two.[8] Yet if we fail to fully extend our hard-won rights in traditional activities to digital, networked activities, those rights will be substantially and perhaps even fatally diminished. If that were to happen, we would all be less safe as a result.

This argument proceeds in four steps. First, I will describe the lay of the land with respect to secret government searches, a phenomenon I term "the secret search epidemic." I argue that it is impossible to fully understand the constitutional issues these searches raise without an appreciation of the essential technical and other roles played by the technology companies whose businesses enable the creation of this data in the first place. Second, I examine these secret searches as "searches," and consider them from the perspective of Fourth Amendment law. This focuses our attention on the "search" part of secret government searches. I argue that the best reading of the Fourth Amendment in this context is that secret searches are unreasonable, and that if we permit them, we risk repeating the mistakes of the past with respect to the Fourth Amendment and new technologies. Third, I consider whether secret searches are a threat to First

---

Corp. v. United States, No. 14-2985-cv (2d Cir. 2016); Microsoft Corp. v. United States Dep't of Justice, et al., 2016 WL 1464273 (W.D. Wash. 2016).

[8] For a similar argument, *see* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007).

Amendment values, either by virtue of their secrecy or by the fact that in the digital context they are often served on cloud providers and accompanied by injunctions forbidding those companies to ever tell their customers about the government's accessing their data. I conclude that secret, unconstrained searches of this kind represent a serious threat to our First Amendment values. Finally, I chart a path forward for secret surveillance law, offering four principles that should govern the delicate task of translating our civil liberties into the digital society.

I. THE SECRET SEARCH EPIDEMIC

Debates over government digital surveillance have raged in the United States since 2001, but particularly since the Snowden revelations of 2013. A central issue in these debates concerns the extent to which government surveillance is either enabled or hindered by the advent of digital technology. One school of thought, championed by law enforcement, is that digital technologies are racing ahead of government abilities to monitor them, and that consequently, law enforcement's crime detection abilities are "going dark." In a 2014 address, FBI Director James Comey explained that with the advent of digital technologies:

> Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[9]

An alternative perspective is offered by law professor Peter Swire, a member of the Review Group on Intelligence and Communications Technology, commissioned by President Obama to review American surveillance practices in the aftermath of Snowden's leaks. Swire argued on the contrary that even though technology was making some forms of government surveillance more challenging,

> it is more accurate to say that we are in a 'Golden Age of Surveillance' than for law enforcement to assert that it is 'Going Dark.' . . . [T]here are indeed specific ways that law enforcement and national security agencies lose specific previous capabilities due to changing encryption technology. These specific losses, however, are more than offset by massive gains, including: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create digital dossiers about individuals' lives.[10]

On balance, Swire's argument seems the more persuasive reading of what has happened to government surveillance power in the Internet era. Despite encryption having made the

---

[9] James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[10] Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, Testimony of Peter Swire, Senate Judiciary Committee (July 8, 2015), http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

government's job difficult in some respects, many of the forms of communication and kinds of data sought by the government simply did not exist in an analog era. By opening vast chunks of human activity up to digital measurement and potentially access, the digital revolution has created at least the potential for scrutiny of human life in ways never before possible. And this potential government scrutiny of our lives could also occur in ways that are unknown to us while it is happening.

Some of the tools for this kind of surveillance already exist, and are being used tens of thousands of times each year to engage in secret searches. The federal government, for example, has substantial powers to engage in secret surveillance of communications and other data held by trusted intermediaries, usually technology companies. Unlike an old-fashioned physical search of a home for letters, demands placed on these trusted intermediaries are much easier to conceal. While it is difficult for the government to search a home for letters, diaries, or other documents without the homeowner noticing, it is much easier for it to secretly access digital communications. In addition, unlike paper communications records, which are physical and hard to copy or remove secretly, electronic records by their nature facilitate the making of unlimited perfect copies with ease.

Beyond their unobtrusive nature, digital searches by the government can offer a second kind of secrecy, which is enforced silence. When the government obtains personal information from technology companies or other organizations with relationships to its search targets, it is often able to place an injunction on the company, ordering them to keep quiet upon penalty of legal action. These powers include the Foreign Intelligence Surveillance Act,[11] the Electronic Communications Privacy Act,[12] and its power under several laws to issue National Security Letters.[13] Although these powers are not known by most people, they are invoked with an astonishing frequency. For example, Facebook reported that in the last six months of 2015 in the United States alone, it received 19,235 requests from law enforcement for data on 30,041 users, and produced data in over 80% of those cases.[14] Other large technology companies report similarly large numbers. Of course, the existence of these transparency reports is a hard-won victory for transparency over silence. But the fact remains that transparency reports are voluntary reports made by a small number of companies, they vary in their scope and specificity, and they report aggregate data rather than specifics.

Beyond these forms of surveillance, many other new avenues of surveillance are available for the government, often without much legal oversight. These technologies can be unobtrusive, secret, or both. For example, social media monitoring technologies are being used

---

[11] 15 U.S.C. § 1801.
[12] 18 U.S.C. § 2703; 2705(b).
[13] There are four federal statutes that allow NSLs: the Electronic Communications Privacy Act (18 U.S.C. § 2709), the National Security Act (50 U.S.C. § 3162), the Right to Financial Privacy Act (12 U.S.C. § 3414), and the Fair Credit Reporting Act (15 U.S.C. § 1681), with significant amendments added by the USA PATRIOT Act (Section 505, P.L. 107-56, 115 Stat. 365-66 (2001)), and the USA Patriot Act Reauthorization of 2006 (P.L. 109-178, 120 Stat. 278 (2006)). *See generally* Electronic Frontier Foundation, *National Security Letters: FAQ*, https://www.eff.org/issues/national-security-letters/faq#38.
[14] *Facebook Transparency Report: United States* (July 2015—Dec. 2015), https://govtrequests.facebook.com/country/United%20States/2015-H2/.

to profile "Black Lives Matter" and other political dissenters based upon their public- or semi-public expression.[15] Automatic license plate readers can create detailed maps over time of which cars go down a street and when, and can be used to build highly-detailed databases of the movement of vast numbers of people in cars.[16] Smartphone microphones and cameras can be hacked in order to turn them into individual bugging devices.[17] And new technologies that are just around the corner will create even more data, even more surveillance, and even more potential for incursions into civil liberties or other forms of abuse. For example, as cars become ever more digital and ever less mechanical, microphone-equipped "connected cars" and self-driving cars will offer enormous potential as surveillance tools against their owners.[18] Voice-activated televisions and other home "Internet of Things" appliances will offer similar potential.[19] A little further down the road, mixed- and augmented-reality devices like the Microsoft HoloLens and Magic Leap will enable the projection of virtual information, objects, and content in physical spaces. In order to do that, they will need to create a comprehensive computer model of the entire world. As an otherwise enthusiastic editor from *Wired* Magazine noted in a cover story on these technologies:

> This comprehensive tracking of your behavior inside these worlds could be used to sell you things, to redirect your attention, to compile a history of your interests, to persuade you subliminally, to quantify your actions for self-improvement, to personalize the next scene, and so on. If a smartphone is a surveillance device we voluntarily carry in our pocket, then VR will be a total surveillance state we voluntarily enter.[20]

Inevitably, the government will assert that all of these records are obtainable under its secret search powers as well.

Searches of digital records create additional problems in addition to the ease of searching and copying they provide. Two of these problems are particularly worthy of note. First, an important check on police surveillance in the past has not been the law but non-legal considerations. Indeed, the Supreme Court has recognized that the government's ability to abuse

---

[15] *E.g.*, Nicole Ozer, *Police use of social media surveillance software is escalating, and activists are in the digital crosshairs*, ACLU of Northern California Medium.com, https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48#.ofibui9jq; Craig Timberg & Elizabeth Dwoskin, *Facebook, Twitter and Instagram sent feeds that helped police track minorities in Ferguson and* Baltimore, report says, WASH. POST. (Oct. 11, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/?wpisrc=al_alert-COMBO-econ%252Btech.

[16] *E.g.*, American Civil Liberties Union, *You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements* (July 2013); Cyrus Farivar, *We know where you've been: Ars acquires 4.6M license plate scans from the cops*, ARS TECHNICA (March 24, 2015), http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/.

[17] Declan McCullagh, *FBI taps cell phone mic as eavesdropping tool*, CNET (Dec. 4, 2006), https://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/.

[18] Camille Francois, *Self-Driving Cars Will Turn Surveillance Woes into a Mainstream Issue*, WIRED (May 30, 2014), https://www.wired.com/2014/05/self-driving-cars-will-turn-surveillance-woes-into-a-mainstream-issue/.

[19] *E.g.*, David Goldman, *Your Samsung TV Is Eavesdropping on Your Private Conversations*, CNN.com (Feb. 10, 2015), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html.

[20] Kevin Kelly, *The Untold Story of Magic Leap, The World's Most Secretive Startup*, WIRED (May 2016), https://www.wired.com/2016/04/magic-leap-vr/.

its surveillance powers have been traditionally limited by non-legal considerations, including "limited police resources and community hostility" to such practices.[21] Secret digital searches substantially eliminate the power of these non-legal checks; it is hard to be hostile to or resist something one knows nothing about, and digital searches can search thousands or even millions of records in bulk in a way that would be impossible for a physical search. In this way, secret digital searches substantially change the power of law enforcement relative to the citizens on whose behalf they work.

Second, in secret search cases, the government frequently argues that information held by "third parties" other than the suspect are unprotected by the Fourth Amendment. This argument rests upon a broad reading of two Supreme Court cases from the 1970s involving bank and telephone records.[22] These cases have been read to suggest that information voluntarily turned over to a "third party" loses a reasonable expectation of privacy and thus can be obtained by the government without a search warrant. In the paper records world of the 1970s, such a doctrine might have made some sense, especially when the contents of telephone calls and paper letters were fully protected by Fourth Amendment doctrine.[23] As a result, a broad reading of the third-party doctrine suggests that anything shared with anyone else loses Fourth Amendment protection. (This is not to suggest that emails are *completely* unprotected, as the government must generally get a warrant to obtain the contents of emails in flight or stored for less than six months under the federal Electronic Communications Privacy Act.[24]) Yet in our digital, cloud-connected world, virtually everything electronic is shared with someone else, as we entrust our information with technological intermediaries like Internet Service Providers, phone companies, email services, social networks, and cloud storage companies so that they can perform their services for us. Moreover, from a technological perspective, essentially all of this information—even emails—is technologically indistinct from business records.[25]

Perhaps unsurprisingly, the third-party doctrine has been controversial. It has almost universally been condemned by scholars,[26] and its broad implications have never been fully

---

[21] Illinois v. Lidster, 540 U.S. 419, 426 (2004).
[22] United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).
[23] Ex Parte Jackson, 96 U.S. 727, 732–33 (1877) (requiring a warrant before the government may open letters in the possession of the postal service); Katz v. United States, 389 U.S. 347 (1967) (requiring a warrant before the government listens to a telephone call).
[24] 18 U.S.C. § 2501 et seq.
[25] Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, HARV. J. L. & TECH. (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2791646.
[26] *E.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 4 (2007); Erin Murphy, *The Case Against the Case for the Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1241 (2009); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 66 (2007); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 110 (2011); Jay Stanley, *The Crises in Fourth Amendment Jurisprudence*, AM. CONST. SOC'Y FOR L. & POL. 4 (2011), https://www.acslaw.org/publications/issue-briefs/the-crisis-in-fourth-amendment-jurisprudence-0; Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011). *But see* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009); Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 4:20 AM),

endorsed by the Supreme Court. Although the federal government maintained in a number of criminal prosecutions that emails held by an Internet Service Provider were subject to the third-party doctrine, a federal appeals court squarely rejected that argument in 2010, holding that emails (like phone calls and paper mail) were protected by the Fourth Amendment and that their owners were entitled to a reasonable expectation of privacy.[27] In recent cases, the Supreme Court has begun to extend the Fourth Amendment to protect against technologically-enabled searches of homes, cars, and mobile phones.[28] In one of these, the location-tracking case of *United States v. Jones*, Justice Sotomayor expressed grave dismay at the broad reading of the third-party doctrine, explaining that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[29] Noting that this information included books read, emails sent, and the phone numbers dialed, she doubted whether, in determining expectations of privacy,

> that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[30]

However, until the Supreme Court takes a third-party doctrine case and either clarifies the law or squarely rejects the doctrine for personal data entrusted to digital intermediaries, there remains an enormous potential for mischief and the erosion of digital civil liberties. Lacking guidance from the Supreme Court, federal courts face the difficult prospect of justifying why specific kinds of personal data held by companies warrants Fourth Amendment protection. In these criminal cases, courts are understandably reluctant to hold that all such data is protected by the Fourth Amendment, and the government can frequently obtain personal information without a warrant. Thus, in the recent case of *United States v. Graham*, the Fourth Circuit held that location data in the possession of a phone company did not require a warrant before it was obtained by the police.[31]

From this perspective, we can see more clearly the context within which the problem of secret government surveillance must be understood. But many questions still remain. The

---

http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

[27] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[28] *E.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (homes); United States v. Jones, 132 S.Ct. 945 (2012) (cars); Riley v. California, 573 U.S. ___ (2014) (smartphones).

[29] *Jones,* 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[30] *Id*. For a thoughtful reading of *Jones* and *Riley* along similar lines*, see* Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73 (2014), http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud.

[31] United States v. Graham, 796 F.3d 332, 354 (4th Cir.), reh'g en banc granted, 624 F. App'x 75 (4th Cir. 2015).

challenge for the law and for lawyers, as is often the case in occasions of legal disruption, is to understand the best way to frame this issue in legal terms. Unfortunately, the problem of secret searches does not easily map onto existing legal structures. Technology has both enabled new forms of surveillance that are invisible to those being watched and destabilized the legal foundations on which those forms of surveillance have traditionally been assessed.[32] While most observers agree that the law has failed to keep up with technology, they differ (as the "Going Dark"/"Golden Age of Surveillance" example illustrates) about how to understand the nature of the problem, and thus how to fix it.

II. SECRET SEARCHES AS SEARCHES

The traditional way of understanding government searches is through the Fourth Amendment's guarantee against unreasonable searches and seizures. From this perspective, secret searches raise a number of issues, but two are most important—the ways in which Fourth Amendment law has been adapted to new technological advances in general, and the specific substantive rules governing so-called "sneak and peek searches."

A. The Fourth Amendment and Technology

As we have already seen, government surveillance techniques that allow secret access to digital files have destabilized the legal foundations of Fourth Amendment law. This is not the first time this phenomenon has occurred, however. In considering the effect of the communications revolution on Fourth Amendment law, it is helpful to consider the long process by which an earlier phase of that revolution—the telephone—was brought within the protection of constitutional law.

As electric and electronic technologies advanced over the twentieth century, and new forms of communication became possible, so too did new kinds of government surveillance and evidence-collection. One early example involved the telephone, which many criminals took to using in order to advance their enterprises. In *Olmstead v. United States* (1927), the Supreme Court considered whether the police needed to get a warrant in order to tap the phones of a Prohibition-era bootlegging conspiracy. Writing for the Court, Chief Justice William Howard Taft concluded that the government's access of electrons on a wire owned by the telephone company did not violate any Fourth Amendment rights of the defendant. Because there was no physical trespass, there was thus no invasion of the Fourth Amendment's textual protection of "persons, houses, papers, and effects."[33]

In a famous dissent, Justice Louis Brandeis disagreed, making two points that continue to be relevant today: the importance of privacy to civil liberties against the state, and the importance of constitutional law evolving with the times to continue to protect the civil liberties that are necessary to democratic self-governance. Brandeis argued that privacy was important because it supported values that were critical to democratic self-government, including "the

[32] *See also* Laura Donohoe.
[33] Olmstead v. United States, 277 U.S. 438, 466 (1928).

significance of man's spiritual nature, of his feelings and of his intellect."[34] This linkage of privacy against the state to democratic self-government protects an interest I have elsewhere called "intellectual privacy."[35]

Brandeis also argued that constitutional law needed to evolve to take account of changed circumstances, or else the rights it guaranteed would become hollow and ineffective protections. For constitutions, he wrote:

> They are, to use the words of Chief Justice Marshall, 'designed to approach immortality as nearly as human institutions can approach it.' . . . [T]herefore, our contemplation cannot be only of what has been, but of what may be. Under any other rule, a constitution would indeed be as easy of application as it would be deficient in efficacy and power. Its general principles would have little value, and be converted by precedent into impotent and lifeless formulas. Rights declared in words might be lost in reality.[36]

Accordingly, he argued, the principle of privacy against the state at the core of the Fourth Amendment needed to be extended to the non-physical invasion of wiretapping, an invention that enabled subtler and more effective forms of eliciting a confession than "stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[37] But crucially, Brandeis warned that the Fourth Amendment needed to continue to evolve. In a passage that seems to have uncannily foreseen the development of cloud computing, Brandeis predicted:

> Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[38]

In the ninety years since Justice Brandeis penned his dissent, his two principles of privacy and evolution have each risen to the forefront of Fourth Amendment law. His first notion, that privacy should be the primary touchstone of the Fourth Amendment, took forty years to be recognized, but after the case of *Katz v. United States* (1968), the government is required to obtain a warrant before it invades a zone protected by a person's "reasonable expectation of privacy," whether that place is a home, a car, a telephone call, or a smartphone.[39]

Brandeis's second prediction—that the Fourth Amendment should evolve to keep up with technological and other social changes—also continues to bear fruit. As noted above, the

---

[34] *Id.* at 478 (Brandeis, J., dissenting).
[35] NEIL RICHARDS, INTELLECTUAL PRIVACY (2015); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).
[36] *Olmstead,* 277 U.S. at 472–73 (Brandeis, J., dissenting).
[37] *Id.* at 473–74 (Brandeis, J., dissenting).
[38] *Id.* at 474 (Brandeis, J., dissenting).
[39] *E.g.*, Wilson v. Layne, 526 U.S. 603 (1999) (home); Kyllo v. United States, 533 U.S. 27 (2001) (homes); United States v. Jones, 132 S.Ct. 945 (2012) (cars); United States v. Katz, 389 U.S. 347 (1967) (telephone call); Riley v. California, 573 U.S. ___ (2014) (smartphones).

Supreme Court seems to be receptive to the principle that Fourth Amendment privacy rights ought to be adapted in order to remain vital as technology advances. In the *Riley* case, in which the Court brought smartphone data within the protection of the Fourth Amendment, the Court found the fact that modern smart phones connect to cloud storage made them more deserving of privacy protection rather than less.[40] The same principles apply to other content stored in the cloud—what the Supreme Court referred to as "the sum of an individual's private life."[41] However, this task of adaptation or translation of constitutional principles to evolving technology remains very much a work in progress, and perhaps permanently so. Yet in considering the application of Fourth Amendment law to cloud computing, Brandeis's cautionary prediction in *Olmstead* about the possibility of secret document production by the government remains important, particularly now that such technologies have been developed and deployed almost a century after he warned of their dangers. As I have argued at length elsewhere, the reading of the Fourth Amendment that is most faithful to its values seems to be that we should recognize that Fourth Amendment rights should be expanded to the cloud, and the broad reading of the third-party doctrine should be rejected as insufficiently protective of our vital civil liberties.[42]

B. Sneaking and Peeking

The protection against secret searches is deeply ingrained in the traditions of the Fourth Amendment. Current doctrine provides that if the government executes a search warrant, it has to give notice to the person being searched. In *Berger v. New York*,[43] a case decided the same term as *Katz,* the Supreme Court invalidated New York's eavesdropping statute, partly because "the statute's procedure . . . has no requirement for notice as do conventional warrants." Several years later, in a case involving federal wiretapping law, the Court explained that "[t]he *Berger* and *Katz* decisions established that notice of surveillance is a constitutional requirement of any surveillance statute."[44]

The rationale for notice is a straightforward one—the government's power to engage in searches and seizures is one that is susceptible to abuse, and the targets of government searches have a right to know that the government has being trawling through their houses, papers, and effects (physical or digital). There are certainly legitimate law enforcement reasons for delayed notice in some circumstances—it would unreasonably hamper a government investigation for it to announce its presence on every phone call that it was wiretapping, for instance. Nevertheless, a government that is accountable to its citizens must, as the Supreme Court has recognized, let those citizens know at some reasonable time that it has been watching them, particularly when that watching has been directed at the constitutionally protected activities and places that the Fourth Amendment and its warrant requirement protects.

In the classic case of a physical search of a home, for example, it is difficult for the police to hide their activity. Homeowners tend to be at home and would notice searches, and physical searches by their nature tend to take time and to leave evidence of their occurrence. While it is

---

[40] Riley v. California, 134 S. Ct. 2473, 2489, 2491 (2014).
[41] *Id*.
[42] *See* Neil M. Richards, *Privacy and the Future of the Cloud*, WASH. U. L. REV. (forthcoming 2017).
[43] 388 U.S. 41, 60 (1967).
[44] United States v. Donovan, 429 U.S. 413, 430 (1977).

possible for the police to wait until the homeowner leaves and perform so-called "sneak and peek" searches, these searches are limited in duration until the homeowner is due to return. "Sneak and peek" searches seem to have been initiated as part of the "War on Drugs" in the 1980s, but their use accelerated with the passage of the Patriot Act in 2001, particularly as applied to searches of digital records of emails and cloud documents held by Internet companies and other trusted intermediaries.[45] When these searches occur, the government tells only the intermediary and frequently places a gag order on that company to tell the subject of the search about its existence. Many of these gag orders are of indefinite duration; for example, the federal Electronic Communications Privacy Act allows the government to obtain a warrant from a cloud storage company of its company's papers "without . . . notice to the subscriber or customer" and to obtain an injunction forbidding indefinitely the company from notifying anyone of the existence of the disclosure.[46]

Searches of this kind cut right at the splintering of the law that the information revolution has caused. The Government is able to use the third-party doctrine to argue that it does not need a warrant to obtain a person's emails or documents from their cloud provider. At the same time, because digital searches are vastly less obvious to the suspect than old-fashioned physical searches, the government can use its statutory ability to obtain delayed notice and the suspect may never learn if the government has been reading her mail. Moreover, the digitization of searching acts as a kind of force multiplier that lets the government engage in vastly more digital searches than it could ever have had the resources to perform physically. In so doing, searches of this kind evade the two traditional non-legal restraints that the Supreme Court has identified in the Fourth Amendment context— "limited police resources and community hostility" to excessive surveillance.[47] They also threaten to replicate the problem of unregulated surveillance that *Olmstead* failed to halt in the telephone age for the Internet age we now live in.

III. Secret Searches as Censorship

Looking at secret searches as searches from the perspective of the Fourth Amendment thus reveals that they menace constitutional commitments at the core of what the Fourth Amendment protects—the importance of a detached magistrate consenting to the government intruding into a home or reading private papers. But there is another way to think about the threat that secret searches pose to civil liberties, which is to focus on their secrecy—the fact that they are unknown to the suspect and frequently accompanied by injunctions that prevent their disclosure. This perspective asks questions of the threat that secret searches pose to First Amendment values of free thought, free speech, and the relationships between free expression and democratic self-governance. As in the Fourth Amendment, there are two separate ways in which secret searches threaten constitutional values.

The most obvious way in which secret searches menace First Amendment values is that they restrict free speech at the core of what the First Amendment protects. The most basic and

---

[45] Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 Pepperdine L. Rev. 3 (2013).
[46] 18 U.S.C. §§ 2703; 2705(b).
[47] Illinois v. Lidster, 540 U.S. 419, 426 (2004).

important justification for why free speech is protected under American constitutional law is because of its close relationship to the processes of democratic self-government. This explanation draws its lineage from important explanations offered by James Madison, Louis Brandeis, and Alexander Meiklejohn.[48] It also rests at the center of the most significant free speech cases decided by the Supreme Court, *New York Times v. Sullivan* (1964),[49] which instilled the commitment to "uninhibited, robust, and wide-open" public debate on government policy at the core of special protection for expression, and *Reno v. ACLU* (1998),[50] which extended that principle to digital expression. Under this theory, the "core meaning" of the First Amendment is that a self-governing citizenry must have the ability to discuss and pass judgment on the actions that elected and appointed government officials perform in their name. This notion, reflected most clearly in the writings of Louis Brandeis, also lies behind the core purpose of the Freedom of Information Act of 1966, [51] which safeguards the citizenry's ability to know "what their government is up to."[52] In order to fulfill this function, those citizens must have free access to the information and opinions of other people so that they can make a full and deliberately informed decision about how to govern themselves. Prior restraints on or subsequent punishment for expression related to those decisions can only be justified by government interests of the highest importance, strictly limited to those restrictions on expression that are absolutely necessary to advance those interests. In practice, this standard has proven very difficult for the government to meet. In the famous *Pentagon Papers* case, for instance, the U.S. government was unable to justify an injunction placed upon the *New York Times* to prevent publication of classified government reports about the conduct of the Vietnam War.[53]

From this perspective, we can see why secret government searches are so menacing to First Amendment values, and why injunctions of indefinite duration that protect secret searches are of dubious constitutionality under well-settled First Amendment law. The gag orders that prevent companies from letting their customers know that their records are being sent to the government prevent willing speakers (the companies) from communicating with willing listeners (the suspects) and the public at large. While it is plausible that there is a government interest in investigations that would justify a short-term delay in notification of suspects in order to prevent, for example, the destruction of evidence or the completion of a discrete investigation, this scenario does not accurately describe the current state of secret searches enjoined by gag orders. In litigation against the federal government alleging that secret searches under federal electronic surveillance law violate the First Amendment, Microsoft presented evidence that it received thousands of requests each year for customer data accompanied by legal orders silencing it from speaking about the requests, and that two-thirds of these injunctions had an indefinite duration.[54]

---

[48] *E.g.*, JAMES MADISON, THE VIRGINIA REPORT OF 1799–1800, TOUCHING THE ALIEN AND SEDITION LAWS; TOGETHER WITH THE VIRGINIA RESOLUTIONS 227 (J.W. Randolph ed., 1850); Whitney v. California, 274 U.S., 357 377 (1927) (Brandeis, J., concurring); ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 27 (1948).
[49] 376 U.S. 254 (1964).
[50] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
[51] Freedom of Information Act of 1966, 5 U.S.C. § 552.
[52] Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).
[53] New York Times Co. v. United States, 403 U.S. 713 (1971).
[54] First Amended Complaint, *Microsoft Corp. v. United States* at ¶ 5, No. 2:16-cv-00538-JLR, W.D. Wash., June 17, 2016.

Prior restraints are straightforward interferences with First Amendment rights that are easy to understand. But secret government searches also menace First Amendment values in a second, more indirect way. This second way is more subtle, yet in the end represents an even greater threat to the ability to think and speak differently in dissent to the dominant view, even in a democracy. The fear that the government might, at any moment, be going through our papers, reading our diaries, and opening our mail cuts to the core of intellectual privacy, the protection from surveillance or interference when we are engaged in the processes of generating ideas—thinking, reading, and speaking with confidantes before our ideas are ready for public consumption. This unfettered ability to develop our political beliefs is at the core of intellectual, and thus political, freedom. Yet when we are watched, our speech, reading, and even our thinking incline to the boring, the bland, and the mainstream. This is particularly the case as ever more of our political and intellectual activities are mediated by information technology—the same information technologies that the government seeks to monitor through secret searches.[55]

The idea that when we are being watched we act in ways that are more socially acceptable has a long tradition in our legal and popular culture, from the First Amendment notion of chilling effects to literary and philosophical classics like George Orwell's *Nineteen-Eighty-Four* and the work of Jeremy Bentham and Michel Foucault.[56] While First Amendment doctrine rarely requires proof of a chilling effect, there is nevertheless an emerging literature in the trans-disciplinary field of surveillance studies that has documented this effect with empirical evidence.[57] Moreover, in the years since Edward Snowden revealed the scope of government surveillance of digital technologies in Western democracies, a new body of scholarship has shown that electronic surveillance chills the exploration of unpopular political ideas, including the willingness to write about or use search engines to learn about controversial topics.[58]

---

[55] *See generally* RICHARDS, INTELLECTUAL PRIVACY, *supra* note 35.

[56] Jeremy Bentham, *Panopticon*, *in* 3 OPINIONS OF DIFFERENT AUTHORS UPON THE PUNISHMENT OF DEATH 321, 328 (Basil Montagu ed., 1816); MICHEL FOUCAULT, DISCIPLINE AND PUNISH 200 (1975); ORWELL, *supra* note 1.

[57] For an introduction to the surveillance studies literature, *see, e.g.*, DAVID LYON, SURVEILLANCE STUDIES (2007); SURVEILLANCE AND DEMOCRACY (Kevin D. Haggerty & Minas Samatas eds., 2010); THE SURVEILLANCE STUDIES READER (Sean P. Hier & Joshua Greenberg eds., 2007).

[58] *See generally* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 467 (2015) ("If the First Amendment serves to foster a marketplace of ideas, surveillance thwarts this purpose by preventing the development of minority ideas."). *See also* Christopher Campbell & Rosamunde Van Brakel, *Privacy as a line of flight in societies of mass surveillance*, ETHICAL SPACE: INT'L J. OF COMMUNICATION ETHICS 12(3/4): 39-46 (2016); CREATING LAW ENFORCEMENT ACCOUNTABILITY & RESPONSIBILITY (CLEAR) PROJECT, CUNY SCHOOL OF LAW, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (Mar. 11, 2013) http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf; Keith N. Hampton et al., *Social Media And The Spiral Of Silence*, PEW RESEARCH CTR. 8, 23 (2014); HUMAN RIGHTS WATCH & ACLU, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE U.S. SURVEILLANCE IS HARMING JOURNALISM, LAW AND AMERICAN DEMOCRACY (July 2014), https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf; Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Apr. 29, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564; PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013), https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; Jonathan W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016).

First Amendment doctrine has been highly protective of the ability of speakers to express their opinions and beliefs without fear of legal consequences. Nevertheless, while it protects the *public expression* of those opinions, the doctrine has been far less sensitive to the processes by which those opinions come to be *privately developed* and tested before they are published. Nevertheless, secret surveillance poses a serious threat to both kinds of First Amendment values, when it censors the discussion of the practices of surveillance, and when it subtly but seriously inhibits the development of political and other forms of protected opinions and beliefs.

IV. Surveillance in a Digital Democracy

Secret surveillance is thus a problem that is increasing and menaces the foundational civil liberties protected in the United States by the Fourth and First Amendments. What then, should be done about this problem? Put more directly, how can we safeguard these vital and hard-won civil liberties to ensure that they remain protected in our increasingly digital democracy? This will be a complex challenge, and one that will go beyond simple fixes like trusting technological innovation or tweaking constitutional doctrine. Nevertheless, I believe that it can be done; indeed, it must be done if we do not wish our systems of progressive self-government to be left behind with the age of newsprint, radio, and paper ballots. In this Part, I offer four principles to guide us as we take on this challenge. These principles are: (1) Secret Surveillance is Illegitimate; (2) We Must Bring Surveillance Within the Fourth Amendment and (3) Within the First Amendment; and (4) Companies Must Be Part of the Solution.

At the outset, however, I want to be clear that it is not my argument that government surveillance has no place in a digital democracy. The criminal and existential risks that are often used to justify surveillance are real, and are threats to democracy themselves. But the evidence seems undeniable that unchecked or insufficiently-checked secret surveillance can also threaten democratic self-government and political liberties are sometimes taken for granted. We must chart a delicate path between these risks, and the four principles that follow are offered as an initial plan for how to do it.

1. Secret Surveillance is Illegitimate

Truly secret surveillance has no place in a democracy. In a democratic society, in which the people constitute and control the government that acts in their name, the people must also have the right to consent to what the government does in their name. This includes the right to consent to government surveillance programs, at least with respect to the nature and broad scope of these programs. This does not mean, of course, that the government needs to notify the subjects of targeted surveillance at the time of the interception. It would be counter-productive, even absurd, to require the government to come on the phone to let us know that our call might be recorded, in the manner of a corporate customer service line "for quality assurance." Nevertheless, the problem alleged in the Microsoft gag order suit—that vast amounts of personal data can be obtained from companies about their users under indefinite court orders of secrecy—is inconsistent with the principle that secret surveillance is illegitimate. This is particularly the case when surveillance powers justified under the existential threat of terrorism drift into becoming "business as usual" tools for the investigation of drug crimes and other infractions of

the ordinary criminal law. In these cases, the secrecy of the programs enables this mission creep by eliminating public accountability.

The typical response to calls for increased regulation of secret surveillance is that it makes us less safe, that criminals and other malfeasants who know about surveillance techniques will be able to adapt to them and evade them. This argument certainly has some validity, but there are, I think, two powerful responses to it. First, perfect security is an illusion. No society, whether democracy or police state, has ever achieved perfect security. In our daily lives, we constantly make calculated risks in which we trade off security against other values, be they convenience, pleasure, commercial or personal opportunity, or privacy. Humans drive cars and fly in airplanes, they use credit cards, eat unhealthy but often delicious foods, and expose themselves to germs and other risks. Risks of crime (or even terrorism) may upset our calculus of risk because they are extraordinary, but many of these risks are irrational. Rather than pursue the chimera of perfect security, we should instead think rationally about these sorts of risks and not fall into the seductive but ultimately unsatisfying trap of a state of perfect surveillance but nevertheless imperfect security.

Second, even if increased surveillance may make us safer against criminals (though this is itself a debatable proposition[59]), unregulated and under-regulated surveillance carries risks of its own. The mounting body of evidence that unchecked or under-regulated surveillance can inhibit engagement with potentially controversial ideas seems well-founded. The personal dangers of this surveillance also go beyond the psychological inhibition that the surveillance literature documents. Consider in this context the NSA surveillance of the pornography habits of political minorities discussed earlier. While that program appears to have been authorized, the history of government surveillance in all countries appears littered with abuses. The most recent debate over surveillance prompted by Edward Snowden brought to light the infamous "LOVEINT" practice of NSA officers occasionally using their surveillance tools in violation of agency practices to spy on love interests—spouses, partners, or potential future partners.[60] Much more serious infractions have been discovered in the less recent history of American surveillance authorities. The FBI under J. Edgar Hoover became infamous for warrantless surveillance of dissidents on political grounds, a practice that was brought to light by the "Church Committee," a Senate committee constituted in the aftermath of Watergate to study intelligence abuses.[61] The worst abuse was undoubtedly the letter sent to Martin Luther King, Jr., whom the FBI had surveilled on the belief that his civil rights activities were being controlled by Moscow. The FBI discovered that King was acting on his own volition, but that he was having an extramarital affair, and sent him an anonymous letter with evidence of the infidelity and a thinly-veiled threat that he would be exposed if he did not commit suicide.[62]

---

[59] *E.g.*, Danielle Keats Citron & Frank A. Pasquale III, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011).
[60] Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, WASH. POST (Aug. 24, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/?utm_term=.a7fcfc42ea4f.
[61] 2 INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENT OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES 5, 10, 15 (Apr. 26, 1976); WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 562 (2016).
[62] DAVID J. GARROW, THE FBI AND MARTIN LUTHER KING, JR. (1981).

The King episode points up one of the chief dangers of secret, unconstrained surveillance—widespread surveillance can be used against political enemies to blackmail or discredit. Indeed, this impulse was precisely the one motivating the government's recent attempt to monitor pornography use by "radicalizers." One does not need too vivid an imagination to contemplate surveillance and selective leaking of the secrets of politicians for political gain.

We can hope of course that our surveillance authorities act with the professionalism that their public trust demands. But law in general (and constitutional law in particular) exists in part to check against the excesses of unconstrained power. As Justice Brandeis reminded us in his opinion in *Olmstead*, concluding his analysis of the Fourth Amendment question, "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."[63] Checks and balances embodied in law will remain important if we are to gain the undeniable benefits of regulated surveillance while avoiding the undeniable dangers of insufficiently-regulated surveillance.

2. Bringing Surveillance Within the Fourth Amendment

One important check and balance that could serve to bring surveillance more squarely within bounds would be to recognize the limitations of the broad reading of the third-party doctrine that suggests that any information shared with another entity loses the protection of the Fourth Amendment, even where that entity is a trusted digital intermediary such as an email provider or secure cloud storage or backup service.

One obvious solution to this problem would be to use Fourth Amendment doctrine to restore the balance that physical searches and limited non-electronic resources provided until recently by affirming that warrants are required before the government can obtain electronic letters or papers held by trusted intermediaries, and that even when such warrants are obtained, indefinitely delayed notice (particularly enforced by injunction) is constitutionally unreasonable. But the existence of federal statutes that purport to allow vast secret searches at scale means that the final source of these rules will ultimately have to be the Supreme Court. An important first step would be for the Court to take Justice Sotomayor's invitation to curtail the third-party doctrine, particularly in the context of electronic information, a proposal I have written about at length elsewhere.[64]

---

[63] *Olmstead,* 277 U.S. at 479 (Brandeis, J., dissenting). In his opinion for the Court in *United States v. United States District Court*, 407 U.S. 297 (1972), Justice Powell made a similar observation, noting that "History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."

[64] *See* Richards, *Privacy and the Future of the Cloud*, *supra* note 42.

There will of course be difficult cases. Not all kinds of electronic information are as analogous to postal mail and telephone contents as emails and cloud documents are. Reasonable minds can differ about the treatment of, for example, cell phone location data or call record "metadata." In addition, constitutional doctrine is often insufficiently granular to prescribe the detailed procedures that are necessary to regulate something so complex as electronic surveillance. Recognizing these problems, California recently passed the California Electronic Communications Privacy Act, which went into effect on January 1, 2016.[65] This law, better known as "CalECPA," is a broad protection of electronic information that requires California police to obtain a warrant before they access electronic information either digitally or from a physical device such as emails, stored documents, or the "metadata" associated with electronic information.[66] Although CalECPA only applies in California, it is a well-drafted statute that could serve as a model for the reform of the Federal Electronic Communications Privacy Act, which has become substantially outdated since its passage in 1986.

3. Bringing Surveillance Within the First Amendment

In updating our laws to ensure they continue to reflect and protect our fundamental civil liberties in digital contexts, we must ensure that First Amendment rights and values are protected as well as Fourth Amendment ones. As discussed earlier, secret government searches of digital information raise two distinct challenges to First Amendment values.

The first of these is the idea that it is a kind of censorship or prior restraint when intermediaries are served with secret search orders for their customers' data, but are indefinitely barred from disclosing the order. This is a credible First Amendment argument with much to recommend it, though this is a somewhat surprisingly complex area of First Amendment law, in which the doctrine is still under-developed. There have been a series of challenges to gag orders in the context of National Security letters, and after much litigation some lower courts have found that they may violate the First Amendment.[67] To be properly resolved, however, this issue needs to go to the Supreme Court, and the Microsoft litigation discussed above represents a likely well-briefed opportunity for the Supreme Court to weigh in and set some parameters for this important issue. In the meantime, a number of technology companies have sought to partially fill the knowledge gap by publishing "transparency reports"—regular statements publishing, in anonymized form, aggregate data about how many and what types of government information requests and orders they receive.[68]

---

[65] California Electronic Communications Privacy Act, SB 178, 2015, codified at CAL. PENAL CODE §§ 1546 -1546.4. (In full disclosure, I signed a letter written to California Governor Edmund G. Brown, Jr. on behalf of a number of legal scholars that asked the Governor to sign rather than veto the bill). *See* Letter of Legal Scholars to Governor Brown (Sept.12, 2015), https://www.aclunc.org/sites/default/files/SB178ScholarsSupport.pdf.

[66] CAL. PENAL CODE §§ 1546 -1546.1.

[67] *E.g.*, Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), vacated on other grounds Doe v. Gonzales, 449 F. 3d 415 (2d Cir. 2006); In re National Security Letter, 930 F. Supp. 2d 1064 (2013).

[68] For particular companies' transparency reports, *see* Google Transparency Report, https://www.google.com/transparencyreport/; Twitter Transparency Report, https://transparency.twitter.com/; Dropbox Transparency Report, https://www.dropbox.com/transparency/.

The second challenge posed by secret government searches is their threat to intellectual privacy. The awareness that our reading, searching, browsing, and video-watching activities might not be private chills our willingness to engage, freely and fearlessly, with ideas that others might think to be dissident, dangerous, deviant, or just plain eccentric.[69] I have also written at length about this problem (and possible solutions to it), but the basic solution must be to use a combination of legal tools to ensure that when people read, think, and engage in these and other processes of intellectual and personal exploration and wondering, they have meaningful guarantees that their mental wonderings and wanderings are not being tracked by government or corporate surveillance systems.[70] Our digital society is increasingly characterized by informational distrust, whether distrust of the rules that govern access to ostensibly private personal information,[71] or distrust in the bias or falsity of information received from online media.[72] One of the great challenges of our time will be to use law and other tools to build and restore trust in the structures through which information about ourselves and our society is collected and used. Secret government searches are but one part of this problem, but bringing them within the rule of law will be an important part of the solution.

One small but important step that can be taken to fix this situation is to remove one of the many obstacles to courts assessing the lawfulness of government surveillance, which is the increasingly strict reading of standing doctrine that the Supreme Court has been applying in privacy cases. Thus, in *Clapper v. Amnesty International* (2013), lawyers, journalists, and human rights activists who spoke frequently with non-U.S. clients and contacts about sensitive topics were found to be unable to bring First and Fourth Amendment challenges to the federal law authorizing the surveillance because they lacked standing to sue under Article III of the Constitution.[73] The Supreme Court dismissed their suit because they could not prove that they were being targeted by the government, even though the government, as defendant, surely knew whether it was monitoring the civil society plaintiffs or not.[74] In so doing, the Court needlessly read the doctrines strictly in a way that denied the ability of the plaintiffs to challenge the consistency of the broad surveillance program with the First Amendment.[75] In the Court's most recent privacy standing case, it similarly signaled that the requirements of standing in privacy cases seem to be getting stricter, rather than more permissive.[76] Yet given the threat that secret government surveillance poses to the important values of intellectual privacy and intellectual freedom more generally, it would be a step in the right direction to, at a minimum, subject these programs to constitutional review, even if they are ultimately found to survive it.

---

[69] *See* RICHARDS, INTELLECTUAL PRIVACY, *supra* note 35.
[70] *See, e.g.*, *id*.; Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689 (2013).
[71] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, STAN. TECH. L. REV. (forthcoming 2017).
[72] John Herrman, *Fixation on Fake News Overshadows Waning Trust in Real Reporting*, NY TIMES, (Nov. 18, 2016), http://www.nytimes.com/2016/11/19/business/media/exposing-fake-news-eroding-trust-in-real-reporting.html; Sapna Maheshwari, *How Fake News Goes Viral*, NY TIMES (Nov. 20, 2016), http://www.nytimes.com/2016/11/20/business/media/how-fake-news-spreads.html?_r=0.
[73] 133 S.Ct. 1138 (2013).
[74] *See id*. at 1149 n.4.
[75] *See* Richards, *The Dangers of Surveillance*, *supra* note 35.
[76] *Spokeo v. Robins*, 136 S.Ct. 1550 (2016).

4. Companies Must Be Part of the Solution

One fundamental difference between the problem of digital surveillance and surveillance issues of the past is the importance of intermediaries. In one sense, Fourth Amendment communications privacy issues outside the home have always involved intermediaries. Companies providing mobile telephone and data, email, or cloud services are certainly the modern analogues of the postal service or the telephone company. But as the Supreme Court recognized in *Riley*, the volume and variety of information stored on (for example) a modern smartphone changes the situation considerably. As the Court noted, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house."[77] Along these lines, a company providing cloud storage of data (such as Google, Microsoft, Dropbox, or Carbonite) starts to closely resemble the future technology envisioned by Justice Brandeis in *Olmstead*, which would enable the reproduction in Court of documents stored in a locked desk drawer.[78]

However we characterize them in descriptive or legal terms—trusted third parties, custodians of our data, or information fiduciaries—intermediaries are inextricably linked to the problem of digital records privacy. Consequently, they must also be part of the solution. Our legal responses to this problem must take into account not only that cloud and other technology companies are entrusted with vast amounts of personal data, but also that the humans who constitute our digital society frequently have little choice about the fact or the terms of that entrustment, at least if they want to participate as ordinary members of that society.[79] The constitutional doctrines and statutory schemes that we use to regulate digital technologies must reflect these nuances, and not rest on blunt and unhelpful distinctions like *Olmstead*'s trespass theory of the Fourth Amendment or the third-party doctrine's suggestion that Fourth Amendment rights are waived in whatever is shared or entrusted to others.

Not only must we ask more of our legal rules as they apply to companies, but we also must ask more of those companies when they confront those legal rules. If we wish to have meaningful privacy and information security, we must demand that companies take steps to protect us, and to help us better protect ourselves. It is in this light that the recent legal struggles between Apple and Microsoft, on the one hand, and federal law enforcement agencies, on the other, are the most encouraging. So too, is the trend towards companies issuing more frequent and more detailed transparency reports,[80] though we must also recognize that transparency reports are merely one small step towards redressing the power imbalance created by secret government searches of digital records. To be sure, corporate efforts to provide protection for their users' civil liberties and transparency of government efforts to encroach upon their privacy are at least partly motivated by business considerations. The trust of their customers is among the most valuable assets technology companies possess, and that trust is threatened by the fear that providers of email, cloud, search, and social media services might be in league with, or

---

[77] *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).
[78] *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).
[79] Richards & Hartzog, *supra* note 71.
[80] *See* Kashmir Hill, *Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government*, FORBES (Nov. 14, 2013), http://www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/#3cf10fc66d06.

compliant to, law enforcement. But the alignment of civil liberties and corporate self-interest is by no means a bad thing, at least as long as those interested in civil liberties are aware of the limitations of corporate self-interest.

Perhaps the best solution to the problem of privacy in a digital age rests on finding an equilibrium, a balance between government and corporate power in the interests of human individuals. As citizens, those humans should seek to have the civil authorities of government regulate companies through law in the public interest. And as consumers, they should push companies through market mechanisms to check the secret surveillance of the government's criminal authorities. Whatever balance of power is ultimately produced from these processes, though, it is evident that companies must be an important part of reaching that balance.

CONCLUSION

The digital revolution has changed much, and one of the most significant changes is the vast amount of personal data that is created and stored remotely in networked (or "cloud") storage. The mere fact that this information exists means that we must understand that we are in fact living in a "golden age of surveillance." As Lawrence Lessig argued over two decades ago, the Digital Revolution presents the problem of translation: How shall we translate our hard-won protections of civil liberties into the digital environment?[81] How we respond to this challenge will be our generation's defining legacy of civil liberties. It will determine whether we are remembered as fondly as the civil liberties activists of the 1960s, or as ashamedly as the protagonists of the Red Scares of the 1920s and 1950s. More fundamentally, it will determine whether our hard-won civil liberties endure, or whether they fail to survive the digital transformation and become remembered (if they are remembered at all) as an accident of history.

[81] Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165 (1993); *see also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000) (applying this argument to the digital environment).