


2014

Four Privacy Myths

Neil M. Richards

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

Follow this and additional works at: https://openscholarship.wustl.edu/law_scholarship

 Part of the [Legal Studies Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Repository Citation

Richards, Neil M., "Four Privacy Myths" (2014). *Scholarship@WashULaw*. 494.
https://openscholarship.wustl.edu/law_scholarship/494

This Book Section is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Scholarship@WashULaw by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.



Four Privacy Myths

Neil M. Richards*

Any discussion about privacy today inevitably confronts a series of common arguments about the futility of privacy in our digital age. “Privacy is Dead,” we hear, and “people don’t care about privacy.” Young people in particular are said to have no interest in privacy. What’s more, privacy just protects bad behavior because those of us with “nothing to hide have nothing to fear.” And anyway, the argument goes, new privacy laws would be bad policy since “privacy is bad for business.”

There are other common claims, but these four are perhaps the most common. They are also myths. Each of these four claims: [1] *Privacy Is Dead*, [2] *(Young) People Don’t Care About Privacy*, [3] *People With Nothing to Hide Have Nothing to Fear*, and [4] *Privacy Is Bad For Business* are either plainly false or deeply misleading. In this essay, I’ll explain why each of these four privacy claims are really four privacy myths. First, privacy cannot be dead because it deals with the rules governing personal information; in an age of personal information, rules about how that information can flow will be more important than ever. Second, people (and young people) *do* care deeply about privacy, but they face limited choices and limited information about how to participate in the processing of their data. Third, privacy isn’t just for people with dark secrets; it’s for all of us because information is power and personal information is personal power. Finally, privacy is not always bad for business. One of the best hopes for meaningful

* Professor of Law, Washington University. For helpful comments, thanks to participants at the University of Alabama conference, Elizabeth Knoll, Greg Magarian, Evan Selinger, Brian Tamanaha. Thanks also to my research assistants Ujjayini Bose, Matt Cin, Carolina Foglia, and Grace Corbett.

2014]

Four Privacy Myths

1

privacy protection in the future is for businesses to compete on privacy, and there is some evidence that this is starting to happen.

My goal here is not just to be contrary. Instead, I hope to clear away some of the confusion surrounding the way we talk about privacy in the digital age. When we do that; when we are clear about what privacy is and why it matters, we can start to talk constructively about the kinds of legal and social rules we want to govern personal information in the information age. Our understandings of privacy must evolve; we can no longer think about privacy as merely how much of our lives are completely secret, or about privacy as hiding bad truths from society. Privacy must be understood as the rules we have as a society for managing the collection, use, and disclosure of personal information.

Our society is experiencing an information revolution as powerful and disruptive as the industrial revolution of the nineteenth century. We need to think and talk about how to harness this revolution's great power while minimizing as many of its costs as we can. Or we can continue to believe the myths about privacy. But if we do that; if we think about privacy as outdated or impossible, our digital revolution may have no rules at all, a result that will disempower all but the most powerful among us.

I. PRIVACY IS DEAD

Privacy is dead. We all know that, right? We live in a society that is constantly generating vast quantities of personal information, which in turn is tracked, screened, and sorted by corporations and government entities.¹ Schools track student sleep and activity patterns;² CCTV cameras guard every street corner and

¹ Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press 2005).

² Mary Shapiro, *Parkway's Use of Fitness Monitors Raises Privacy Questions*, St. Louis Post-Dispatch, Jan. 3, 2012, available at <http://www.stltoday.com/suburban->

traffic light,³ and drones are starting to appear in our skies.⁴ We're even tracking ourselves, using personal electronics like GPS watches, fitness trackers, and other gadgets that make the "quantified self" a realistic possibility.⁵

Academic and public commentators have long bemoaned the Death of Privacy. The last twenty years have seen the publication of innumerable books bearing variations on the titles "Privacy is Dead" or "Privacy Is Dying."⁶ At the launch of Sun Microsystems' Jini technology in January 1999, Sun's CEO Scott McNealy famously declared "You have zero privacy anyway. Get over it."⁷ McNealy's outburst made headlines at the time, and has outlived both the Jini technology and Sun's existence as an independent company. It continues to be quoted today by scholars, journalists, and industry figures.⁸ More recently, Vint Cerf, a leading figure in

journals/metro/education/parkway-s-use-of-fitness-monitors-raises-privacy-questions/article_af46b549-of1e-5a41-8a26-7f77c91ced20.html.

³ Julia Angwin, *Dragnet Nation* (New York: Times Books, 2014).

⁴ M. Ryan Calo, *The Drone as Privacy Catalyst*, Stan. L. Rev. Online 64 (2011), available at http://www.stanfordlawreview.org/sites/default/files/online/articles/64-SLRO-29_1.pdf.

⁵ Gary Wolf, *The Data-Driven Life*, N.Y. Times Magazine, April 28, 2010, available at http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?pagewanted=all&_r=0.

⁶ *E.g.*, Lori Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (New York: Free Press, 2012); Ross Clark, *The Road to Big Brother: One Man's Struggle Against the Surveillance Society* (London: Encounter Books, 2009); Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol, CA: O'Reilly, 2000); David H. Holtzman, *Privacy Lost: How Technology Is Endangering Your Privacy* (2006); *Privacy is Dead! (Long Live Privacy!)* (Index on Censorship)(London: Sage 2011); Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage, 2001); James B. Rule, *Privacy In Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (2009); Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: Chicago Press, 2007).

⁷ Polly Sprenger, *Sun on Privacy: Get Over It*, Wired.com (Jan. 26, 1999), <http://www.wired.com/politics/law/news/1999/01/17538>.

⁸ *E.g.*, Bruce E. Boyden, "Regulating At the End of Privacy," University of Chicago Legal Forum, 173 (2013): 173; Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, Stanford Law Review 62 (2010): 1038; Paul Rosenzweig, "Privacy

the creation of the Internet and Google's "Chief Internet Evangelist" suggested that privacy might be a historical anomaly. Facebook founder Mark Zuckerberg was more blunt, declaring that "the age of privacy is over."⁹ Privacy is dead, or at the very least, it is dying.

But if privacy is dead (or dying), it is dying a very long, slow, and drawn-out death. Privacy's death throes (if that's really what they are) go back to at least 1890, the year in which anxiety about privacy in American law is typically first noted. In that year, East Coast elites were gripped by a kind of privacy panic motivated by changes in technology and society. In June, New York opera star Marion Manola obtained an injunction against a theater promoter who wanted to publish a photograph of her wearing tights that had been taken on stage with one of the new cameras.¹⁰ In July, E.L. Godkin, editor of *The Nation*, argued for what he termed "the right to privacy," a person's right "to decide how much knowledge of his personal thought and feeling, and how much knowledge, therefore, of his tastes and habits, of his own private doings and affairs, and those of his family living under his own roof, the public at large shall have."¹¹ And in December, Louis Brandeis and Samuel Warren's famous article "The Right to Privacy"¹² bemoaned the rise of gossip journalism and portable cameras, and called for the

and Counter-Terrorism: The Pervasiveness of Data," *Case Western Reserve Journal of International Law* 42 (2010): 629; Jonathan Zittrain, "Privacy 2.0," *University of Chicago Law Forum* 2008 (2008): 68.

⁹ Marshall Kirkpatrick, *Facebook's Zuckerberg Says The Age of Privacy is Over*, Readwrite (Jan. 2, 2010), http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~002UUoqssyO3eq.

¹⁰ *Manola Gets an Injunction*, N.Y. Times, June 18, 1890, at 2; *Photographed in Tights*, N.Y. Times, June 15, 1890, at 2; see also Don R. Pember, *Privacy and the Press: The Law, the Mass Media, and the First Amendment* (Seattle: U. Washington Press, 1972), at 56.

¹¹ E.L. Godkin, *The Rights of the Citizen: IV. To His Own Reputation*, Scribner's Magazine 8 (1890) 65.

¹² Samuel Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193

creation of a tort to keep embarrassing true facts out of the newspapers.¹³

Legal historian Lawrence Friedman has shown how these events (among others) were the result of elites feeling anxious that their dominant place in society was being threatened by a new democratic press using new tools to shine the light of publicity upon them.¹⁴ But the attention to privacy took root in American law, and a body of privacy law began to develop.¹⁵ This body of law protected a wide variety of interests, including intrusions into private places, the use of people's photographs for commercial purposes without consent, and disclosures of facts that were either embarrassing or portrayed a person in a "false light."¹⁶

Another privacy panic gripped the United States in the 1960s, as emerging computer technology begin to allow the creation of "data banks" holding personal information. This digital privacy problem prompted a spate of books and cultural attention on threat to privacy. With the public now aware of the rising importance of credit reporting bureaus and other uses of data in society, Congress passed the Fair Credit Reporting Act of 1970, and, following the Richard Nixon surveillance scandal, the Privacy Act of 1974. At the same time, some of the notions of privacy that Warren and Brandeis had suggested for matters of private law began to work their way into constitutional law as well. In a series of blockbuster cases, the United States Supreme Court held that the Constitution protected privacy interests in areas as diverse as police wiretapping,

¹³ Neil M. Richards, "The Puzzle of Brandeis, Privacy, and Speech," *Vanderbilt Law Review* 63 (2010): 1295.

¹⁴ Lawrence Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy* (Palo Alto: Stanford University Press, 2007).

¹⁵ Neil M. Richards & Daniel J. Solove, "Prosser's Privacy Law: A Mixed Legacy," *California Law Review* 98 (2010): 1887.

¹⁶ William Prosser, *Privacy*, *California Law Review* 48 (1960): 383.

political group membership, contraceptives, abortion rights, and the possession of obscene pornography.¹⁷

There have been other privacy panics, but these two will do for my purposes here. Notice how each of these earlier privacy panics followed a similar pattern – new technologies and social practices threatened established social norms about how information could be used. This was followed by a great deal of soul-searching, a sense of crisis, and then the gradual accommodation of the new practices through a combination of regulation, acceptance, and the passage of time. Privacy was threatened, and the threat was tamed, though each time norms shifted, and the resulting society was less “private” than before, at least by the standards of the old social norms.

This brings us to the present day, in which we understand that another series of threats to privacy to signal another Death of Privacy. The continued growth of digital technologies after the 1960s produced the personal computer boom of the 1980s, the Web boom of the late 1990s, and the explosion of cell and smart phones in the 2000s. We are now witnessing the beginnings of the “Internet of Things,” in which millions and then billions of electronic devices will connect to the Internet, collecting and relaying unimaginably large amounts of data. At the same time, the terrorist attacks of 9/11 and 7/7, among others, have energized security services across the democratic world. Today we see levels of surveillance of the citizens of democratic societies that would previously have been politically and technically unimaginable. Edward Snowden and Glenn Greenwald’s revelations about the scale of surveillance by the National Security Agency have prompted a global debate about surveillance and privacy that has produced front-page news for over six months. But surely privacy

¹⁷ *Katz v. United States*, 389 U.S. 347 (1967); *NAACP v. Alabama*, [357 U.S. 449 \(1958\)](#); *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Roe v. Wade*, 410 U.S. 113 (1973); *Stanley v. Georgia*, 394 U.S. 557 (1969).

is really dead now? Surely we face the end of any notions of privacy, right?

No. I'd like to suggest, to the contrary, that Privacy Is Not Dead. Privacy is one of the most important questions facing us as a society. Privacy is actually very much alive. But it all depends on what we mean by "privacy." Privacy can of course mean many things. If we mean merely "how much information people know about us," then privacy is shrinking. But this is a very narrow and unhelpful way of understanding privacy.

Let's take a step back from the Internet of Things and digital privacy Armageddon for a moment. Certainly, many of the kinds of things we call "privacy" aren't currently threatened by new digital technologies and are very much alive. At a general level, we still put locks on our houses, we still wear clothes, and we still use doors to keep the general public out of our bathroom and bedroom. We require the government to get a warrant before it enters our home and (NSA revelations notwithstanding) wiretaps our phone, and reads our mail (whether electronic or paper). We expect our lawyers and our therapists to keep our confidences in trust, and expect our accountant and our bank to do the same with our financial details. We expect our doctors to do the same with information about our health, and while we realize that many of our health records are now electronic, we don't expect them to become available on a Google search or left lying carelessly around on a laptop at the airport. The fact that data breaches are newsworthy (and cause substantial personal, legal and business harm) supports these expectations rather than diminishes them.

What about the argument that information technology is inevitably gobbling up privacy, causing the zone of our privacy to dwindle to almost nothing? To answer that question, let's look at our previous privacy panics. Warren and Brandeis were worried

2014]

Four Privacy Myths

7

about gossip columnists and so-called “Kodakers lying in wait.”¹⁸ These phenomena still exist today, but they were managed by changes in law and social norms, and by the passage of time. Today, we have rules governing journalistic breaches (though in the United States such rules sometimes conflict with the First Amendment), and we have rules preventing stalking or overzealous tactics by the paparazzi. Similarly, commentators in the 1960s were worried by wiretapping, the creation of data banks, and the processing of personal data. These phenomena exist today, but they have also been managed (at least in their pre-internet forms) by changes in law and social norms, and by the passage of time. I’d like to suggest that our ongoing worries about the Death of Privacy (privacy’s century-old melodramatic death throes) are really an ongoing social and legal conversation about how to manage some of the costs caused by changes in information technologies.

If we think about privacy as the *scope* of information we can keep completely secret or unknown, then that kind of privacy is certainly diminishing. We are living through an information revolution, and the collection, use, and analysis of many kinds of personal data is inevitable. But if we think about privacy as the question of what *rules* should govern the use of personal information, then privacy has never been more alive. In fact, it is perhaps the most important and most vital issue we face as a society today.

Reflecting this broader understanding, legal scholars use the term “privacy” to mean at least four kinds of legal rules governing (1) invasions into protected spaces, relationships, or decisions; (2) collection of information, (3) use of information, and (4) disclosure of information. In the leading conceptual work on privacy, Daniel Solove has taken these four categories and expanded them to an occasionally bewildering sixteen categories, including surveillance,

¹⁸ Robert E. Mensel, “Kodakers Lying in Wait’: Amateur Photography and the Right of Privacy in New York, 1885-1915,” *American Quarterly* 43 (1991): 24.

interrogation, aggregation, and disclosure. These understandings are much broader than the scope of how much personal information is being recorded, and they ask not merely how much information is being collected, but how it might be used and retained, and what limits might be placed on such use and retention.¹⁹

As our information revolution develops, and new things become possible, we will likely develop new categories of privacy. We will certainly need new rules for the many new ways that information is being and will be used. But it's important not to forget that we have many such rules already. Some of these rules are ones that we typically think of as "privacy rules." For example, tort law governs invasions of privacy including peeping (or listening) Toms,²⁰ the unauthorized use of photographs for commerce,²¹ and the disclosure of sexual images without consent.²² Some states also protect against criminal invasions of privacy, as the prosecution of Dharun Ravi for recording Tyler Clementi's private sexual activities illustrated.²³ The Fourth Amendment requires that the government obtain a warrant before it intrudes on a "reasonable expectation of privacy," and is backed up by a complex web of federal and state laws regulating eavesdropping and wiretapping by both government and private actors.²⁴ In addition

¹⁹ Daniel J. Solove, *Understanding Privacy* (Boston: Harvard University Press 2008).

²⁰ *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1964).

²¹ *Agence France Presse v. Morel*, 769 F. Supp. 2d 295 (S.D.N.Y. 2011); Use of another's name, voice, signature, photograph, or likeness for advertising or selling or soliciting purposes, Cal. Civ. Code § 3344 (West)(2013).

²² *Lee v. Penthouse Int'l, Ltd.*, CV96-7069SVW (JGX), 1997 WL 33384309 (C.D. Cal. Mar. 19, 1997),

²³ N.J. Stat. Ann. § 2C:14-9 (West 2004); *State of New Jersey v. Ravi*, 2011 WL 1512060 (N.J. Super. 2011).

²⁴ *Katz v. United States*, 389 U.S. 347 (1967); Electronic Communications Act of 1986, 18 U.S.C. §§ 2510–2522 (1986); California Penal Code § 632(a).

to the Privacy Act and the Fair Credit Reporting Act, federal laws regulate the collection and use of financial information, medical and genetic information, and video privacy, among others.²⁵ States, led by California, have also added privacy protections, such as California's constitutional right of privacy (applicable to private actors), reading privacy laws, data breach notification statutes, and the recent spate of laws prohibiting employers from asking for the social media account passwords of their employees.²⁶

We have other rules that regulate the use of information that we might not typically think of as privacy rules. For example, civil rights law prohibits (among other things) the use of sensitive information such as race or gender to make hiring or promotions decisions.²⁷ Patent law regulates the use of information to design and build products – indeed, intellectual property law in general is all about regulations of the use of information.²⁸ Trade secret law allows companies to restrict access to private commercial information and grants remedies for breaches of such commercial privacy.²⁹ Even the First Amendment, long thought of as the enemy of privacy, is a kind of information rule that mandates the circumstances in which other laws cannot restrict certain free flows of information, such as the publication of true and newsworthy

²⁵ Health Insurance Portability and Accountability Act of 1996, [42 U.S.C. § 300gg](#) and [29 U.S.C. § 1181](#) *et seq.* and 42 USC 1320d *et seq.* (1996); Gramm-Leach-Bliley Financial Services Modernization Act of 1999, 15 U.S.C. §§ 6801, 6809, 6821, 6827 (1999); Video Privacy Protection Act, [18 U.S.C. § 2710](#) (1988),

²⁶ Cal Const. art. I, § 3(b)(3); Reader Privacy Act, West's Ann. Cal. Civ. Code §§ 1798.90 (2012); Disclosure of breach of security of computerized records, N.J. Stat. Ann. § 56:8-163 (West)(2013); Request for access to social networking account prohibited N.M. Stat § 21-1-46 (2013).

²⁷ Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e *et seq.* (1964).

²⁸ *Eldred v. Ashcroft*, 537 U.S. 186, 216 (2003).

²⁹ See generally Roger M. Milgrim, *Milgrim on Trade Secrets* (New York: Lexis, 9th ed., 2011).

facts by journalists, or truthful and non-misleading advertisements for lawful products.³⁰

Taking this broader perspective on “privacy” reveals that our society has some very surprising advocates for privacy. In fact, the very institutions that are usually thought of as opposing privacy for individuals often use law to secure privacy for their institutional operations. For example, consider Facebook, long thought of as being antithetical to privacy as a result of its encouragement to everyone to “share” as much of their personal information as possible to as many people as possible. But even Facebook cares about privacy. Visitors to its campus (like its employees) are required to sign non-disclosure agreements, by which they agree to keep confidential any information they learn on their visit. At a news conference at its Seattle offices recently, Facebook personnel reportedly tried to get journalists to sign an NDA before they could attend.³¹ The National Security Agency – indeed, the entire national security apparatus – is similar. While the NSA and other security agencies accumulate vast amounts of sensitive personal information in the United States and abroad, they insist on vast amounts of privacy for their own operations. This includes the secret FISA court, the “gag orders” placed upon recipients of National Security Letters and orders pursuant to section 215 of the Patriot Act, and many other legal measures. Indeed, the only reason the public knows about many of the NSA’s surveillance activities is as a result of leaks by Edward Snowden and others, which almost certainly violated laws and agreements crafted to preserve the operational privacy of the national security apparatus.

³⁰ Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, in *Intellectual Privacy*, William & Mary Law Review (forthcoming 2014), available at SSRN: <http://ssrn.com/abstract=2335196>.

³¹ Elana Zak, *Facebook Asks Reporters to Sign Non-Disclosure Agreement*, 10,000 Words, (Jan. 26, 2012, 6:14 PM), http://www.mediabistro.com/10000words/facebook-asked-reporters-to-sign-non-disclosure-agreement_b10303.

My purpose in these examples is not to pick on these organizations. On the contrary, when used appropriately, privacy rules like trade and government secret protection can advance important social interests. I am trying instead to make a point that is easy to overlook: When the very entities that are used as exemplars of the “Death of Privacy” use suites of robust legal tools to preserve their own privacy, it makes no sense to claim that privacy is dead. On the contrary, these examples show that privacy is a complex phenomenon, and that we should be talking about the balance between different kinds of privacies and different rules for managing flows of information rather than privacy’s demise. When viewed from this perspective, neither Facebook nor the NSA reject privacy; on the contrary, they have a complicated relationship to privacy, embracing (like to many other people and institutions) privacy for themselves but somewhat less privacy for others, especially where they have institutional incentives to make money or protect government interests.

Thus, when we expand our idea of “privacy” beyond embarrassing secrets to include the regulation of information flows more generally, we see that privacy – and privacy law – are very much alive. Privacy law is one of fastest-growing fields of legal practice. Indeed, as a legal specialty, privacy law is booming. Thousands of law firms in the United States alone advertise their privacy practices.³² The International Association of Privacy Professionals (IAPP), the privacy industry’s largest professional group, currently has more than 12,000 members; an increase of nearly 3,000 just since the beginning of 2012.³³ The IAPP itself attributes the exponential growth of the privacy profession to several factors, including that many different kinds and sizes of

³² Martindale, <http://www.martindale.com/Find-Lawyers-and-Law-Firms.aspx>, Practice Area Search term: “Privacy Law,” (last searched on Nov. 16, 2013).

³³ Alec Foege, *Chief Privacy Officer Profession Grows with Big Data Field*, Data Informed (Feb. 5, 2013 1:30 PM), <http://data-informed.com/chief-privacy-officer-profession-grows-with-big-data-field/>.

organizations are employing “Chief Privacy Officers” or other privacy professionals, in order to manage the legal and other responsibilities that come from holding increasingly large amount of personal data on customers, employees, and others.³⁴ In two influential studies, Kenneth Bamberger and Deidre Mulligan have documented both the establishment of the professional corporate privacy officer, the emergence of the Federal Trade Commission as a powerful regulator of consumer privacy and the development of a substantive notions of privacy by corporate professionals that contradict any suggestions of a Death of Privacy.³⁵

The important point I want make here is this: However we define privacy, it will have to do with information. And when we think of information rules as privacy rules (as we have in many cases for a very long time), we can see that digital technologies and government and corporate practices are putting many existing notions of privacy under threat. But privacy in general isn’t dying. This is because privacy is the shorthand we have come to use to identify information rules. If we were designing things from scratch, we would probably want to use a different term than privacy (“information” springs to mind, as does the accurate but unexciting European term “data protection”). But in the English-speaking world at least, “privacy” is so deeply rooted as the word we use to refer to the collection, use, and disclosure of information that we are probably stuck with it, for better and for worse.

The idea that Privacy Is Dead is thus a myth. Certain kinds of privacy may fade or become obsolete, but this is natural, because privacy is usually the product of social norms, and social norms

³⁴ International Association of Privacy Professionals, *A CALL FOR AGILITY: The Next-Generation Privacy Professional* (May 15, 2010), www.huntonprivacyblog.com/uploads/file/IAPP_Future_of_Privacy.pdf.

³⁵ Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books and on the Ground, *Stanford Law Review* 63 (2011); Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy in Europe: Initial Data on Governance Choices and Corporate Practices, *George Washington Law Review* (forthcoming 2014).

2014]

Four Privacy Myths

13

change over time and across societies. Nineteenth century notions of privacy are dead, but so, too, is everyone from the nineteenth century.³⁶ Yet the need for rules governing the uses of information persists. Legal and social rules that govern how information about us is obtained and used (broadly defined) are always necessary, and the information revolution is increasing the importance of these rules rather than decreasing them. Some of these rules will require hard choices, but a hard choice is a vital choice.

Seen from this perspective, privacy is vital, too. It is very much alive. Privacy isn't dead. Rather, privacy is inevitable.

II. PEOPLE DON'T CARE ABOUT PRIVACY

But even if the reports of privacy's death have been exaggerated, surely it is true that few ordinary people care about privacy any more? Or at least young people have given up on privacy, right? The exponential growth of social networks like Facebook and Twitter, in which users share increasing amounts of personal information, the rise of "sexting," and the perceived willingness of us all to trade our personal information for convenience and safety all seem to suggest that public interest in privacy is on the decline. More pointedly, many observers have suggested that because young people have eagerly embraced digital technologies and social networks, they care even less about privacy than older generations.³⁷

³⁶ At the time of writing, there are only five people on Earth verified to have been born before 1900. Wikipedia, *Oldest People*, https://en.wikipedia.org/wiki/Oldest_people#Ten_verified_oldest_people_living (Nov. 19, 2013).

³⁷ Janet Kornblum, *Online privacy? For young people, that's old-school*, USA Today, Oct. 22, 2007, available at http://usatoday30.usatoday.com/tech/webguide/internetlife/2007-10-22-online-privacy_n.htm.

There is some empirical evidence to back up such notions. A 2013 government study of British internet users suggested that British adults have become less concerned about online privacy over the past decade; whereas 70% of those surveyed in 2005 were concerned about online privacy, now only 52% responded similarly. Of course, 52% is still a majority, and it is difficult for surveys to probe exactly what “concerned about privacy means” – whether it is a fear that one’s name and address is vaguely “out there” or a more nuanced concern about the effects of databases being used to profile, sort, and nudge consumers and citizens towards behaviors corporations and governments might desire.

Privacy is notoriously difficult to define, and this definitional looseness no doubt contributes to ambiguity in consumer surveys. When asked whether they care about privacy, are consumers thinking about the fact that their tweets can be read by the world, the fact that Google is serving ads to them based upon a transcript of their web-surfing, or the fact that the government is logging the recipients of all their emails and telephone calls? This imprecision is reflected in other surveys finding that consumers do care about online privacy, and that they are often unaware of issues like Do Not Track or the protections afforded by privacy law. Several studies suggest that consumers believe that privacy law is more protective of them than is actually the case; for example, one prominent study showed that most consumers incorrectly believe that websites with privacy policies cannot share data about them without their consent.³⁸

Nevertheless, there does seem to be some truth to the idea of a “privacy paradox”: the idea that people indicate a concern about privacy in general, but then act in ways that might seem contradictory; for example by selling their personal information

³⁸ Chris Jay Hoofnagle & Jennifer King, *What Californians Understand About Privacy Online*, Sept. 3, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130.

very cheaply in practice.³⁹ There could be several explanations for this discrepancy. Consumers could be misled by the terms of transactions in which they hand over their data. They might undervalue the risks of over-sharing data, or of the value of their data, especially in contexts where a “free” service is offered in exchange. They might be coaxed by highly persuasive interfaces that use sophisticated testing models to be as effective as possible, or which limit their ability to make meaningful choices about their privacy.⁴⁰ Or it may simply be that while consumers sincerely value their privacy in the abstract, in the bustle of their everyday lives the bewildering need to check and re-check privacy settings can be too much. This latter explanation suggests that the regime of “privacy self-management” – the idea that consumers must manage a system of dense privacy policies, hidden opt-outs, and ever-changing settings – might be a failure, and that we need something better to replace it.⁴¹ This could be a generally-applicable consumer privacy law like virtually every other democracy has, or it could be more specific default rules that track consumer expectations. There is certainly substantial anecdotal and empirical evidence to support the proposition that consumers are bewildered and concerned by the difficulties of managing their privacy in practice.⁴² One notable study found that merely to read all of the privacy policies an average

³⁹ Patricia A. Norberg, Daniel R. Horne, and David A. Horne, “The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors,” *Journal of Consumer Affairs*, 41(1) (2007): 100-26.

⁴⁰ Dixon, P., Gellman, R., “Online Privacy: A Reference Handbook” (2011), e-book, accessed 24 September 2013, <http://wustl.eblib.com.libproxy.wustl.edu/patron/FullRecord.aspx?p=766988>: 15 – 16.

⁴¹ Daniel J. Solove, “Privacy Self-Management and the Consent Dilemma,” *Harvard Law Review* 126 (2013): 1880.

⁴² Mary Madden & Aaron Smith, *Reputation Management and Social Media*, Pew Internet & American Life Project (May 26, 2010), <http://www.pewinternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx>, at 6; McGraw Hill Financial Global Institute, *Consumers: Losing Control of Online Privacy* (Oct. 30, 2013), <http://www.mhfigi.com/societal-trends/consumer-concerns-about-data-privacy/>.

Internet user encounters in a year would take 76 work days.⁴³ Thus, while more study of it is certainly needed, the “privacy paradox” is thus more likely a symptom of our ineffective system of privacy management than anything else.

Of course, the trump card in the “People Don’t Care About Privacy” argument is young people. Even if older people, the argument goes, care about privacy, our young generation of digital natives certainly don’t. Young people growing up with digital communications technologies care much less about privacy, with their lives shared, tweeted, and Instagrammed extensively.⁴⁴ One journalistic account of young people’s privacy preferences expressed this sentiment aptly:

“Kids today. They have no sense of shame. They have no sense of privacy. They are show-offs, fame whores, pornographic little loons who post their diaries, their phone numbers, their stupid poetry—for God’s sake, their dirty photos — online. They have virtual friends instead of real ones. They talk in illiterate instant messages. They are interested only in attention—and yet they have zero attention span, flitting like hummingbirds from one virtual stage to another.”⁴⁵ As the CEO of Disney put it more succinctly,

⁴³ See Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4.3 I/S: A Journal of Law and Policy for the Information Society (2008): 540; see also Alexis C. Madrigal, *Reading the Privacy Policies You Encounter In a Year Would Take 76 Work Days*, The Atlantic, March 1, 2012, available at <http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>.

⁴⁴ Shea Bennett, *Tumblr, Facebook, Twitter, Instagram & Snapchat – How Teens Use Social Media [INFOGRAPHIC]*, All Twitter: The Unofficial Twitter Resource (Oct. 18, 2013), http://www.mediabistro.com/alltwitter/teens-social-media_b50664.

⁴⁵ Emily Nussbaum, *Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll*, New York Magazine, Feb 12, 2007, available at <http://nymag.com/news/features/27341/>.

2014]

Four Privacy Myths

17

when it comes to privacy, “kids don’t care...they can’t figure out what I’m talking about.”⁴⁶

It may be trendy to talk anecdotally young people who seem not to care about privacy, but there is a substantial body of evidence demonstrating that it, too, is a myth. Young people *do* care about privacy; in fact, they often are much more sophisticated about privacy – and digital privacy – than their elders. Young people do look at privacy differently, but those differences as much as anything else reflect their sophistication about the importance of practical privacy management in their lives. In their study of young people’s attitudes towards privacy, Hoofnagle et al. found that young people care as deeply about privacy as their elders, and that they might even be more vigilant and more likely to engage in privacy-protective behaviors (such as supplying false information) than older people.⁴⁷ There is further empirical evidence that young people are more likely to engage in sophisticated tweaking of the privacy settings they are given on social networks than older people.⁴⁸

Young people might certainly share information about themselves that shocks their elders,⁴⁹ but young people doing sometimes risky things to shock old people has been the defining characteristic of youth culture for the past fifty years. In reality,

⁴⁶Gina Keating,, *Disney CEO bullish on direct Web marketing to consumers*, Reuters (July 23, 2009, 12:26 AM) <http://www.reuters.com/article/2009/07/23/us-media-disney-idUSTRE56MoZY20090723?pageNumber=1&virtualBrandChannel=0>.

⁴⁷ Chris J. Hoofnagle, Jennifer King, Su Li, & Joseph Turow, *How Different are Young Adults From Older Adults When it Comes to Information Privacy Attitudes and Policies?* (2010), available at SSRN: <http://ssrn.com/abstract=1589864> or <http://dx.doi.org/10.2139/ssrn.1589864>, at 10.

⁴⁸ Marwick, A., Murgia-Díaz, D., and Palfrey, J., “Youth, Privacy and Reputation” (2010): 33.

⁴⁹ Henley, J., “Are teenagers really careless about online privacy?”, *The Guardian* (Oct 21 2013). Available at: <http://www.theguardian.com/technology/2013/oct/21/teenagers-careless-about-online-privacy>

young people care deeply about privacy, but they care about privacy in a different way that reflects their outlook on life. Sociologists danah boyd and Alice Marwick explain that young people's concern about privacy is less about privacy against their peers, and much more about privacy against the perceived authority figures in their lives – their parents, teachers, and (for older ones) potential employers.⁵⁰ By contrast, young people enthusiastically embrace electronic platforms as a way to meet like-minded young people, to experiment with identity, to create a social space defined by young people and not by adult parents and teachers, and because they see the benefits of connectivity, including the small chance that they might “go viral” or become a micro-celebrity.⁵¹ Although some of these goals require the sharing of sometimes intimate personal information with others, none of them necessarily equate to a lack of concern with privacy. Indeed, in their engagement in the processes of “boundary management” with multiple publics, boyd and Marwick suggest that young people are both more concerned with privacy and have a more sophisticated understanding of the nuances of information flows in digital social environments.⁵²

Why, then, if young people care deeply about privacy, have some journalistic and popular accounts of young people's privacy preferences focused on their apparently privacy-denying behavior? One explanation is that young people frequently engage in risky behavior with a diminished sense of the likelihood of negative future consequences. From this view, why should risky privacy behavior be any different from other risky behaviors including sex, alcohol and drugs, or reckless driving? Another explanation is that

⁵⁰ boyd, d. and Marwick, A. E., “Social Privacy in Networked Publics...” (2011): 15.

⁵¹ boyd, d. and Marwick, A. E., “Social Privacy in Networked Publics...” (2011): 15; see also Marwick, A., Murgia-Díaz, D., and Palfrey, J., “Youth, Privacy and Reputation” (2010): 13;

⁵² *Id.*

the social networks that teens and other young adults encounter are engineered by default to be more public. From this view, all people, including young people, have a range of limited choices when it comes to privacy. In their study of young people's engagement with social networks, boyd and Marwick explain that social dynamics in the physical world are typically "private-by-default, public-through-effort."⁵³ It is difficult to get to know people in the physical environment, and personal information requires effort to obtain. But by contrast, in an online environment in which social networking companies have a financial incentive to maximize the amount of personal information that is disclosed (in order to sell more and better advertisements), the model of privacy is public-by-default, private-through-effort. Faced with such radically altered default settings and a limited range of choices, it should thus be no surprise that young people appear to be less privacy-conscious.

As with the Death of Privacy, a closer look at public attitudes towards privacy shows that the reality is far more complicated than the simple mantra that people no longer care about privacy. A more accurate interpretation of the available evidence suggests that people do in fact care about privacy, but they are bewildered by the difficulty of protecting their personal information in a time of rapid technological change and limited options. Indeed, the myth that People Don't Care About Privacy suggests a kind of reverse privacy paradox – if people really don't care about privacy, why do they talk about it so much? After all, if we didn't really care about privacy, it wouldn't be regular front page news, books on privacy wouldn't sell, and it would not be a major topic of public debate.

More fundamentally, the debate about whether people do or do not care about privacy obscures a much more important point: In the English-speaking world, we are using the word "privacy" to capture our anxiety about many of the changes that the digital

⁵³ boyd, d. and Marwick, A. E., "Social Privacy in Networked Publics..." (2011): 10.

revolution has enabled. I argued in response to the myth that Privacy Is Dead that we should think about “privacy” as more than merely nineteenth-century fears of unwanted publicity. When we think about privacy more broadly as the ability of people to participate in how their personal information is collected, processed, and used, it becomes clear that people (and young people) definitely care about this problem. They care deeply about it, because it is one of the defining questions of our age.

III. IF YOU HAVE NOTHING TO HIDE, YOU HAVE NOTHING TO FEAR

How people understand privacy is crucially important to understanding a third myth about privacy, which is the oft-repeated belief that People with Nothing to Hide Have Nothing to Fear. On this view, privacy is no more than the ability to hide unpleasant truths about ourselves from the public. And it follows from this assumption that privacy is only for those of us with dark secrets. It is the protection for a misbehaving minority; a kind of false advertising of one’s character and reputation. As Richard Posner famously put it, privacy is no more than a person’s “right to conceal discreditable facts about himself.”⁵⁴

But the Nothing to Hide argument is a myth. Most of the time, it is just false. More importantly, though, it is a misleading way of thinking about the issues that privacy raises in digital societies. It frames the question of privacy in ways that ignore the reasons why privacy matters. And it does this in three separate ways.

First, all of us have “something to hide”; or at least information that we don’t want to have broadcast to the world. Few people would be comfortable with having images of their activities in the bedroom or bathroom made public, even where those

⁵⁴ Richard A. Posner, *Economic Analysis of Law* (New York: Aspen, 5th ed. 1998): 46.

activities are common to all or to many. In particular, disclosure of facts or images about our naked bodies or sex lives would be psychologically catastrophic to many people. Rutgers University freshman Tyler Clementi infamously jumped to his death from the George Washington Bridge when his roommate shared a video stream of him being intimate with another man in his dorm room.⁵⁵ And as cameras become ubiquitous (and also a part of many people's sex lives⁵⁶), the problem of "revenge porn" has become a national problem, in which (usually) men disclose videos of their former lovers engaged in sex acts. As legal scholar Danielle Citron puts it, "[r]evange porn is as harmful to the person who shared intimate photos with a trusted loved one as the person whose picture was taken by someone else and then disclosed without consent. Sharing sensitive information with a confidante does not waive one's privacy expectation in the information."⁵⁷

Another category of information many people would want to keep secret are their intellectual activities, especially their tastes in books or films. Reading and thinking are the core of a free society, and the foundation for a robust exercise of First Amendment rights.⁵⁸ Thus, when Judge Robert Bork was nominated to the Supreme Court in 1987, his controversial beliefs that there was no right to privacy caused an enterprising reporter for the Washington

⁵⁵ Neil M. Richards, *The Limits of Tort Privacy*, *Journal of Telecommunications & High Technology Law* 9 (2011): 357; Ian Parker, *The Story of a Suicide*, *The New Yorker*, February 6, 2012, available at http://www.newyorker.com/reporting/2012/02/06/120206fa_fact_parker.

⁵⁶ Jonathan Freedland, *Are Smartphones Causing A Bonking Crisis?*, *The Guardian*, November 26, 2013, available at <http://www.theguardian.com/commentisfree/2013/nov/26/smartphones-bonking-crisis-british-less-sex-technology>.

⁵⁷ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Boston: Harvard University Press, forthcoming 2014): ms. 143.

⁵⁸ Neil M. Richards, *Intellectual Privacy* (New York: Oxford University Press, forthcoming 2014).

City Paper to find and publish his movie-watching history.⁵⁹ While the most embarrassing movie on Bork's account was John Hughes' *Sixteen Candles*, the episode caused Congress to pass the Video Privacy Protection Act. Congress no doubt feared the disclosure of more salacious titles rented by members of the House and Senate – fears that the selective disclosure of their intellectual pursuits might cause people to be judged out of context.

More generally, intellectual privacy like that afforded by movie or reading privacy protections is an important civil liberty. It allows us mental breathing space to experiment with unpopular, dangerous, or even deviant ideas, from politics to sex to religion. Many people who fear that their intellectual activities are being monitored will restrict them to the mainstream, the conventional, and the boring. Such self-censorship has effects not only on what people read but on what they write and say. For example, one recent survey of over 500 American writers found that the fear of government surveillance had caused many of to curtail what they read, write, and say.⁶⁰ And when writers are chilled in their own liberties of thinking and expression, society as a whole is deprived of the insight of their views.

Mere surveillance of our reading can be used to deter, but disclosure of those habits can also be used to discredit or destroy. In late 2013, the *Huffington Post* reported that the U.S. government was monitoring the web-surfing habits of clerics and academics who spoke about their radical Islamic beliefs. Although the subjects of surveillance were speakers and not terrorists, data on their preferences in pornography was being collected in order to disclose it and thereby discredit them. One enthusiastic supporter of this

⁵⁹ Michael Dolan, *The Bork Tapes Saga*, *The American Porch: An Informal History of an Informal Place*, <http://theamericanporch.com/bork2.htm>. See generally Neil M. Richards, *The Perils of Social Reading*, 101 *Geo. L. J.* 689 (2013).

⁶⁰ PEN America, *Chilling Effects: NSA Surveillance Drives Writers to Self-Censor* (November 12, 2013), available at http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

policy argued that “dropping the truth on them” was better than dropping a bomb on them.⁶¹ Of course, democratic governments aren’t allowed to censor speakers they disagree with (much less bomb them). But the threat of disclosure of embarrassing reading habits can be used to censor indirectly. Such a threat is not limited to terrorists or radical speakers, particularly if surveillance of reading habits or political views by governments or private actors is widespread.⁶² If we care about vibrant public debate, we must care about intellectual privacy. After all, in a free society, there is no such thing as a bad (or even a discreditable) idea.⁶³

A second reason why the “Nothing to Hide” argument is misleading is that it reduces privacy to an individual’s right to hide big secrets. Such a crude reduction of the issue ignores both the complexity of privacy, as well as the social value that comes from living in a society that not everything about us is publicly available all of the time. This is the insight of legal scholar Daniel Solove in his book “Nothing to Hide.” Solove shows how thinking of privacy as the hiding of discreditable secrets by individuals is a mistake because privacy is about more than hiding secrets, and can mean a wide variety of things. Moreover, he notes that “privacy is “often eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone.”⁶⁴ Privacy, in this view, is a social value rather than merely an individual one. Rather than thinking about privacy as merely the individual right to hide bad deeds, we should think more broadly about the kind of society we

⁶¹ Glenn Greenwald et al., *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit ‘Radicalizers’* The Huffington Post (Nov. 26, 2013, 11:20 PM), http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html.

⁶² Neil M. Richards, “*The Perils of Social Reading*,” *Georgetown Law Journal* 101 (2013): 689.

⁶³ Neil M. Richards, *Intellectual Privacy*,” *Texas Law Review* 87 (2008): 387.

⁶⁴ Daniel J. Solove, *Nothing To Hide: The False Tradeoff Between Privacy and Security* (New Haven: Yale 2011): 30.

want to live in. A society in which everyone knew everything about everyone else would be oppressive because it would place us all under the glare of publicity all the time; there would be no “free zones for individuals to flourish.”⁶⁵ Legal scholar Julie Cohen goes further, arguing that privacy is necessary for humans to be able to decide who they are. In Cohen’s account, our selves are fluid, constantly being built and changed by our activities, thoughts, and interactions with other people. Privacy, in her view, shelters the development of our dynamic selves “from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable.” Privacy protects our ability to manage boundaries between ourselves and others so that self-determination is possible.⁶⁶ It helps us avoid the calculating, quantifying tyranny of the majority. Privacy is thus essential for individuality and self-determination, with substantial benefits for society.

Third, reducing privacy to an individual right to hide dark secrets ignores the power effects of privacy. Information is power, and knowing information about someone gives power over them – the power to blackmail, persuade, and classify. Let’s take blackmail first. As the example of the NSA porn surveillance reveals, secrets can of course be used to blackmail or silence. Such occurrences are regrettably common even in democratic societies. As I have written about elsewhere, the FBI’s surveillance of Martin Luther King, Jr.’s communications produced evidence of marital infidelity that it used to blackmail him.⁶⁷ But blackmail can occur beyond secrets we want to hide. “Revenge porn” nude or sexual images are often used to blackmail or silence former lovers. Other kinds of non-embarrassing personal information are also a threat in the wrong

⁶⁵ *Id.* at 50.

⁶⁶ Julie E. Cohen, “What Privacy Is For,” *Harvard Law Review* 126 (2013): 1905.

⁶⁷ Neil M, Richards, *The Dangers of Surveillance*, *Harvard Law Review* 126 (2013): 1934.

hands, such as financial information or account passwords. None of these are dark secrets we want to hide, but their revelation or the threat of identity theft can be used for blackmail purposes.

More fundamentally, small or large collections of personal information can be used to persuade others to do our bidding. Businesses that hold a lot of information about us can market to us more persuasively, potentially reaching us at a moment of weakness when our guard is down. Such practices might not be illegal under current law; indeed, depending on one's view of consumer rights, they might also be unproblematic from a policy perspective. But they certainly change the power relationships between those who hold personal information and the subjects of that data. Existing consumer protection law is based upon the idea that certain kinds of power differentials can be problematic in the marketplace, which is why we require labelling and ingredient lists, and forbid practices like redlining, coercive installment contracts,⁶⁸ negligence waivers,⁶⁹ or coercive company stores.⁷⁰ Consumer protection law forbids not just deceptive acts, but those that are unconscionable – those that are characterized by a lack of meaningful choice on the part of the consumer or by a gross inequality in bargaining power.⁷¹ Consumer profiles backed by so-called “big data analytics” enable

⁶⁸ *Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 445 (D.C. Cir. 1965).

⁶⁹ *Tunkl v. Regents of the U. of Cal.*, 383 P.2d 441 (Cal. 1963).

⁷⁰ Price J. Fishback, *Did Coal Miners Owe Their Souls to the Company Store?*, *Journal of Economic History* 46 (1986): 1101. This type of practice has been outlawed by laws such as Ohio Rev. Code Ann. § 4113.18 (West)(2013).

⁷¹ See, e.g., Kan. Stat. Ann. § 50-627 (West)(2013)(forbidding suppliers from taking “advantage of the inability of the consumer reasonably to protect the consumer's interests because of the consumer's...ignorance,...inability to understand the language of an agreement or similar factor); Idaho Code Ann. § 48-603C (West)(2013)(permitting the court to take into account “whether the alleged violator knowingly or with reason to know, induced the consumer to enter into a transaction that was excessively one-sided in favor of the alleged violator” when determining if an act, practice, or method is unconscionable).

exactly this kind of enhanced persuasion. This is something I have elsewhere called the “Power Paradox” of big data –big data analytics are powerful, but that power is typically wielded by those who are already powerful.⁷² Communications scholar Joseph Turow makes a similar point – while our new digital technologies are usually framed as giving us enhanced choice, the reality is very different. Businesses using consumer profiles that most people don’t know exist can tailor content to persuade and influence those people, often without them knowing about it.⁷³

The persuasive effects of data-based marketing have not been limited to commerce, and have started to influence the political process. The Obama Campaign was feted after the 2012 Presidential Election for its use of data-based analytics to target its campaign advertising, outreach, and other efforts. Spearheaded by University of Chicago data scientist Rayid Ghani, the campaign used publicly-available data from voter records to plot the electorate on a grid and used analytic techniques to segment the electorate, assessing how likely each voter was to vote for Obama and Romney, and then assessing them for persuadability.⁷⁴ On the one hand, the use of new technologies by political campaigns is nothing new. But on the other, the use of these new technologies to segment, sort, identify, and persuade voters heralds a new kind of political persuasion, one based upon targeting and data rather than speaking and canvassing. Surely banning the use of data by campaigns would be impossible as a practical (or likely a constitutional) matter. It might not even be good policy even if we

⁷² Neil M. Richards & Jonathan H. King, “Three Paradoxes of Big Data,” *Stanford Law Review Online* 66 (2013): 41, available at http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_41_RichardsKing.pdf.

⁷³ Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (New Haven: Yale 2012).

⁷⁴ Jonathan H. King, *The New Washington Data Grid*, jhking.com (Sept. 16, 2013), <http://jhking.com/2013/09/16/the-new-washington-data-grid/>.

could. But my point is to highlight the increased persuasive power that data-based analytics give to already powerful entities – advertisers, corporations, political machines, and government entities. Assessing the degree to which these developments are a problem is impossible if we think about privacy or information rules as only hiding discrete pieces of discreditable information about ourselves.

The segmenting power of data analytics suggests a third power effect that personal data can enable – the power to sort. In an influential 1993 book, sociologist Oscar Gandy described the digital privacy revolution as ushering in something he called “The Panoptic Sort.”⁷⁵ Gandy used this term to mean the use of large datasets by government and private bureaucracies to classify, assess, and sort individuals for analysis and control – a system of power based upon personal information. More recently, Joseph Turow has illustrated the even more powerful sorting ability that two decades of computer and data science have enabled. Today, personal data is used to classify and sort us all.⁷⁶

On the one hand, the increased efficiency of sorting enabled by the information revolution has many useful applications. Large-dataset analytics has many powerful applications that don’t even use personal data, such as weather and traffic forecasting, the design of better automotive components, spell-checkers, and search engines.⁷⁷ Analytics based on personal data are useful, too, enabling better decisions in the medical, credit and insurance contexts, as well as the prevention of terrorism and other crimes.⁷⁸

⁷⁵ Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press 1993).

⁷⁶ Turow, “The Daily You...”

⁷⁷ Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, And Think* (New York: Houghton Mifflin, 2013).

⁷⁸ Omer Tene & Jules Polonetsky, “Privacy in the Age of Big Data: A Time for Decisions,” *Stanford Law Review Online* 64 (2012) 63, available at http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf.

But this increased power to sort can be used for bad or morally ambiguous purposes as well. Lawyers have another word for this kind of sorting, which is “discrimination.” Consider the use of consumer profiles to determine the likelihood we would buy products at a given price. Such relatively simple analytic techniques could enable a website (say, like Amazon.com) in which all prices were optimized to the highest value we might be willing to pay. Sophisticated analytics could also raise the spectre of a new kind of “redlining” – the denial or discrimination of services to people on the basis of race or other suspect criteria. Of course, predictive analytics need not use race directly; they could be designed to ignore race and use other variables that correlate with race. Or perhaps such algorithms might not use race indirectly, but impose a brutal individualized economic rationalism upon us all as consumers and citizens.

Thankfully, the strong form of that society is not upon us yet, but some of its weaker cousins are. And if we dismiss the problems caused by privacy or personal data as nothing more than bad people hiding bad deeds, we will miss the transformative power effects of the digital revolution entirely. For better or worse, we use the term “privacy” as a shorthand to capture all of the issues raised by personal data. As a result, privacy is not just for those of us with something to hide. Of course, we all have something to hide. But more fundamentally, questions of privacy include many of the most fundamental questions of civil liberties, economic, and political power in a digital society. From that perspective, privacy is for everyone.

IV. PRIVACY IS BAD FOR BUSINESS

Let’s say you agree with me so far. Let’s concede for purposes of argument that privacy is alive, that people care about it, that it’s broader than hiding discreditable information, and that it’s not merely censorship in another guise. All this means is that the

choice to protect privacy is a policy choice; it is a choice that we could make, but it is also one that we need not make. It's at this point in debates about privacy that the policy trump card gets played: privacy might be something people want, but it's bad for business. Privacy gets in the way of technological innovation; it's a kind of tax on progress. We have a free Internet built on personalized advertising, which requires that businesses know about the people surfing the web. We also have all sorts of free mobile applications and other services that are paid for by eyeballs. If we stopped or slowed the free flow of personal information, our digital revolution could grind to a halt. Privacy is bad for business.

At the outset, there are a few problems with this claim, such as the idea that maybe our information policy shouldn't be entirely geared towards what is good for business. But let's talk about the "free" Internet first. We hear a lot about the "free" Internet, and "free" apps and services. Consider Facebook's promise, featured prominently on its web sign-up page that "It's free and always will be."⁷⁹ Of course, Facebook isn't really "free." Consumers don't pay money to use the Facebook service, but they can't use it without giving Facebook the right to collect and use often vast amounts of personal information about them. Facebook collates and uses such personal information to target advertisements to its users. It encourages its users to share information about themselves, and those users are then sold to Facebook's real customers, its advertisers. Some observers have termed this arrangement "digital sharecropping" rather than "free stuff."⁸⁰ But however we characterize it, when personal information is bartered for access (whether users know that or not), an economic exchange is taking place. When that's happening, it's misleading to call such services

⁷⁹ Facebook, www.facebook.com.

⁸⁰ *E.g.*, Nicholas Carr, *The Economics of Digital Sharecropping*, RoughType.com, (May 4, 2012, 10:11 AM), <http://www.roughtype.com/?p=1600>.

“free.” In fact, there is good evidence from the behavioral sciences that calling something “free” tends to cause consumers to make irrational choices, overvaluing the benefits of “free” goods and ignoring the costs.⁸¹

Debunking the idea of the “free” internet is important because it shows the extraordinary economic value of personal information. Much of the popular rhetoric of the internet suggests that nothing much of value is transferred by users. Any individual piece of personal data may have minimal value, but vast amounts of tiny value add up. Indeed, the sheer size of Internet fortunes based upon personal information demonstrates this point nicely. Facebook’s Initial Public Offering was valued at \$104 billion, and its only real assets were its users, their data, and their eyeballs as viewers of advertising.⁸² One recent study estimated that each user’s data is worth \$98 Facebook, roughly equivalent to the values for LinkedIn (\$93) and Twitter (\$110).⁸³ So rather than thinking about the Internet as services provided for free, we should think of them as they are – as companies making money from personal information that has substantial value.

This brings us back to the idea that Privacy Is Bad for Business or is anti-innovation. From a narrow perspective, requiring businesses to account for privacy might make things more expensive. After all, if personal information collected or harvested from users is valuable, restrictions on what information businesses

⁸¹ *E.g.*, Kristina Shampa’ner, Nina Mazar, & Dan Ariely, *Zero as a special price: The true value of free products*, 26 *Marketing Science* 742, available at <http://people.duke.edu/~dandan/Papers/PI/zerofree.pdf> and Chris Jay Hoofnagle & Jan Whittington, “The Price of ‘Free’: Accounting for the Cost of the Internet’s Most Popular Price,” *UCLA Law Review* (forthcoming 2014).

⁸² Andrew Tangel & Walter Hamilton, *Stakes are high on Facebook's first day of trading*, *The Los Angeles Times*, May 17, 2012.

⁸³ George Anders, *A Twitter User Is Worth \$110; Facebook's \$98; LinkedIn's \$93*, *Forbes.com* (Nov. 7, 2013, 2:28 PM), <http://www.forbes.com/sites/georgeanders/2013/11/07/a-twitter-user-is-worth-110-facebooks-98-linkedins-93/>.

can collect or how they can use it would cut into profits. If Facebook, Twitter, or LinkedIn had to pay their users even a fraction of what their data was worth, it would get very expensive very quickly. From this perspective, privacy rules are a kind of tax on both innovation and profitability. This is a common refrain heard from business groups. (A perhaps flippant response to this argument might be that paying employees fairly for their labor is also a kind of a tax on profitability, but one that the law requires.)

More fundamentally, viewing privacy rules as a tax ignores the importance of trust in the digital environment. Customers share their data with companies under the expectation that it will be treated ethically and responsibly. There is good evidence that consumers share because they think that privacy law is considerably more protective than it really is; for example that the existence of a privacy policy means that personal information will not be shared or sold to others without their actual consent.⁸⁴ There is also evidence that the presence of privacy controls in computer interfaces makes individuals more likely to share their personal information.⁸⁵ This is an insight that has long pedigree in our legal system. Some of our oldest privacy rules, including the duties of professional confidentiality, reflect an understanding that trust promotes the sharing of information. I have elsewhere called this idea the *information-sharing function of confidentiality*.⁸⁶ To get better medical, legal, or other advice, we need to tell the truth, to

⁸⁴ Chris Jay Hoofnagle & Jennifer King, *Research Report: What Californians Understand About Privacy Offline*, May 15, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075; Chris Jay Hoofnagle and Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev. (forthcoming 2014).

⁸⁵ Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, Presentation at Workshop on the Econ. of Info. Sec.: Negative Information Looms Longer than Positive Information, (June 14, 2011), available at <http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf>.

⁸⁶ Neil M. Richards, *The Perils of Social Reading*, 101 Geo. L. J. 689 (2013).

share fully and frankly. But because information is power, sharing information frequently puts us at the mercy of our confidante, who can use this information to their benefit or our detriment. Confidentiality solves both problems, letting us get better advice and protecting us from being taken advantage of by our confidantes.⁸⁷

But confidentiality protects our professional confidantes as well, though this is a feature of confidentiality that is easy to overlook. To stay with the example of doctors and lawyers, if their clients Confidentiality – privacy rules – are thus a huge asset to confiders and confidantes, professionals and their clients. They are an elegant solution to the fact that information is power. That solution is the insight that confidentiality of information promotes trust, reliance, and investment in the relationship. Confidentiality rules help to guarantee that the professional won't abuse the power difference with her client. And the information-sharing function of confidentiality encourages more information to flow to the professional, allowing her to provide better advice. Confidentiality thus promotes trust and improves the quality of the professional services on offer. The very word "confidentiality" implies this double meaning, for when we share a *confidence* we trust our confidante; quite literally, we have *confidence* in their discretion.

No doubt because of these mutually-beneficial features, confidentiality rules are well-established in the older information professions including law, medicine, librarianship, the priesthood, and psychology. They are starting to take root in our newer information professions as well. As noted earlier, the past decade has seen the rise of the "Chief Privacy Officer," a senior executive responsible for managing the legal and other risks of a company's personal information management policies. The rise of the CPO has also been reflected in the remarkable growth of organizations

⁸⁷ *Id.*

like the Future of Privacy Forum and the larger International Association of Privacy Professionals. The IAPP's mission is to help "organizations manage and protect their data," and its members include CPOs at large and small corporations, partners at law firms, and general counsel at companies of various sizes. Scholars studying the rise of the CPO position have concluded that CPOs (and privacy professionals more generally) self-consciously fulfil an important regulatory role within companies even in the absence of formal legal rules for the management of personal information.⁸⁸ They conclude that much of the impetus for the creation of internal mechanisms and professionals to manage information practices are the privacy expectations of their own customers. As one leading privacy professional puts it, from a CPO's perspective, "[t]he end objective in my mind is always what's the right thing to do to maintain the company's trusted relationship with our employees, with our clients, with any constituency in society that has a relationship to us, which is probably pretty much any constituency."⁸⁹

At the same time, privacy also represents an opportunity for companies on which they can compete with each other by innovating on privacy and trust. A recent ACLU report suggests ways in which a demonstrable commitment to privacy and other ethical information processing practices is essential for the long-term sustainability of technology companies. According to the report, which relies on case studies of corporate privacy practices, companies that safeguard their users' privacy can "increase use and consumer spending," and "generate positive press and create customer loyalty."⁹⁰ The report also notes the insight of Bamberger

⁸⁸ Kenneth A. Bamberger & Deidre K. Mulligan, *Privacy on the Books and on the Ground*, Stanford Law Review 63 (2011): 247, available at <http://www.stanfordlawreview.org/print/article/privacy-books-and-ground>, at 249-54.

⁸⁹ *Id.* at 271.

⁹⁰ ACLU of Northern California, *Privacy & Free Speech: It's Good For Business*, (Nicole A. Ozer, ed. 2d ed. 2012), available at

and Mulligan that even though legal safeguards in the United States for personal information currently lag behind technological advances, customers expect (and often demand) that the businesses with which they deal engage in ethical custodianship of their personal information. The report concludes that “[a]s consumers become more aware of the consequences of online activity and are faced with an ever-expanding array of options, they will increasingly demand products that are not only innovative but also protect their privacy,” and notes that the relative maturation of the digital technology sector presents companies with an opportunity to innovate and compete on privacy grounds.⁹¹

The importance of privacy as customer trust has been illustrated most clearly by the effect of the Snowden revelations on the goodwill of the American technology industry. One of the earliest and most controversial revelations by *The Guardian* was that most of the major U.S. cloud and internet companies had been participating in the National Security Agency’s PRISM program, under which they shared large amounts customer information with the government.⁹² Some smaller technology companies closed their doors rather than participate with what they considered to be such an egregious breach of user trust. Ladar Levison, the owner of secure email company Lavabit, halted operations of his company and posted an open letter to his customers suggesting that he had been forced to disclose the contents of customer emails to the government.⁹³ Another secure communications provider, Silent

http://www.aclunc.org/docs/technology/privacy_and_free_speech_it's_good_for_business.pdf, at 1.

⁹¹ *Id.* at 27.

⁹² Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google, and others*, *The Guardian*, June 6, 2013, available at <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

⁹³ Lavabit, <http://lavabit.com/> (last visited Oct. 24, 2013). See also Michael German, *America, NSA Surveillance is Bad for Business*, ACLU (Aug. 13, 2013), <https://www.aclu.org/blog/national-security-technology-and-liberty/america-nsa-surveillance-bad-business> (quoting open letter on lavabit.com).

Circle, also shut down its e-mail service, stating that it had “not received subpoenas, warrants, security letters, or anything else by any government,” but that it was acting preemptively before it was forced to adhere to such requests.⁹⁴ With trust undermined by seemingly unfettered U.S. government access, American technology companies started to lose the trust of their users, especially those users in other countries. The technology giants got the message, and within a few months of the Snowden revelations had begun to advocate and lobby for limitations on government surveillance of their users. In an open letter of their own, a website, and advertisements in major newspapers, eight of the leading internet companies, led by Google and Microsoft, spoke out against government surveillance. As the general counsel of one of the companies put it aptly, “people won’t use technology they don’t trust.”⁹⁵

The Snowden revelations, of course, involve government surveillance, rather than data collection and use by the companies themselves. And it is precisely because large internet companies collect and retain so much personal information that government security services so eagerly look to access their servers. But the Snowden affair reveals that companies are beginning to understand how important customer trust is to their businesses, and how integral privacy rules – the ethical collection and use of personal information – are to those businesses. Along with the rise of the CPO and a broader ethical sensibility with respect to personal data, it also suggests that privacy will be a space in which competitive innovation can occur among businesses in the future. Just as the information trade and data analytics have been a spur to innovation, allowing things like Google search, Amazon.com, and

⁹⁴ Michael German, *America, NSA Surveillance is Bad for Business*, ACLU (Aug. 13, 2013), <https://www.aclu.org/blog/national-security-technology-and-liberty/america-nsa-surveillance-bad-business> (quoting open letter on lavabit.com).

⁹⁵ Edward Wyatt & Claire Cain Miller *Tech Giants Issue Call for Limits on Government Surveillance of Users*, N.Y. Times, Dec. 9, 2013, at B1.

Pandora, so can the need to engage in ethical and trust-promoting information processing spur the kind of innovation needed to take advantage of the undeniable benefits of our new information technologies while minimizing their equally undeniable social costs.

CONCLUSION

In this essay, I have tried to show that privacy – the ways individuals participate in data about them – isn't dead. In fact, privacy is one of the most important issues facing modern information societies. How we shape the technologies and data flows will have far-reaching effects for the social structures of the digital societies of the future. Even the decision to do nothing about these new technologies is a decision, whether it is made as a matter of policy, a misguided understanding of constitutional rights, or technology-induced paralysis. If the law, social norms, or the market do not regulate privacy, engineers writing code in Silicon Valley or elsewhere will.⁹⁶ Our technological trajectory is not natural or inevitable; either way, it will be the product of many individual human choices about how those technologies are built.

But how we understand the problem; how we frame privacy matters.⁹⁷ Framing privacy as a regressive attempt to hide embarrassing secrets or as a kind of censorship is very different from other frames like to what extent ordinary people will be able to participate in the ways their data is used. Unfortunately, much of the public and legal debate about privacy has been clouded by misleading (and sometimes self-serving) myths about what privacy is and why it matters. Clearing away these myths reveals the scope of the challenge that faces us – crafting rules for the collection and

⁹⁶ *But cf.* Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic 1999).

⁹⁷ Woodrow Hartzog, *The Fight to Frame Privacy*, *Michigan Law Review* 111 (2013): 1021.

2014]

Four Privacy Myths

37

flow of personal information that balances the values of privacy, autonomy, security, and profitability, among others. But in a democratic information society, the rules basic rules for information flows should be made through public deliberation, rather than technocratic isolation. Clearing away the myths about privacy is an important first step.