Foreword

*Nancy Libin**

In 1999, Scott McNealy, cofounder of Sun Microsystems, was widely rebuked for saying about privacy in the digital era, "You have zero privacy anyway. Get over it."[1] At that time, the commercial use of the Internet was in its relative infancy. Since then, mobile and Internet services have converged, putting powerful computers in our pockets.

Now, as we surf online, call our friends, send emails and text messages, and upload photos to our social network pages, we expose ourselves digitally in a way that is more intimate, public, and enduring than most people will ever know.

This trend will continue. According to the International Data Corporation, the amount of digital information we generate doubles every two years, with 7.9 zettabytes[2] expected in 2015.[3] More of this data will be information about us and our activities rather than content we create ourselves.[4]

Internet service and wireless providers collect, analyze, and use this personal data. And they are not the only ones. Smartphone applications, search engines, social networks, websites, and data aggregators know what we have purchased, what we have searched for online, where we live, where we have been and where we are going tomorrow, and—with the advent of facial recognition technology—even what we look like. Although this information can reveal a great deal about our preferences, habits, associations, and interests—particularly when aggregated and mined with powerful analytic tools—much of it is currently protected only by corporate privacy policies.

Personal data are a treasure trove for companies that use it to target advertisements for their products and services, as well as for data brokers that compile and sell personal information for profit.[5] Personal data also

* Nancy Libin is the Chief Privacy and Civil Liberties Officer of the U.S. Department of Justice. The views expressed here are her own and do not necessarily represent the views of the Department of Justice or the United States.

[1] Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED (Jan. 29, 1999), http://www.wired.com/politics/law/news/1999/01/17538.

[2] This amount is equivalent to eighteen million times the amount of information in the Library of Congress. *See* Sean Ammirati, *Infographic: Data Deluge – 8 Zettabytes of Data by 2015*, READWRITEENTERPRISE (Nov. 17, 2011, 9:30 AM), http://www.readwriteweb.com/enterprise/2011/11/infographic-data-deluge—-8-ze.php.

[3] JOHN GANTZ & DAVID REINSEL, INT'L DATA CORP., EXTRACTING VALUE FROM CHAOS 1, 5 (2011), *available at* http://idcdocserv.com/1142.

[4] *Id.* at 10.

[5] An entire industry has developed around the mining and analysis of individuals' Internet activity collected through web-browser tracking technology. According to the Internet Advertising Bureau, annual revenues for the online advertising industry reached $31.7 billion for 2011, up from $6 billion in 2002. INTERNET ADVERTISING BUREAU, IAB INTERNET ADVERTISING REVENUE REPORT, 2011 FULL YEAR RESULTS 7 (2012), *available at* http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2011.pdf.

comprise the building blocks of criminal investigations by law enforcement officials. Employers who want to monitor current (or evaluate potential) employees and lending institutions that need to assess the creditworthiness of potential borrowers also use personal data.

It is precisely because personal data are so widely available and may be used by so many public and private groups for so many different reasons that people's privacy is at risk. The current lack of comprehensive legislation or regulations governing personal data use has led consumers and privacy advocates to call for greater protections.

The solution is more complex than simply imposing greater controls on entities that collect and use our data. For instance, any new laws must take into account the competing obligations that state and federal authorities have to ensure public safety on the one hand, and to protect personal privacy on the other. After all, when law enforcement officers and prosecutors enforce criminal laws, they must collect personal information about suspects, witnesses, and victims to build and prosecute their cases. But the government also has an obligation to respect the privacy of its citizens' personal information, as recognized in laws like the Electronic Communications Privacy Act (ECPA),[6] which protects the privacy of electronic communications by allowing government access only if certain conditions are met.

Government institutions—including legislators, judges, and regulators—are struggling to figure out how best to protect the privacy of personal data in the information age without compromising the government's ability to fulfill its other responsibilities to protect and serve the public. It is important that government institutions find the right balance. Failure to do so could impinge on citizens' freedom to exercise other fundamental rights—such as freedom of expression and association—that are essential to a democratic society. This Symposium—*Privacy and Accountability in the Twenty-First Century*—tackles this topic with three articles that both explore the privacy impact of the collection and use of sensitive digital information and suggest legislative and regulatory reforms.

Part of the challenge for courts, agencies, and Congress is defining "privacy," a concept that defies easy explanation. As privacy scholar Daniel Solove noted in his recent book *Understanding Privacy*, "[w]hen people claim that privacy should be protected, it is unclear precisely what they mean. This lack of clarity creates difficulty when making policy or resolving a case because lawmakers and judges cannot easily articulate the privacy harm."[7] And because "interests on the other side—free speech, efficient consumer transactions, and security—a are often much more readily articulated, . . . privacy is not balanced against [these] countervailing interests."[8]

---

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

[7] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 7 (2008).

[8] *Id.* at 7–8.

Although the word "privacy" does not appear in the text of the Constitution, the Supreme Court has interpreted several amendments in the Bill of Rights to confer a fundamental right to privacy in certain situations. The Fourth Amendment's prohibition against unreasonable searches and seizures protects against unwarranted government intrusion in the form of physical and electronic surveillance. The Supreme Court's Fourth Amendment jurisprudence, however, has gone through several phases of conflicting evolution, leaving ill-defined the privacy interests that the Fourth Amendment protects and creating uncertainty about the extent to which the Fourth Amendment safeguards personal information in the digital age.

The Court first suggested that the Constitution protected the privacy of personal communications in *Ex Parte Jackson*,[9] where it stated, in dicta, that the Fourth Amendment protected the contents of a sealed letter transmitted through the postal service.[10] Almost fifty years later, however, the Court in *Olmstead v. United States*[11] held that wiretapping a phone to obtain the contents of a conversation did not violate the Fourth Amendment.[12] The Court reasoned that because the Fourth Amendment protects "houses, persons, papers, and effects," a "search" or "seizure" occurs only when the government trespasses onto property or seizes material objects.[13] Because wiretapping a phone involved neither, wiretapping did not implicate the Fourth Amendment.

Justice Brandeis wrote a famous (and prescient) dissent, which foretold the kinds of issues courts and policymakers are considering today as they apply the Fourth Amendment to government interception of modern telecommunications:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. 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.[14]

The Court adopted Justice Brandeis's expansive reading of the Fourth Amendment almost forty years later in *Berger v. New York*[15] and *Katz v. United States*.[16] In *Katz*, the Court appeared to abandon the "trespass" doctrine that it had followed in *Olmstead* and held that the Fourth Amendment

---

[9] 96 U.S. 727 (1877).
[10] *Id.* at 733.
[11] 277 U.S. 438 (1928).
[12] *Id.* at 464.
[13] *Id.* at 466.
[14] *Id.* at 474 (Brandeis, J., dissenting).
[15] 388 U.S. 41, 63 (1967) (holding that the Fourth Amendment protected "conversations" and invalidating a New York statute, that failed to include procedural requirements mandated by the Fourth Amendment).
[16] 389 U.S. 347 (1967).

"protects people, not places."[17] Writing for the majority, Justice Stewart declared that the user of a public telephone "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[18]

But Justice Harlan's concurring opinion in *Katz* articulated the two-part "reasonable expectation of privacy" test that has governed Fourth Amendment analysis until recently. The Fourth Amendment protects expectations of privacy, Justice Harlan wrote, where a person has "exhibited an actual (subjective) expectation of privacy" that "society is prepared to recognize as 'reasonable.'"[19] Applying the test to the facts in *Katz*, he concluded that making a call from an enclosed phone booth warranted constitutional protection, even without a trespass. He noted that the "trespass" doctrine was "bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical intrusion."[20]

Justice Stewart's majority opinion in *Katz*, which emphasized the importance of the telephone to communications in modern society, suggests the Fourth Amendment should protect electronic data we generate in the digital age. Electronic communications devices and computers are as—if not more—integral to private communications now as telephones were in 1967. But the Court nonetheless continued—until recently—to use Justice Harlan's "reasonable expectation of privacy" test as its main analytical framework, even as many of the Justices have had difficulty applying this test to modern technology.

Two decisions the Court issued several years after *Katz* have exacerbated the problem. In *United States v. Miller*[21] and *Smith v. Maryland*,[22] the Court used the "reasonable expectation of privacy" test to define privacy under the Fourth Amendment as something akin to secrecy. In *Smith* and *Miller*, individuals sought Fourth Amendment protection for personal phone records and bank records, respectively. Under what is known as the "third-party records" doctrine, the Court held that individuals have no reasonable expectation of privacy in information they voluntarily reveal to a third party, even if disclosure of that information was limited to that third party and was for the sole purpose of conducting a particular transaction.[23]

The implications of the third-party records doctrine for personal privacy in the twenty-first century are profound. If the mere disclosure of information to another—for whatever limited purpose—eviscerates *any* privacy rights in that information, then Scott McNealy might be right. After all, we

---

[17] *Id.* at 351.
[18] *Id.* at 352.
[19] *Id.* at 361 (Harlan, J., concurring).
[20] *Id.* at 362.
[21] 425 U.S. 435 (1976).
[22] 442 U.S. 735 (1979).
[23] *See id.* at 743–45 (holding that where petitioner knew the numbers he dialed were revealed to the phone company, he could not have thought they would remain private and he assumed the risk the phone company would turn the information over to the police).

cannot obtain financial services, seek medical care or government benefits, travel, work, buy things, or search for information online without revealing personal information to third parties, some of whom we do not even realize have access to our information.[24] In their recent article entitled *Information Accountability*, Daniel Weitzner and others used a powerful example to illustrate the tangible harm an individual can suffer when private (as opposed to government) third parties misuse his or her personal digital information. They described a scenario where a woman who has a chronically ill child conducts searches and purchases books online, and participates actively in online chat rooms, in order to learn more about her child's illness.[25] After she applies for and is denied a job, she wonders whether the potential employer's background check uncovered any of this information, and if so, whether the employer determined the cost of her health care coverage would make her a prohibitively expensive hire.[26] The authors' example raises a provocative question about how our privacy laws could discourage someone from, or even penalize someone for, using online information to help care for a child. This example also shows how gaps in our privacy laws could inhibit exercise of rights to free expression and association.[27]

The Court's recent unanimous judgment in *United States v. Jones*[28] forced some of the Justices to consider how the third-party records doctrine would apply to digital information. Justice Scalia, writing for five Justices, held that the government's monitoring of a vehicle's movements with a global positioning system (GPS) device for a prolonged period of time was a "search" under the Fourth Amendment.[29] He relied on the trespass doctrine, arguing that the *Katz* test added to, but did not supplant, the property-based analysis.[30]

Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concurred in the result, but applied Justice Harlan's two-part test from *Katz*. Justice Alito found that the extended monitoring of the respondent's vehicle violated his reasonable expectation of privacy and therefore was a "search" under the Fourth Amendment.[31] Justice Alito's analysis did not depend on finding a trespass, and he criticized Justice Scalia for resurrecting the "old approach" the Court had "'repudiated'" in *Katz*,[32] stating that it would "present particularly vexing problems in cases involving surveillance that is car-

---

[24] A group of plaintiffs recently sued mobile application developers, alleging the application developers had uploaded the plaintiffs' address books from their phones without their consent. Elinor Mills, *Privacy Suit Filed Against Path, Twitter, Apple, Facebook, Others*, CNET (Mar. 16, 2012, 1:31 PM), http://news.cnet.com/8301-27080_3-57399021-245/privacy-suit-filed-against-path-twitter-apple-facebook-others.

[25] Daniel J. Weitzner et al., *Information Accountability*, 51 COMM. OF THE ACM 82, 84–85 (2008).

[26] *Id.* at 85.

[27] *Id.*

[28] 132 S. Ct. 945 (2012).

[29] *Id.* at 949.

[30] *Id.* at 950.

[31] *Id.* at 964 (Alito, J., concurring).

[32] *Id.* at 959–960 (quoting Rakas v. Illinois, 439 U.S. 128, 143 (1978)).

ried out by making electronic, as opposed to physical, contact with the item to be tracked."[33]

Justice Sotomayor joined Justice Scalia's opinion, but wrote her own concurrence to make clear she agreed with Justice Alito that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"[34] She also questioned whether the third-party records doctrine makes sense in an era where "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[35] For this reason, she believed, the third-party records doctrine developed in *Miller* and *Smith* is "ill suited to the digital age."[36] She suggested that it might well be time to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[37]

Advocates for greater digital privacy rights welcomed Justice Sotomayor's words, but she stood alone on this issue. Indeed, the Court's decision in *Jones* left unanswered many basic questions, such as how the Fourth Amendment would apply to location information generated by one's cell phone and obtained by law enforcement from a cell phone service provider rather than from a device attached to one's car.[38]

Recognizing the courts' inability to protect adequately against certain privacy harms, Congress has responded at various times over the last forty years with legislation that protects discrete types of sensitive information, like financial records, health records, and video rental information.[39] Congress intended that these laws protect privacy rights while allowing the free flow of information necessary for commercial activity, civic participation, protection of public safety, and access to needed services.

But this sectoral approach has left unprotected much of the information we generate online. Since the 1990s, the Federal Trade Commission (FTC) has occasionally stepped in to fill the gap.[40] With varying degrees of success, the FTC has used its authority under Section 5 of the Federal Trade Commission Act to bring enforcement actions against companies that violate

---

[33] *Id.* at 962.
[34] *Id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring)).
[35] *Id.* at 957.
[36] *Id.*
[37] *Id.*
[38] *See id.* at 963 (Alito, J., concurring).
[39] Congress generally has been reactive, however. For instance, it passed the Right to Financial Privacy Act in response to the Court's decision in *Miller* and the Video Privacy Protection Act in response to reporters' attempts to obtain Judge Robert Bork's video rental records during his Supreme Court nomination hearings. *See* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY IN THE INFORMATION AGE §§ 1:4.2[D][4], 1:4.3[B][5] (Kristen J. Mathews ed., July 2011).
[40] The FTC began protecting consumer privacy in the 1970s, after Congress gave it power to enforce the Fair Credit Reporting Act. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS, at A-3 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC Report].

their privacy policies.[41] The FTC has also encouraged companies to adhere to several (but not all) of what are known as the "fair information practice principles."[42]

The three articles in this Symposium raise questions about whether the current legal framework is adequate to protect privacy in the digital age and whether government institutions have struck the appropriate balance between fulfilling their obligation to protect personal privacy and carrying out their other responsibilities to the public.

Dieter Dammeier's article illustrates how new technologies and open government laws are putting pressure on employee privacy in the government workplace. Judge Stephen Wm. Smith argues for greater disclosure of court orders granting government access to electronic communications data. And Professor Hoofnagle and his colleagues—Ashkan Soltani, Nathaniel Good, Dietrich Wambach, and Mika Ayenson—make a compelling argument for government intervention to protect consumers online.

Dieter Dammeier argues that courts' application of the Fourth Amendment to government employers and expansive interpretations of Freedom of Information Act disclosure provisions have combined to limit public employees' privacy rights. Like all employers, public employers need to ensure that their employees comply with agency or department policies and hold their employees accountable for work-related misconduct. But the Fourth Amendment applies to government employers when they enforce their employment policies. This puts the government in a tough spot. Government agencies must make sure that their employees do not act in ways that violate the public trust, but unlike private employers, government agencies must adhere to constitutional limits when they monitor their employees' conduct.

Dammeier recently represented the government employee plaintiffs in *City of Ontario v. Quon*,[43] a case that examined government workplace privacy in the digital age. *Quon* involved a city employee who sent personal texts using his city-issued pager. The Supreme Court considered whether the city's review of transcripts of Quon's texts violated his rights under the Fourth Amendment.[44] The Court assumed, without analysis, that Quon had a reasonable expectation of privacy in the text messages that he had sent using

---

[41] Section 5 of the FTCA prohibits companies from engaging in "deceptive acts or practices." 15 U.S.C. § 45 (2006). A list of privacy-related cases the FTC has brought under Section 5 is available at BUREAU OF CONSUMER PROTECTION BUSINESS CENTER, *Legal Resources*, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Apr. 11, 2012).

[42] The fair information practice principles comprise an internationally recognized information-handling regime that is reflected in U.S. privacy laws, international privacy guidelines, and the privacy laws of other nations. The principles include transparency, access and correction, use limitation, data quality, and security. The FTC chose to emphasize only certain principles—notice, choice, access, and security. *See generally* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE – A REPORT TO CONGRESS (2000).

[43] 130 S. Ct. 2619 (2010).

[44] *Id.* at 2624.

the pager.[45] But the Court held that the city's "search" of the text transcripts was reasonable in scope and therefore did not violate the Fourth Amendment.[46]

Dammeier discusses the difficulties several Justices had during the oral argument understanding both how mobile communications technology works and the central role it plays in individuals' lives today. He is not sanguine about what this bodes for public employees' privacy in the future. As the Court's decision in *Quon* shows, public employees' use of government-issued communications devices has blurred the lines between public and private spheres and between professional and personal conduct. It is not uncommon, for instance, for government employers to allow *de minimis* personal use of such equipment. Courts must consider how this affects the "operational realities of the workplace" and the reasonableness of the scope of a particular search.[47]

Magistrate Judge Stephen Wm. Smith examines government surveillance of a different kind: law enforcement's collection of communications content and metadata[48] under the Electronic Communications Privacy Act. He argues that the growing tendency of magistrate judges to seal orders for electronic surveillance (and sometimes entire docket sheets for cases) prevents the public scrutiny and appellate review necessary both to evaluate whether the ECPA is striking the right balance between privacy and security and to hold law enforcement accountable when it overreaches.

The ECPA requires judges to seal orders for real-time surveillance in order to prevent the target from learning of the investigation. Orders for stored content can also be sealed, pending delayed notice to the target. While evidence obtained in violation of the Fourth Amendment is subject to suppression, evidence obtained only in violation of the ECPA is not. Targets of investigations therefore are rarely motivated to challenge the introduction of the evidence, and as Judge Smith points out, these orders increasingly remain sealed in the absence of any incentive to appeal them. Judge Smith recognizes that law enforcement has a legitimate and compelling need to keep orders sealed during the surveillance, and he suggests several statutory reforms that would increase transparency without compromising law enforcement investigations.

---

[45] *Id.* at 2630.

[46] *Id.* at 2632.

[47] Under *O'Connor v. Ortega*, 480 U.S. 709 (1987), analysis of Fourth Amendment claims against government employers requires (1) consideration of the "operational realities of the workplace" and how they affect an employee's reasonable expectation of privacy, and (2) if an employee does have a reasonable expectation of privacy, a determination of whether the employer's intrusion was reasonable under the circumstances. *Id.* at 717–18, 725–26.

[48] Metadata is data about other data. MERRIAM-WEBSTER, *Metadata*, http://www.merriam-webster.com/dictionary/metadata (last visited Apr. 11, 2012). The Electronic Communications Privacy Act governs access to certain kinds of communications metadata, including the name and address of a subscriber, IP addresses, and means and source of payment. *See* 18 U.S.C. § 2703(c)(2) (2006).

Finally, Professor Hoofnagle and his colleagues make the case for government action to ensure consumers are able to make informed choices online. Their focus is the online advertising industry's use of small files called "cookies," which websites use to track users' behavior online. The authors' research exposed the way that online advertisers are using a relatively new type of "cookie"—called a Flash cookie—to thwart users' efforts to block tracking of their online activity. Websites can surreptitiously install Flash cookies onto Internet users' browsers, where they "respawn" other cookies that users try to delete. Flash cookies also store a much greater amount of information about users' activity than cookies have stored in the past, enabling advertisers to create more detailed consumer profiles. Flash cookies defeat consumers' attempts to control with whom, and for what purpose, they share their personal data. The authors make a strong case for greater regulation and government intervention to ensure consumers have sufficient notice of online tracking and the ability to manage it.[49]

The government has already begun to respond. The FTC recently proposed that browsers be equipped with a Do Not Track tool that would give users greater control over advertisers' access to their online activity.[50] Members of Congress have introduced legislation that would require the same. In addition, the Obama administration recently issued its blueprint for greater commercial data privacy protection. It proposed a combination of federal legislation and enforceable industry codes of conduct to address the gaps in privacy protection under current law.[51]

The Obama administration's data privacy proposal does not address the government's access to information, however. Although members of Congress have introduced bills that would provide some greater privacy protections for electronic communications data sought by law enforcement, they do not codify the reforms Judge Smith proposes. And the Court's narrow decisions in *Jones* and *Quon* leave many unresolved issues about privacy expectations in the digital age. Justice Alito's concurrence in *Jones*, for instance, suggested that the objective prong of the "reasonable expectation of privacy" test might one day collapse under the weight of society's resignation to "the diminution of privacy that new technology entails," even if "the public does not welcome" it.[52] His concurrence showed how the "reasonable expectation of privacy" test could fall short of providing adequate protection in today's dynamic environment, where the rate of technological change often outpaces our ability to understand its impact on personal privacy.

---

[49] A number of Internet users have brought class action lawsuits against websites that have used Flash cookies, alleging violations of the Computer Fraud and Abuse Act as well as other federal and state laws. Jennifer Valentino-Devries & Emily Steel, *'Cookies' Cause Bitter Backlash*, WALL ST. J., Sept. 19, 2010, at B1.

[50] FTC Report, *supra* note 40, at viii.

[51] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[52] United States v. Jones, 132 S. Ct. 935, 957 (2012) (Alito, J., concurring in the judgment).

As Congress, federal agencies, and the courts work to address these difficult issues, they will have to balance privacy interests against the government's need to ensure public safety, protect national security, and maintain the public trust through transparency and accountability. They will also have to find a way to protect consumers without destroying the online advertising industry that has enabled Internet users to obtain (what may seem like) "free" online content and services. In that regard, consumer-citizens need to become more educated about the way technology increasingly captures, stores, and shares personal data, so that they understand online services and new surveillance techniques can come at a very real cost.