Center for Technology Innovation at BROOKINGS

MAY 2015

The privacy paradox: The privacy benefits of privacy threats

Benjamin Wittes and Jodie C. Liu

Benjamin Wittes is a senior fellow in Governance Studies at Brookings. He co-founded and is the editor-in-chief of the Lawfare blog, which is devoted to sober and serious discussion of "Hard National Security Choices," and is a member of the Hoover Institution's Task Force on National Security and Law.

Jodie C. Liu is a member of Harvard Law School, Class of 2015, and a 2012 graduate of Columbia College. She formerly researched national security issues at the Brookings Institution as a Ford Foundation Law School Fellow.

INTRODUCTION

The 1971 Woody Allen film *Bananas* contains a scene of cringing comedic embarrassment: Allen is at a newspaper store, trying to buy pornography, and doing so in person makes him acutely conscious of being watched and judged. He flips through some magazines, hoping to disguise his purchase amid others. He then stops and nervously scans the store. An older, stern-countenanced woman stands close by. Turning back to the magazines, he narrates aloud as he gathers his selections.

"I'll get a copy of *Time* magazine." He pauses, shoots a quick glance at the older woman. "I'll take the *Commentary* and *Saturday Review*. And uh, let's see, *Newsweek*…"

In between the respectable magazines, he sandwiches his porn selections.

Satisfied that he has buried the disreputable within the higher-minded, he walks up to the counter. He'll take them all, he says, anxious to pay for his selections and leave.

But Allen's plan falls apart when the cashier rings up his purchases and hollers loudly to a colleague: "Hey Ralph! How much is a copy of *Orgasm*?" His mortification grows when Ralph doesn't catch the title the first time, prompting the cashier to shout the question even louder.

"*Orgasm*! This man wants to buy a copy! How much is it?"[1]

This scene may lack the same comic pointedness for younger readers—for whom adolescence did not involve the minor humiliations associated with purchasing pornography in person—as it will for folks, particularly men, above a certain age. But nearly every male, and more than a few women, who went through puberty in the pre-Internet age will smile in memory of some variation of

1 Bananas (Jack Rollins & Charles H. Joffe Productions 1971).

Allen's humiliation. If you didn't go to the magazine store yourself to purchase girly magazines, you asked an older brother, cousin, or friend. Or maybe you went to a friend's house or borrowed something from some kid at school. Pornography then, like alcohol today, was something teenagers wanted to get their hands on but could only obtain by facing another person and effectively confessing vice.

While you could consume it in private, you couldn't *obtain* it in private.

The *Bananas* portrayal of the embarrassing need to face an actual person to obtain porn seems quaintly anachronistic now, because the pornography consumer no longer has to face the judgmental old lady while nervously cramming *Orgasm* between *Time* and *Newsweek* at a corner store. Today, adolescents and adults alike simply click open their favored porn website. They can tab it somewhere between Gmail, Facebook, and SparkNotes on their browsers for easy switching purposes. Or if they fear detection, Google Chrome conveniently provides a helpful "Incognito Mode" that does not store browsing history. Much to their parents' dismay, teenagers have access to all of this material without ever setting foot outside their bedrooms.

They have something one might call privacy.

And so do we all. We have it not just—or even principally—with respect to erotic material, but with respect to all sorts of other content as well: medical information, politically sensitive publications and purchases, and secret communications. And we have it because of a series of technologies that are the subject of endless anxiety among commentators, scholars, journalists, and activists concerned about—ironically enough—protecting privacy in the digital age.

Something is not right here.

> ...the American and international debates over privacy keep score very badly and in a fashion gravely biased towards overstating the negative privacy impacts of new technologies relative to their privacy benefits

In this paper, we want to advance a simple thesis that will be far more controversial than it should be: the American and international debates over privacy keep score very badly and in a fashion gravely biased towards overstating the negative privacy impacts of new technologies relative to their privacy benefits.

Many new technologies whose privacy impacts we fear as a society actually bring great privacy boons to users, as well as significant costs. Society tends to pocket these benefits without much thought, while carefully tallying and wringing its hands about the costs. The result is a ledger in which we worry obsessively about the possibility that users' internet searches can be tracked, without considering the privacy benefits that accrue to users because of the underlying ability in the first instance to acquire sensitive material without facing another human, without asking permission, and without being judged by the people around us.

While our public debate largely ignores these benefits, as we shall show, our behavior as consumers is often exquisitely attuned to the reality that the march of technological development is not—contrary to the assumption that so dominates the privacy literature—simply robbing us of our privacy in exchange for convenience. Rather,

technologies often offer privacy with one hand while creating privacy risks with the other, and consumers choose whether or not to use these technologies based, in part, on whether they value more the privacy given or the privacy taken away. Countless teenagers—and adults, for that matter—now acquire their medical information, as well as their pornography, online because they would rather be tracked online by commercial vendors than have to face parents, teachers, doctors, or the stern-faced old lady at a news stand. From Google searches to online shopping to Kindle readers, the privacy equation is seldom as simple as a trade of convenience for privacy. It is far more often a tradeoff among different types of privacy.

How we balance the relative value of different forms of privacy is, we will argue, a function of how much we fear the potential audiences from whom we want to keep certain information secret. Privacy is a value that we often discuss in the abstract but generally does not exist in the abstract. The person who deeply resents being tracked online for commercial purposes might quite reasonably weigh the privacy risks of seeking medical information on the web differently from, say, the pregnant teenager whose primary privacy concern is shielding her situation from her parents. This latter person may see the possibility of Google's or Microsoft's tracking her search as the most minor of concerns next to the ability search engines are providing her to find an abortion provider on her own. As we will show, the privacy that consumers value in practice is not always the privacy that activists devoted to privacy value on their behalf.

How we balance the relative value of different forms of privacy is, we will argue, a function of how much we fear the potential audiences from whom we want to keep certain information secret.

We proceed in several steps. We first briefly survey the literature on the privacy implications of technology to demonstrate the dominance of the theme that privacy is eroding. We then then set forth the argument that the reality is more complicated than that, and that technologies may enhance privacy in some areas while eroding it in others. We then seek to illustrate this argument by highlighting certain commonplace technologies generally believed to be privacy threats but that actually provide key privacy benefits as well. We conclude with a call for better means of keeping score in the privacy debates and for making policy on the basis of a more holistic understanding of privacy impacts.

THE TRADITIONAL VIEW: PRIVACY IS ERODING

That personal privacy is eroding as a consequence of technological development is a premise so deep, so widely shared, and so earnestly felt that scholars seldom examine it carefully. They debate how dire privacy's condition really is.[2] They even debate whether we should venerate the value itself quite as much as we do or whether privacy is overrated.[3] But in the vast literature on privacy and technology, very few commentators acknowledge the potential privacy *gains* associated with the technologies we fear. Rather, the overwhelming consensus among privacy

2 Judge Richard Posner, for instance, suggests that people are not as concerned about privacy as they often profess. People are willing to "surrender [their informational privacy] at the drop of a hat," so long as the "details of their health, love life, finances" will not be "used to harm them in their interactions with other people," and so long as they "derive benefits from the revelation," such as a sense of security. Richard Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 251 (2008).

3 *See, e.g.*, Amitai Etzioni, The Limits of Privacy (2000). Etzioni takes a generally skeptical view about the value of privacy. For instance, he wonders whether "significant harms" may result from upholding privacy too strictly: "Privacy is treated in our society (more than any other) as a highly privileged value. The questions this book grapples with are: Under which moral, legal, and social conditions should this right be curbed? What are the specific and significant harms that befall us when we do not allow privacy to be compromised?" *Id.* at 3.

scholars is that technology and big dat a inherently chip away at privacy, which will erode unless we do something dramatic to stop that erosion.

The origins of this view run deep—as deep as the origins of privacy law itself. Samuel Warren and Louis Brandeis's seminal 1890 article *The Right to Privacy*—which gave birth to privacy law[4] and has been called the "most influential law review article of all"[5]—began by pointing to "[r]ecent inventions and business methods" as threat to which society needed a right to privacy as a response.[6] For Warren and Brandeis, the major offenders were "[i]nstantaneous photographs and newspaper enterprise," and these developments had "invaded the sacred precincts of private and domestic life."[7]

In modern scholarship, the notion that technology's march comes with privacy costs permeates the literature. The solutions vary, but the diagnosis is almost always the same.

In modern scholarship, the notion that technology's march comes with privacy costs permeates the literature. The solutions vary, but the diagnosis is almost always the same. David Brin's book *The Transparent Society*, for example, urges radical transparency as an antidote to the loss of privacy. And in that sense, Brin's book runs counter to much of the privacy literature, which focuses on preventing privacy harms. But if Brin's solution differs, his diagnosis of the basic problem is orthodox: privacy is slipping away. "[I]t is already far too late to prevent the invasion of cameras and databases" he writes. "The *djinn* cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay. Light *is* going to shine into nearly every corner of our lives."[8]

Daniel Solove, author of any number of books on privacy, is less fatalistic than Brin about the inevitability of privacy's loss and the futility of policy intervention to prevent it. Yet he agrees with Brin's premise that the privacy harms technology has unleashed cannot be wholly prevented: "Those that say the genie can't be stuffed back into the bottle are correct," he writes.[9] For Solove, loss of privacy tracks with loss of power. "Digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. . . . The information gathered about us has become quite extensive, and it is being used in ways that profoundly affect our lives. Yet . . . we lack the power to do much about it."[10] This "powerlessness" over our own privacy can be traced chiefly to a consequence of digital technology: "the collection of data" and "our complete lack of control over the ways [such data] is used or may be used in the future."[11]

4 *See* Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 Tenn. L. Rev. 623 (2002) ("[Warren and Brandeis's article] has been widely recognized by scholars and judges, past and present, as *the* se minal force in the development of a 'right to privacy' in American law.").

5 Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 Law & Contemp. Probs. 327, 327 (1966).

6 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890).

7 *Id.*

8 David Brin, The Transparent Society: Will Technology Force us to Choose Between Privacy and Freedom? 8–9 (1999).

9 Daniel J. Solove, The Digital Person 227 (2004).

10 Daniel J. Solove, The Digital Person 1–2 (2004).

11 *Id.* at 51.

Unlike Brin, Solove does not think that protecting privacy is a lost cause. He urges, rather, that "[l]aw must intervene to protect privacy."[12] But he operates on the premise that absent some tourniquet to stem the slow leakage of our privacy, technology will gradually erode it until little is left. Only significant policy intervention and committed efforts to reshape the legal conceptions of privacy can shield what remains.[13]

The fundamental premise that technology will, unchecked, erode privacy animates even those who look to technology itself for the solution—such as the scholars of the "privacy enhancing technologies" (PET) literature. Animating this scholarship is the idea that privacy can be engineered but that one has to decide to engineer it. Much like Solove, PET scholars tend to think that there is hope for privacy if we profoundly reform the way we develop and use technology, although instead of looking to law, these scholars look to the widespread embrace of technologies designed to stem the larger erosion. Bert-Jaap Koops and Ronald Leenes typify the PET perspective on the technology-privacy relationship:

> Technology usually makes privacy violations easier. Particularly information technology is much more a technology of control than it is a technology of freedom. Privacy-enhancing technologies (PETs) have yet to be implemented on any serious scale. The consequent eroding effect of technology on privacy is a slow, hardly perceptible process. If one is to stop this almost natural process, a concerted effort is called for, possibly in the form of "privacy impact assessments," enhanced control mechanisms, and awareness-raising.[14]

In other words, one can build privacy protections into systems design and thereby retard or prevent the erosion, but if one doesn't engineer privacy into new technologies, the erosion—which is the default effect of new technologies—will proceed. "In the absence of a proactive implementation of PETs,"[15] writes one scholar, we could find ourselves hurtling towards a "Cyber-Panopticon, where one's every move can be monitored in real-time, stored in electronic form, and later analyzed with granular particularity."[16] And just as with Bentham's conception of the Panopticon, the government can exploit the Cyber-Panopticon as a tool for "effective social control."[17] PET scholars seek a different means of stemming the tide, but they accept the larger literature's premise.

There are many variants of this theme. Orin Kerr, for example, has argued that advanced technologies may be necessary to limit the privacy intrusions of less advanced surveillance measures.[18] He has suggested that electronic technologies like "the Internet [reverses] the common associations about the relationship between technology and privacy." Specifically, he posits that the privacy impact of technology may depend on whether the environment under examination is the physical world, where advanced technologies "provide a powerful way to invade privacy,"[19] or the cyber world, where the "default will be the most invasive search possible, and . . . advanced technology is needed to

12 *Id.* at 224.

13 *See id.* at 224–28.

14 Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 Mich. Telecomm. Tech. L. Rev. 115 (2005). *See also* Michael A. Froomkin, *PETs Must Be on a Leash: How U.S. Law (and Industry Pracitce) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 Ohio St. L.J. 965 (2013).

15 Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. Sci. & Tech. L. 288, 316 (2001).

16 *Id.* at 293. *See also* Daniel J. Solove, The Digital Person 30–31 (2004) (analogizing the collection of information online to the Panopticon).

17 *Id.* at 291 (quotations omitted).

18 *See* Orin Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 650 (2003).

19 *Id.* at 650. Kerr provides a simple illustration of this point: "A single police officer can search a single room in a house, but cannot search an entire neighborhood, or a large city. To search an entire city, advanced technology would be required." *Id.*

minimize the invasion of privacy."[20] But the underlying point is nearly always a default assumption that as technology develops, the capacity to surveil develops with it, as do concentrations of data—and that such capacities and data concentrations are inimical to privacy values.

The themes that academics have whispered in the pages of law reviews, civil liberties and privacy groups have, as Brandeis might say, shouted from the rooftops. For these groups, the damage to privacy is more marked and immediate than a gradual erosion. And the response has been a sustained campaign of political and rhetorical advocacy. Technology gives rise to "*intrusions* [that] have devastating implications for our right to privacy,"[21] says the American Civil Liberties Union. It "enabl[es] unparalleled *invasions* of privacy," says the Electronic Freedom Foundation.[22] According to the ACLU, the privacy-technology playing field is something of a zero-sum game: if we do not overhaul the laws governing technology and privacy, we will have to "choose between using new technologies and keeping [our] personal information private."[23]

Privacy-minded groups like the ACLU focus in the policy space on the negative privacy consequences of technology. And policymakers have themselves internalized the basic premise. Consider the White House's landmark May 2014 report on Big Data, commonly referred to as the Podesta Report (named for presidential counselor John Podesta, who was charged with producing it). For obvious political reasons, the Podesta Report steers clear of couching the technology-privacy relationship in fatalistic terms, and it makes sure to nod to the Obama administration's prioritization of the development of privacy enhancing technologies.[24] New technologies are "fundamentally changing the relationship between a person and the data about him or her."[25] Big data technologies may not be *invading* privacy interests or *intruding* on our lives, but they are "transformative" in a way that "raises considerable questions about how our framework for privacy protection applies in a big data ecosystem."[26] For all its caution, the Podesta Report too accepts that "[t]he technological trajectory is . . . clear: more and more data will be generated about individuals and will persist under the control of others."[27]

There is, of course, no small measure of truth in this premise, and we do not mean to argue either that these themes are incorrect or that technology, in fact, augments privacy in the aggregate. Create new channels of communication, and you also create new channels of surveillance. Create new abilities for people to do things in fashions that inherently generate data—storing things in the cloud, or buying things electronically, for example—and you create opportunities that did not previously exist to harvest and analyze those data. Conduct your life online, and your life is trackable. All of that is true.

Conduct your life online, and your life is trackable.

And yet, it is not quite the whole privacy story either, and the larger literature lacks an adequate accounting of the other side of the ledger: the privacy benefits of technologies that give privacy, as well as take it.

20 *Id.* at 651 (emphasis in original). Kerr suggests, "In contrast to the physical world, total surveillance of traffic through a point on the Internet is simple, but narrow and limited surveillance requires advanced filtering." *Id.*

21 *Internet Privacy*, American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/internet-privacy (last visited Feb. 3, 2015).

22 *Privacy*, Electronic Freedom Frontier, https://www.eff.org/issues/privacy (last visited Feb. 3, 2015).

23 *Internet Privacy*, American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/internet-privacy (last visited Feb. 3, 2015).

24 *Id.* at 55.

25 *Id.* at 9.

26 *Id.* (introductory letter).

27 *Id.* at 9.

Look deep enough, and there are countervailing argumentative currents buried in the literature. Professor Ric Simmons, for example, has argued that "one of the primary effects of technology on society over the past two hundred years has been to *increase* the amount of privacy in our everyday lives."[28] We often overlook these privacy boons because we "quickly adapt . . . and fail to notice how fundamentally our lives are changing."[29] In fact, however, we are able to perform more activities privately—especially activities that involve communicating and handling information—thanks to technology.[30]

One such technology Simmons believes has increased privacy is, oddly enough, a technology long at the heart of privacy concerns: the telephone.[31] Picture yourself living in the 1950s, Simmons suggests. Compared to the other existing communication implements at your disposal—mail or in-person conversation—the telephone greatly "increased [your] chances of having a private conversation."[32] Like mail and in-person conversation, the telephone was not a "foolproof" method of communication.[33] But the telephone clearly offered a mode of privacy that was not previously available: It therefore provided "more options to choose from in deciding which method of communicating is the most secure."[34]

Simmons has it right in at least one critical respect: Technology tends to present a double-edged sword privacy-wise. Even technologies designed to protect privacy have a different side to them, and very few technologies will be either purely and inherently privacy enhancing or purely and inherently privacy eroding.

Think for a moment about the door—one of the most basic privacy-enhancing technologies, though perhaps not the type of technology that most readily comes to mind in modern privacy discussion. A world with doors is significantly more protective of privacy than a world without doors. But the privacy that doors offer is not absolute—and the presence of doors will tend to make surveillance more surreptitious. Watching someone in a world without doors is tricky to do without detection. Close a door, however, and someone can watch you through the keyhole, slip something unpleasant between the door and the threshold, or listen furtively behind the door. Behind closed doors, moreover, you feel comfortable doing certain things you would never imagine doing before you closed the door. In other words, the door gives you some degree of privacy that you did not have before, but it also masks attempts to undermine the privacy it offers.

And there's the catch: just as the door does not simply protect privacy, technologies we assume will *erode* privacy have complicated multi-directional effects too. By ignoring or diminishing these privacy effects, we mask the very complicated impacts of new technologies on individual privacy in the aggregate.

28 Ric Simmons, *Why 2007 is Not Like* 1984*: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. Crim. L. & Cri. 531, 531 (2007).

29 *Id.* at 536

30 *See id.* at 540 ("In short, one of the primary effects of technology on society over the past two hundred years has been to *increase* the amount of privacy in our everyday lives. Individuals—including criminals—can now conduct many more activities secretly, particularly activities which involve communicating, storing, or processing information.").

31 *Id.* at 536–40.

32 *Id.* at 537.

33 *Id.* at 537.

34 *Id.* at 539.

PRIVACY FROM WHOM?

In thinking about big data and digital technologies as a one-way, privacy-eroding street, we are grossly oversimplifying the true nature of the technology-privacy interface. Just as the door is not a pure privacy gain, few technologies involve pure privacy loss. The Internet, after all, is not simply a series of surveillance technologies. Surveillance capabilities, rather, are largely collateral consequences of the main point: the opening up of new communications channels. And those new channels involve, in the first instance, privacy gain—or, rather, a series of privacy gains—because they enable greater choice about how individuals communicate with one another. Create phone lines for the first time and you create the possibility of remote verbal communication, the ability to have a sensitive conversation with your mother or uncle or lawyer from a distance. It is only against the baseline of that privacy gain that you can measure the loss of privacy associated with the sudden possibility of wiretapping.

A huge amount of technological development follows this basic pattern. Google and Microsoft and Yahoo! enable you to search for information privately—with data collection by the companies and possible retrieval by other actors as a consequence. Amazon lets you buy all sorts of products with nobody the wiser—but with your purchase history stored and mined for patterns. Your smartphone lets you put all this capability in your pocket and take it with you—and thus also lets you use it more and record your location along the way. That information too is then subject to retrieval. Facebook allows you to identify discrete groups of people with whom you want to share material—yet it stores your actions for processing and retrieval as you go.

In our mental tabulation of gain and loss, we tend to count only one side of the ledger, pocketing what we have won as though it were of no privacy value while bemoaning what we have given up. Even more mischievously, when we do acknowledge the gains, we tend to redefine them as gains in something *other than privacy.*

In our mental tabulation of gain and loss, we tend to count only one side of the ledger, pocketing what we have won as though it were of no privacy value while bemoaning what we have given up. Even more mischievously, when we do acknowledge the gains, we tend to redefine them as gains in something *other than privacy*. We define them, most commonly, as mere convenience or efficiency gains[35]—a dismissive description that implies we have won something inconsequential or time-saving while giving up something profound. But the construction leaves us with a distorted and altogether-too-bleak outlook on technology's impact on our lives. Yes, technology involves gains in convenience and efficiency, but those are not the only gains.

To reiterate, we do not argue here that technology is necessarily privacy-enhancing in the aggregate, or that technology does not erode privacy. Rather, our general point is that the interaction between technology and privacy is less clear-cut than the debate commonly acknowledges, that we don't keep score well, and that the actual privacy scorecard is a murky one.

35 *See, e.g.*, Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B. U. J. Sci. & Tech. L. 288, 291 (2001) ("Through technology we can accomplish tasks with startling efficiency and perform others that were once thought impossible. Many technological changes, however, create unforeseen consequences that cut against values society seeks to protect. . . . The Internet has raised a number of such unforeseen problems, including what many view as serious privacy concerns.").

One of the reasons for its murkiness is that whether technology increases or diminishes a given person's privacy in any given circumstance depends in large part on the particular audience that person fears will discover his or her personal information. The same technology used in exactly the same way by two different people can erode one person's privacy while enhancing the other's, for the simple reason that those two people value different privacy goods and the technology may serve one good at the expense of the other.

People often throw around the term "privacy" as though everyone were trying to shield the same things about themselves and shield them from the same groups of people. But privacy is not an abstract value. We care about privacy as it relates to the people *from whom we want to keep certain pieces of information secret*. And that won't always be the same from person to person. For some people, the fear is government surveillance. For others, it's corporate behavior. For many others, it's the people they work with or go to school with or live with every day. For some people, it's just about everyone. Depending on what information a given individual wants to keep private—and from whom—a given technology may be privacy-enhancing or privacy eroding or both at the same time.

Does the Internet erode your privacy? It certainly tends to diminish individuals' privacy from the companies that provide them online services. To provide those services, after all, the companies necessarily gather and transmit data about what individuals want and when they want it, data the companies processing those requests may later use, say, to improve their Internet services. Moreover, those same companies also exploit these data for marketing purposes. By a similar token, the Internet also tends to diminish privacy from the government, which can in certain circumstances exploit those data for law enforcement and intelligence functions.

But for many people, these threats feel highly theoretical. While many people fear government surveillance, many others make the calculation that NSA has limited interest in them and that legal restrictions restrain whatever interest the agency might have. They think it unlikely they will become involved in a criminal probe. For people like these, and for people who are not overly concerned about mechanized processing of data for commercial purposes, the privacy threats from internet companies may seem quite diffuse.

At the same time, however, the internet enables dramatically *greater* privacy from the people around us.[36] It's not just the sexually active teen who no longer has to look her childhood doctor in the eye to learn about the symptoms of an embarrassing sexually transmitted disease, or ask her parents to make the doctor's appointment in the first place. It's not just the teenaged boy confused about his sexuality.[37] And it's not just the pornography consumer. It's everyone who has looked up a medical symptom. It's everyone who has participated in an anonymous discussion board of some kind and learned something useful from it. It's people who have amassed religious materials—or irreligious materials—in settings where those materials would not be welcome. By allowing individuals to avoid deeply personal and often embarrassing interpersonal situations while acquiring the information they need and transacting

36 Although we distinguish between two general types of privacy, and how technological development bears on that distinction, we do not suggest that the distinction serves as an overarching framework for understanding the scope of privacy. Helen Nissenbaum objects to similar bright-line approaches to defining the right to privacy, such as a private/public dichotomy framework that "restrict[s] [privacy's] sphere of legitimacy to the private." Helen Nissenbaum, Privacy in Context 125 (2010). Instead, Nissenbaum urges a more fine-tuned framework of "contextual integrity," under which privacy depends on any number of context-specific informational norms about "the respective roles of the subject, the sender . . . and the recipient of this information, and the principles under which the information is sent or transmitted from the sender to the recipient." *Id.* at 127.

37 At a symposium at Washington and Lee School of Law in January 2015, journalist Shane Harris described the privacy impact of Google's search functions on him as a teenager and during his twenties, the period in which he discovered he was gay. While the text of his remarks is not available, he later characterized it in an email to one of the present authors as follows: "I was in the process of coming out, and I wasn't ready to be honest with my family or even my closest friends about my feelings, and I had a huge number of unanswered questions about what it was like to be out as a gay person. It was a huge relief to be able to privately and anonymously connect with and talk to other gay men, and to read about the coming out process, without having to worry about being discovered."

the business they wish to transact, the internet can wildly enhance privacy in the situations in which—and involving the people from whom—privacy is most salient.

To summarize, then, let's identify four basic principles:

- First, most new technologies that implicate privacy, instead of inexorably eroding it, often both enhance and diminish it depending on how it is used, who is using it, and what sorts of privacy that person values.

- Second, individual concern with privacy often will not involve privacy in the abstract but rather privacy vis à vis specific audiences—which is to say that the question of privacy *from whom* matters.

- Third, at least some modern technologies that we commonly think of as privacy-eroding may, in fact, enhance privacy *from* the people in our immediate surroundings, while also eroding privacy *from* large physically remote entities (corporations and governments, most commonly, but also sometimes hackers).

- Fourth, many individuals may be willing to accept less privacy from these remote entities in exchange for greater privacy from more personally-connected, more local entities.

This fourth idea is—to some degree anyway—testable. When a new mode of technology causes forms of privacy to conflict with one another, individuals make in-the-moment decisions that provide some insight into their privacy preferences. To be sure, their continuing to use technologies on a regular basis about which privacy advocates harbor anxiety may not say anything definitive about the aggregate effect of technology on privacy. But it does suggest that there is a gap between the privacy many users want and the privacy that self-appointed watchdogs want for them.

Privacy gain and loss are quite difficult to measure. For one thing, we have no agreed-upon units of privacy. For another, privacy gains and losses almost always correlate with other gains and losses. When your password gets compromised, you lose both privacy and security. Are those two losses so hopelessly entangled that they are really the same thing? Or should one try to disaggregate them and describe both a security loss and separate privacy loss? Similarly, when one gains in privacy, one gains in other areas as well. Privacy gains particularly tend to correlate with gains in convenience—one of the reasons people tend to dismiss the privacy benefits of new technologies as merely gains in convenience. Indeed, as we have discussed, convenience is perhaps the go-to benefit that privacy scholars tend to cite when discussing the privacy implications of technology.[38] But it is far too simplistic to reduce all the benefits of new technologies to convenience, efficiency, and economic rationality. At least some of them have to do with an interplay between the different forms of privacy we describe above—that is, privacy from individuals in our immediate environment, as opposed to privacy from people and organizations farther removed from our daily routines.

Because of the inherent difficulty of measuring privacy, we do not attempt here to do it. Rather, we attempt only to show that there is another side of this ledger, that technologies presumed to erode privacy have significant privacy benefits, that these benefits matter to real people and influence their adoptions and uses of the technologies, and that consumers appear to weigh in certain instances the privacy benefits of these technologies more heavily than do privacy advocates. To do this, we look at a set of technologies that come into play frequently in our day-to-day

38 *See, e.g.*, Jonathon W. Penney, *Privacy and the New Virtualism*, 10 Yale J.L. & Tech. 194, 232 (2008) ("Often, we *want* some information about us to be offered to sites (i.e. bits of data in cookies) to make our online travels more convenient or easier to negotiate.").

lives and identify some of the ways in which they enhance our privacy, often without our conscious acknowledgment. Taken together, the following examples lend support to the intuitive theory that technology can enable individuals to gain privacy from people in their immediate surroundings, while at the same time potentially causing individuals to lose privacy from physically remote entities that come into possession of the same personal information.

CASE #1: GOOGLE AUTOCOMPLETE

One window into the privacy advantages of technologies people think of as corrosive of privacy is the "Autocomplete" algorithm embedded in Google's search function. These days, Googling ideas, products, and people is just about the first thing we do to find out about them. So aggregate search data is a great way of looking into what people are thinking about. This is, of course, why privacy advocates worry so much about the negative privacy impacts of the data generated by search engines. But there is a flip side to this problem: while the ability to store searched data may produce privacy harms, the ability to search large quantities of data in the first place on one's own computer systems offers huge privacy benefits. Looking at the proposed Autocompletes associated with certain search terms can illustrate the array of sensitive information which people are turning to the internet to procure privately, as well as the relative frequency with which they try to procure it.

If you use the Internet regularly, you are probably already familiar with Autocomplete: as individuals start typing their queries into the Google search box, Google automatically produces a list of "search predictions that might be similar to the search terms [they are] typing," so as to reduce the amount of time spent searching, correct misspelled search terms, or point toward related topics.[39] Naturally, the search predictions are not the result of a random generation instrument but are, rather, based in some way on the popularity of searches that contain the phrases the users are typing. While the precise algorithm is proprietary, Google does confirm that the Autocomplete search predictions are "automatically generated by an algorithm without any human involvement, based on a number of objective factors, including how often past users have searched for a term."[40] The constantly updating nature of the algorithm means that the Autocomplete suggestions may vary slightly depending on the time and place one executes the search. Admittedly, Autocomplete is an imperfect predictor of search frequency—articles and blog posts dedicated to exposing Autocomplete failures attest to that,[41] and Google acknowledges that the algorithm is, at least in part, "designed to reflect the diversity of . . . users' searches and content on the web."[42] But the basic ambition of the Autocomplete algorithm is to point individuals toward searches that other users have frequently entered and are thus likely to be the searches they are also trying to enter.

It turns out, however, that people confess all sorts of things to Google in the form of search queries—as the Autocomplete algorithm can attest.

It turns out, however, that people confess all sorts of things to Google in the form of search queries—as the Autocomplete algorithm can attest.

39 *Autocomplete*, Google, https://support.google.com/websearch/answer/106230?hl=en (last visited Jan. 27, 2015).

40 *Id*. In addition, there are geographic and time dimensions to determining popularity. *See How Google Instant's Autocomplete Suggestions Work*, Search Engine Land, http://searchengineland.com/how-google-instant-autocomplete-suggestions-work-62592 (last visited Jan. 27, 2015).

41 *See, e.g.*, *10 WTF Google Autocomplete Search Fails, Illustrated*, Mashable, http://mashable.com/2014/07/13/google-autocomplete-funny-illustrations/ (last visited Jan. 27, 2015).

42 *Autocomplete*, Google, https://support.google.com/websearch/answer/106230?hl=en (last visited Jan. 27, 2015).

A quick note on using "Autocomplete" data: The algorithm will not always produce the same results for different users. Because the system is proprietary, we could not be sure the best way to control for individual variability. We typed the entries below in the Google search bar on a computer at the Brookings Institution's offices in Washington, D.C. in August 2014 after having logged out all users from Google's services. We then repeated the queries from a different computer at Harvard Law School, also logged out of all Google services, in January 2015. We note variability of the results in the footnotes below.

Type in the word "symptoms" to Google and among the fairly common conditions and diseases that appear in the Autocomplete search predictions are "symptoms of strep throat," "symptoms of high blood pressure," "symptoms of diabetes," and "symptoms of anxiety." But there also appeared, at least in our case, a markedly less common disease: "symptoms of hiv."[43] Even though the incidence of HIV/AIDS in the United States population is rather low (roughly 0.3 percent of the population[44]) compared to the percentages of the United States population with high blood pressure (31 percent of all adults[45]) or diabetes (9.3 percent of the population[46]), a large enough number of individuals are ostensibly concerned that they or their partners might have HIV/AIDS that "symptoms of hiv" is comparable in popularity as a search to "symptoms of high blood pressure" or "symptoms of diabetes." Large numbers of people seem willing to trust Google with their lists of suspected maladies—apparently even, or disproportionately, when those maladies are sexually transmitted.

Entering into Google "I think I am" demonstrates that people are as candid with their search engines as they are with their diaries: "pregnant," "depressed," "bipolar," "gay," and "crazy" show up.[47] Similarly, entering "I'm scared that" or "I'm worried that" informed us that commonly Googled concerns include fears that "I'm gay," that "I might have HIV," that "I have herpes," or that "I'm pregnant."[48] And the search predictions for "I'm confused about" revealed to us that many turn to Google to deal with confusion about "my gender," "my religion," or "my sexuality."[49] People also tell Google that they are "unsure about" things like "abortion."[50]

Perhaps more revealing were the Autocomplete suggestions for "was I," which included "was I molested," "was I molested as a child," and "was I sexually assaulted."[51] Concerns about sexual abuse showed up in other, somewhat unexpected instances. When asking "how to know" something, some people are simply trying to figure out if they

43 Google, www.google.com (search "symptoms") (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned slightly different results when we repeated the search, likely a reflection of different seasonal sicknesses, but still included "symptoms of hiv." Google, www.google.com (search "symptoms") (last visited Feb. 3, 2015) (screenshot on file with authors).

44 *HIV in the United States: At a Glance*, Center for Disease Control and Prevention, http://www.cdc.gov/hiv/statistics/basics/ataglance.html (last visited Jan. 27, 2015).

45 *High Blood Pressure Facts*, Center for Disease Control and Prevention, http://www.cdc.gov/bloodpressure/facts.htm (last visited Jan. 27, 2015).

46 *Surveillance Reports*, Center for Disease Control and Prevention, http://www.cdc.gov/diabetes/pubs/statsreport14.htm (last visited Jan. 27, 2015).

47 Google, www.google.com (search "I think I am") (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned virtually the same results when we repeated the search. Google, www.google.com (search "I think I am") (last visited Feb. 3, 2015) (screenshot on file with authors).

48 Google, www.google.com (search "I'm scared that" and "I'm worried that") (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned virtually the same results when we repeated the search. Google, www.google.com (search "I'm scared that" and "I'm worried that") (last visited Feb. 3, 2015) (screenshot on file with authors).

49 Google, www.google.com (search "I'm confused about") (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned similar results when we repeated the search, but did not contain the result "I'm confused about my sexuality." Google, www.google.com (search "I'm confused about") (last visited Feb. 3, 2015) (screenshot on file with authors).

50 Google, www.google.com (search "unsure about") (last visited Aug. 6, 2014) (screenshot on file with authors). The same result about abortion did not appear when we repeated the search, but one new suggestion was "unsure about having a baby." Google, www.google.com (search "unsure about") (last visited Feb. 3, 2015) (screenshot on file with authors).

51 Google, www.google.com (search "was I") (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned very similar results when we repeated the search. Google, www.google.com (search "was I") (last visited Feb. 3, 2015) (screenshot on file with authors).

were “blocked on Instagram” or “hacked,” but many also want to know if they were “roofied,” “drugged,” “abused as a child,” or “sexually abused.”[52]

Teenagers have a special set of concerns vis à vis their parents, largely revolving around sexuality, pregnancy, and depression. They look to Google for advice about how to tell their parents that they are pregnant, bisexual, or gay; that they cut themselves; or that they are depressed.[53] They seek outlets to vent about how their parents do not understand their depression, obsessive compulsive disorder, or ADHD.[54] They wonder what they should do about their parents not knowing that they smoke, or that they have a boyfriend or girlfriend.[55] They complain about their parents’ being racist, poor, or stupid; they want to talk about their parents’ divorces.[56]

Purchasing products related to sexual health is another frequently Googled topic. When someone wants to gripe to Google about how he “hate[s] buying” something, there’s a good chance that he “hate[s] buying condoms”; if the person is female, there is a possibility that she “hate[s] buying pads.”[57] Autocomplete also tells us the less-than-shocking reason why many men—and some women—hate buying condoms: they are “embarrassed” about it.[58] Other items people divulge to Google that they are “embarrassed to ask” for are Viagra, Plan B, and birth control.[59]

The substance of these Autocomplete search predictions will come as no surprise. That teenagers are worried about telling their parents about a pregnancy, that we in general experience anxieties about religion and sexuality, or that buying condoms is a perpetually awkward affair for teens is almost too obvious for proof.

Less immediately apparent, however, is that in disclosing these types of personal details to Google, we reveal our preferences for certain types of privacy over others. Although John Doe runs the risk that someone at Google will come across the search revealing his confusion about his sexuality, he probably values keeping that information private from the unnamed Google analyst less than he values keeping it private from his family, friends, and colleagues. The ability to make this choice is no small privacy benefit for him—and it is emphatically not merely a

52 Google, www.google.com (search “how to know if I was”) (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned virtually the same results when we repeated the search. Google, www.google.com (search “how to know if I was”) (last visited Feb. 3, 2015) (screenshot on file with authors).

53 Google, www.google.com (search “how do I tell my parents”) (last visited Aug. 6, 2014) (screenshots on file with authors). Autocomplete returned virtually the same results when we repeated the search. Google, www.google.com (search “how do I tell my parents”) (last visited Jan. 25, 2015) (screenshot on file with authors).

54 Google, www.google.com (search “my parents don’t understand”) (last visited Aug. 6, 2014) (screenshots on file with authors). Autocomplete suggestions for this search often have to do with mental difficulties, with some minor variations. For instance, the first search produced suggestions about the searcher’s “mental illness,” while the second search yielded suggestions relating to the searcher’s “anxiety” and “stress.” Google, www.google.com (search “my parents don’t understand”) (last visited Jan. 25, 2015) (screenshot on file with authors).

55 Google, www.google.com (search “my parents don’t know”) (last visited Aug. 6, 2014) (screenshot on file with authors). With this search phrase, the Autocomplete suggestions of the first versus the second search were not as similar as with the previous search phrases, but they were still similar in tenor. For instance, the first search generated suggestions about smoking marijuana, while the second mentioned smoking only generally. The first produced Autocomplete suggestions about the searcher drinking alcohol where the second did not — but the second produced suggestions about the searcher having a tattoo where the first did not. Google, www.google.com (search “my parents don’t know”) (last visited Jan. 25, 2015) (screenshot on file with authors).

56 Google, www.google.com (search “my parents”) (last visited Aug. 6, 2014) (screenshot on file with authors). The autocomplete results were quite different when we repeated the search. The second search indicated that searchers thought their parents hated them, were dead, fought all the time, or were gay. Google, www.google.com (search “my parents”) (last visited Jan. 25, 2015) (screenshot on file with authors).

57 Google, www.google.com (search “hate buying”) (last visited Aug. 6, 2014) (screenshot on file with authors). Similar Autocomplete suggestions appeared when we repeated the search. Google, www.google.com (search “hate buying”) (last visited Feb. 3, 2015) (screenshot on file with authors).

58 Google, www.google.com (search “embarrassed to”) (last visited Aug. 6, 2014) (screenshot on file with authors). The suggestion about condoms did not appear when we repeated the search, but among the new Autocomplete suggestions were “embarrassed to be a virgin.” Google, www.google.com (search “embarrassed to”) (last visited Jan. 25, 2015) (screenshot on file with authors).

59 Google, www.google.com (search “embarrassed to ask”) (last visited Aug. 6, 2014) (screenshot on file with authors). Similar suggestions appeared when we repeated the search. Google, www.google.com (search “embarrassed to ask”) (last visited Jan. 25, 2015) (screenshot on file with authors).

convenience. In the absence of the ability to access such sensitive types of information privately, he likely would have to turn to someone in his community for advice about his sexuality, potentially exposing himself to bigotry and disdain; worse yet, he might refrain from seeking out this information altogether and simply remain in the dark about his own sexuality.

And remain in the dark many do. Although the percentage of men who are gay is estimated to be fairly consistent across states, the percentage of men who are openly gay is dramatically lower in states in which homosexuality is more deeply frowned upon than in states that are generally supportive of same-sex rights, and by a much larger factor than can be explained by mere movement of gay men from less tolerant to more tolerant states.[60] Many closeted men end up marrying women, and this gives rise to another Autocomplete example.

For many of these women, perhaps unsure where in their community they can turn for advice, confide in Google their own concerns about their husbands' homosexuality. As research by economist Seth Stephens-Davidowitz has shown, the search "is my husband gay" is nationwide more common than the search "is my husband cheating," and it is more common in the least gay-tolerant states:

> Searches questioning a husband's sexuality are far more common in the least tolerant states. The states with the highest percentage of women asking [the question "is my husband gay" in Google] are South Carolina and Louisiana. In fact, in 21 of the 25 states where this question is most frequently asked, support for gay marriage is lower than the national average.61

Indeed, a geographical mapping of searches questioning a husband's sexuality reflects a remarkably consistent pattern (see Figure 1). Those states with the highest number of closeted gay men are by and large the same states that exhibit the highest search volume for queries such as "husband gay."[62]

60 Seth Stephens-Davidowitz, *How Many American Men Are Gay?*, *New York Times* (Dec. 7, 2013), *available at* http://www.nytimes.com/2013/12/08/opinion/sunday/how-many-american-men-are-gay.html?_r=0. Stephens-Davidowitz's empirical research suggests that the percentage of men who are gay is similar across all states, but that the percentage of men who are *openly* gay exhibits a very large degree of contrast across states and correlates strongly with a state's general attitudes about homosexuality. *Id.* The "closeted gap" between less tolerant and more tolerant states is particularly acute among the teenaged population. *Id.*

61 *Id.*

62 *Id.*

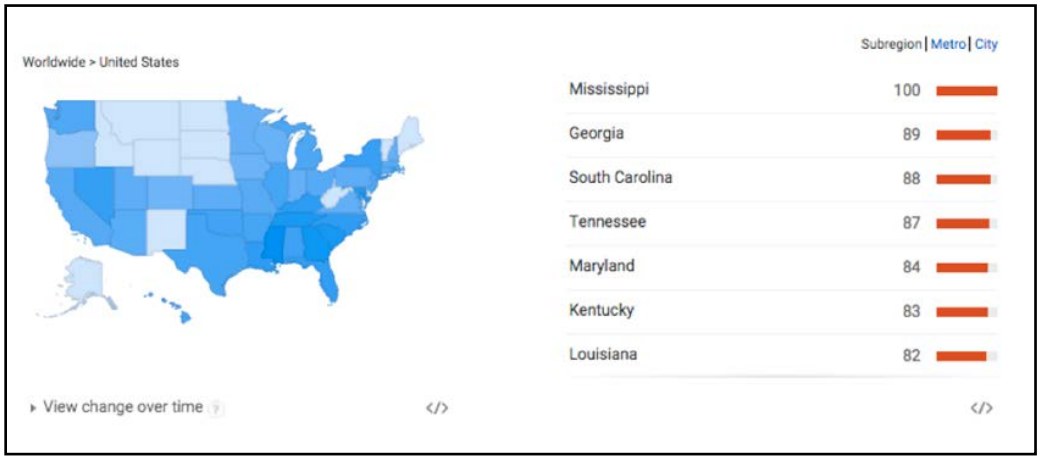

Figure 1. Search volume for the query "husband gay" is most darkly shaded, and thus highest, in states in the deep South, where the number of closeted gay men is likely to be greatest.[63]

CASE #2: ONLINE SHOPPING, SELF-CHECKOUT MACHINES, AND E-BOOK READERS

Online shopping involves similar dynamics to online search. You can't use cash. Your purchases are trackable. And in these senses, your privacy is eroded. On the other hand, you don't have to face anyone to make your purchase. So when you shop, you pick your privacy pain, and you also pick your privacy gain. Again, consumers seem to put somewhat different weights on the relative costs and benefits of online shopping than do activists.

Luckily for the many people who have told Google they hate buying condoms or are embarrassed about it, condoms are available not just through online mega-retailers like Amazon, but also through online companies dedicated solely to selling condoms and nothing else. With names like Undercover Condoms, Condom Jungle, Condom Depot, Discount Condom King, Rubber Club, Condom Corner, All Condoms, Official Condoms, Condom USA, Condom Bazaar, Condom Man, Condom Country, and Rip N Roll, these stores share in common their prominently displayed promises to deliver condoms in discreet packaging and to show up on credit card statements under a generic company name (read: not "Condom Mania").

To be sure, some of the demand for online condom sales likely is driven by the price discount that comes with buying items in bulk. But while bulk-purchase discounts may explain the appeal of online shopping in general, they do not, in themselves, account for the vast number of stores specifically devoted to selling one specific item that is available for (much quicker) purchase at every corner store. For that, a spokesperson for Rubber Club, a subscription service that sends condoms in monthly installments, explains that a primary impetus for online condom stores like Rubber Club is a desire to "enable individuals to practice safe sex more privately" and the ability to tap into their reluctance to purchase condoms in person.[64]

Another strategy for those who want to avoid the Woody Allen embarrassment of the face-to-face encounter with the store clerk is to use self-checkout machines. We were unable to obtain commercial data from retailers bearing

63 Google Trends, www.google.com/trends (search "husband gay") (last visited April 27, 2015).

64 Interview (August 5, 2014), on file with authors.

on this question, but consider the following as a thought experiment: When CVS installed self-checkout machines in the company's many stores, do you imagine that condom sales remained flat, decreased, or increased? What about teen condom sales, in particular? If you imagine a significant increase, as we do, you've just intuited that these machines are offering large numbers of people privacy relief.

Countless articles,[65] blog posts,[66] Yahoo! Answer questions,[67] WikiHow instructions,[68] and internet memes[69] illustrate individuals' relief at being able to purchase condoms using self-checkout, and their despair when self-checkout is not an option. Indeed, to describe this effect with one of the earlier examples we discussed, Google's Autocomplete algorithm provides "condoms" as one of the searches suggested if you enter "self checkout," suggesting that condom buying is one significant use to which people put self-checkout machines.[70]

The embarrassment associated with checking out before an actual human extends to situations less obvious than condom purchases. Consider, for instance, checking out library books. As library researchers Stephanie Mathson and Jeffrey Hancks explain, the process of presenting one's book selections to a human being at the circulation desk may inflict such uneasiness on library patrons that it dissuades some from checking out certain books at all:

> One of the least private aspects of library information retrieval remains the process by which materials are [checked] out of the library. Generally speaking, patrons must take items to a centralized location in full view of other people and check out those materials under the supervision of a library staff member. The public nature of this transaction makes the check-out moment a confessional and self-revealing one. It is our thesis that this compulsory self-disclosure inhibits access to information.71

Here, too, self-checkout machines can save the day by eliminating the need for librarian-patron interaction. While self-checkout machines are not yet present in most public libraries, two are available at the Charles V. Park Library at Central Michigan University, where Mathson and Hancks have "examine[d] [their] impact . . . on the circulation of potentially embarrassing or controversial materials."[72]

At Charles V. Park Library, students typically staff the circulation desks, compounding the awkwardness a fellow student faces when checking out materials of a personal or sensitive nature. During 2006 and 2007, Mathson and Hancks anonymously monitored the circulation histories of select LGBT materials histories using the self-checkout machines versus the student-manned circulation desk, and then compared them with the analogous circulation histories of select control materials, carefully choosing the two samples so as to avoid other possible explanations

---

65 *See, e.g.*, *Buying Condoms*, Cracked, http://www.cracked.com/funny-5955-buying-condoms/ (last visited Jan. 27, 2015); *10 Things That Are Way More Awkward to Buy Than Condoms*, The Frisky, http://www.thefrisky.com/2009-06-12/10-things-that-are-way-more-awkward-to-buy-than-condoms/ (last visited Jan. 27, 2015).

66 *See, e.g.*, Self Checkout Stations, Tumblr, http://hatethefuture.tumblr.com/post/246228693/self-checkout-stations-pros-no-embarrassment.

67 *See, e.g.*, https://answers.yahoo.com/question/index?qid=20140111224752AAUSmAD.

68 *See, e.g.*, *Buy Condoms Discreetly*, WikiHow, http://www.wikihow.com/Buy-Condoms-Discreetly; *Buy Condoms*, WikiHow, http://www.wikihow.com/Buy-Condoms.

69 *See, e.g.*, http://thechive.files.wordpress.com/2013/02/goodwill-captions-0.jpg?w=275; http://joyreactor.com/post/629028; http://www.quickmeme.com/meme/3s118h.

70 Google, www.google.com (search "self checkout") (last visited Aug. 6, 2014) (screenshot on file with authors). Autocomplete returned similar results when we repeated the search. Google, www.google.com (search "self checkout") (last visited Feb. 3, 2015) (screenshot on file with authors).

71 Stephanie Mathson & Jeffrey Hancks, *Privacy Please? A Comparison Between Self-Checkout and Book Checkout Desk Circulation for LGBT and Other Books*, 4 J. Access Services 27, 28 (2007).

72 *Id.* at 27.

for a book disparity (for example, distance from shelf location to self-checkout machine).[73] Of the twenty-one books in the control group that students checked out during the experiment period, two (9.52 percent) went through the self-checkout machines. In contrast, students checked out eight of the twenty-seven (29.63 percent) checked-out books in the LGBT sample using the self-checkout machines.[74]

The study sample is admittedly small, but the results are consistent with the notion that individuals use self-checkout machines to make selections privately, away from prying drugstore cashiers or library staff. They also tend to confirm Mathson and Hanck's hypothesis that, in libraries without self-checkout machines, at least some individuals decide against checking out certain books that might cause them embarrassment at the circulation desk.

One type of book that is almost by definition checked out electronically is the e-book. And once again, we see both the effect of privacy concerns and privacy benefits operating concurrently in e-book purchases. Many commentators have raised privacy concerns about e-readers.[75] The Kindle, after all, lets Amazon know not merely what books we have read but what *pages* we have read.

That said, the technology also may enable more private consumption and acquisition of books. Some days, we want to relieve our brains from any serious thinking and simply unwind with a clichéd piece of murder-mystery, chick lit, psychological thriller, or sci-fi fantasy. But we don't necessarily want to be seen carrying these books around, and not everyone wants to be seen buying them either.

Consider the case of that best-selling phenomenon, *Fifty Shades of Grey*. As of February 2014, the *Fifty Shades of Grey* trilogy had sold more than 100 million copies worldwide.[76] In 2012, the first book in the BDSM-glorifying series had, in Britain anyway, outsold the best-selling book in the *Harry Potter* series, *Harry Potter and the Deathly Hallows*, to become the best-selling book of all time in Britain.[77] Yet consider how often you've seen someone reading *Fifty Shades of Grey* on the morning ride to work, or caught a glimpse of the book sitting in a colleague's bag, as compared to the number of times you've seen adults with *Harry Potter and the Deathly Hallows*.

One reason we do not physically *see* people reading their paperback copies of *Fifty Shades of Grey* on the metro, in cafés, and in hospital waiting rooms, is that in much larger proportions than with other books, people are reading *Fifty Shades of Grey* on electronic book readers,[78] with which they can both buy and consume the book without anyone immediately around them knowing. Kindle sales of the book have outstripped print sales by far. According to one account, "at the height of its popularity back in April 2012, [the first book in the *Fifty Shades* series] was selling

73 *Id.* at 31–33.

74 *Id.* at 34.

75 *See, e.g.*, Alison Flood, *E-readers Reading Your Reading: A Serious Invasion of Privacy?*, The Guardian (Dec. 5, 2012), *available at* http://www.theguardian.com/books/booksblog/2012/dec/05/ereaders-reading-privacy; Alexandra Alter, *Your E-Book Is Reading You*, Wall St. J. (July 19, 2012), *available at* www.wsj.com/articles/SB10001424052702304870304577490950051438304; Martin Kaste, *Is Your E-Book Reading Up On You?*, NPR (Dec. 14, 2010), *available at* www.npr.org/2010/12/15/132058735/is-your-e-book-reading-up-on-you. The Electronic Freedom Frontier has even compiled charts showing the extent to which certain e-reader platforms have the capacity to store information regarding your e-reading activities. Electronic Frontier Foundation, *E-Reader Privacy Chart, 2012 Edition* (2012), *available at* https://www.eff.org/pages/reader-privacy-chart-2012.

76 Alison Flood, *Fifty Shades of Grey Trilogy has Sold 100m Copies Worldwide*, The Guardian (February 27, 2014), *available at* http://www.theguardian.com/books/2014/feb/27/fifty-shades-of-grey-book-100m-sales.

77 Anita Singh, *Fifty Shades of Grey is Best-Selling Book of All Time*, The Telegraph (Aug. 7, 2012), *available at* http://www.telegraph.co.uk/culture/books/booknews/9459779/50-Shades-of-Grey-is-best-selling-book-of-all-time.html.

78 *See* Mark Sweney, *Fifty Shades of Grey Publisher Random House Posts Record Profits*, The Guardian (March 26, 2013), *available at* http://www.theguardian.com/media/2013/mar/26/fifty-shades-random-house-record-profit ("About 50 percent of revenues from the [*Fifty Shades of Grey*] trilogy were from ebooks, compared to [the book's publishing house's] global average of about 20 percent from digital sales.")

six times more Kindle books than print books."[79] In fact, *Fifty Shades of Grey* and similar "lowbrow fiction" may be among the major driving forces behind the popularity of e-readers.[80]

CASE #3: PORNOGRAPHY

Then there's porn.

While many people don't feel comfortable talking about pornography, it provides a particularly stark illustration of how technology can change the privacy landscape for the better. To be sure, facilitating pornography consumption is far from the only privacy benefit of online technologies; if it were, it would probably be fair to see those benefits as negligible. Porn may not be the world's greatest vice, but its propagation is surely not a particular virtue either. What makes pornography interesting for purposes of this paper is that it is a large and studiable category of material that exemplifies a still-larger category: It is material we consume in great quantity about which we are embarrassed and which we thus prefer to consume in private.

The major medium for conveying pornography has changed dramatically since *Bananas*, when it involved mostly printed material and movies played in theaters. Unsurprisingly, pornography is a commodity people greatly prefer to consume on their own, and there is no question that individuals consume pornography more privately these days than a few decades ago—a fact no doubt related to the huge growth of the online porn industry that has taken place alongside the growth of the Internet. Which privacy-conscious porn viewer would prefer traveling to a crime-ridden red light district to watch films in a seedy theater with countless shadowy figures to viewing those films in the privacy of his or her own bedroom? Yes, there is privacy cost to this: You can't pay cash and your viewing habits are trackable. But clearly, consumer behavior suggests there is a major privacy gain as well.

PornHub, one of the largest online video-hosting platforms for pornography, has looked into some of these private pornography-viewing habits. At PornHub Insights,[81] a team of data analysts examines, on aggregate levels, how much pornography people view through PornHub's sites, of what types, at what times, and from which locations around the world. Most of the data the site presents are unsurprising and can be summed up pithily: people watch a lot of porn. But some of the statistics are more surprising and may shed light on online pornography as a privacy boon.

For instance, when it comes to gay porn, we might expect that more LGBTQ-friendly regions would surpass less LGBTQ-friendly regions in gay porn viewing. At the very least, we would expect that the areas with the highest percentage of the LGBTQ population would roughly track the areas with the highest percentage of gay porn viewing. Yet the gay porn viewing pattern that emerges across states reflects a trend remarkably similar to the one in Stephens-Davidowitz's research on Google searches by women questioning their husbands' sexuality. While a 2012 Gallup poll reveals that the states with the highest population of people identifying as LGBT were the District of Columbia (10.0 percent), Hawaii (5.1 percent), and Vermont (4.9 percent)—all of which have legalized same-sex

79 Sital S. Patel, *Read Lowbrow Fiction in Public: Novels Like Fifty Shades of Grey Spark Sales on E-Readers*, MarketWatch (July 25, 2014), *available at* http://blogs.marketwatch.com/themargin/2014/07/25/romance-novels-like-fifty-shades-of-grey-ignite-sales-on-e-readers/.

80 *See id.*

81 *Insights*, Pornhub, http://www.pornhub.com/insights/ (last visited Feb. 3, 2015).

marriage[82]—PornHub Insights finds a very different ranking of states with the highest percentage of "gay users."[83] The states with the highest percentage of gay users are Mississippi (5.58 percent), Louisiana (5.44 percent), and Georgia (5.38 percent), none of which have legalized same-sex marriage.[84] Gay pornography is so popular in the South, in fact, that "the percentage of gay viewers for every single state in the South is higher than the average" of the states in which same-sex marriage is legal."[85] Interestingly, however, the percentages of the population that "identify" as LGBT in the top three gay porn user states are not high. Mississippi has the third lowest percentage in the country (2.6 percent), while Louisiana is tied for the eighteenth lowest (3.2 percent) and Georgia sits in the middle of the pack (3.5 percent).[86]

One should not draw any categorical conclusions from these data; there are too many unknown variables that might be driving the unexpectedly high percentage of gay PornHub users in the less LGBTQ-friendly southern states. Moreover, the phenomenon in the southern states is not replicated in other less LGBTQ-friendly states, such as Montana and North Dakota, where the percentages of gay PornHub users are among the lowest in the country.[87] Other results of the gay pornography study are similarly unsurprising: on average, states that have legalized same-sex marriage watch more gay porn than states that have not.[88]

But the gay pornography trend in the South provides at least some support for the theory that perhaps closeted individuals living in Bible Belt states are more concerned for their privacy from people in their immediate communities—for which online pornography offers some protection—than they are about protecting their privacy from remote online entities, which online gay pornography tends to erode. They seem to mind less the fact that some data cruncher at PornHub Insights might identify their interest in gay pornography than they mind that someone in their community might see them at a gay bar or scouring the local bookstore for a gay-themed magazine.

Some individuals are so at ease with distant data analysts being privy to their porn-viewing habits, in fact, that they are willing actively to submit their porn preferences for digital analysis. Devised by the same people who run PornHub and launched in late 2013, PornIQ is a "deliciously addictive" new online service that curates porn videos to users' tastes much in the same way that Pandora curates music.[89] Upon registering, users have only to answer a short series of questions about their pornography inclinations and just like that, the site—as the *Telegraph* puts

82 The study is based on "responses to the question, 'Do you, personally, identify as lesbian, gay, bisexual, or transgender?' included in 206,186 Gallup Daily tracking interviews conducted between June 1 and Dec. 30, 2012. This is the largest single study of the distribution of the LGBT population in the U.S. on record, and the first time a study has had large enough sample sizes to provide estimates of the LGBT population by state." However, the study probably does not accurately capture the true percentage of the population that is LGBT, since many LGBT individuals still in the closet probably would not "identify" as LGBT. Gallup admits this is a limitation of the study: "A second limitation is that this approach measures broad self-identity, and does not measure sexual or other behavior, either past or present." *LGBT Percentage Highest in D.C., Lowest in North Dakot*a, Gallup, http://www.gallup.com/poll/160517/lgbt-percentage-highest-lowest-north-dakota.aspx (last visited Feb. 3, 2015).

83 As the website notes, "gay users" for the purposes of this data analysis was limited to PornHub users who looked for porn "in the Gay (male) section[,] as the lesbian category is very popular with straight men and women." *Gay USA Porn Equality*, PornHub, http://www.pornhub.com/insights/gay-usa-porn-equality/ (last visited Feb. 3, 2015). The percentage of gay users on PornHub is taken out of the total number of users on PornHub. *Id.*

84 *Id.*

85 *Id.*

86 *Id.*

87 *Id.* The figures of gay users in Montana and North Dakota are 2.65 percent and 2.79 percent respectively. These states have the two lowest percentages of the population that identifies as LGBT: Montana (2.6 percent) and North Dakota (1.7 percent). *LGBT Percentage Highest in D.C., Lowest in North Dakot*a, Gallup, http://www.gallup.com/poll/160517/lgbt-percentage-highest-lowest-north-dakota.aspx (last visited Feb. 3, 2015).

88 *Gay USA Porn Equality*, PornHub, http://www.pornhub.com/insights/gay-usa-porn-equality/ (last visited Feb. 3, 2015).

89 Mic Wright, *PornIQ is the Most Addictive Pornography Site Ever Built. This is Going to Ruin Relationships*, The Telegraph (October 23, 2013), available at http:blogs.telegraph.co.uk/technology/micwright/100011275/porniq-is-the-most-addictive-pornography-site-ever-built-this-is-going-to-ruin-relationships.

it—"delivers tailored filth to its feverish fans in four button presses or fewer."[90] It gets better: "Every time users click [on something], the owners of PornIQ are increasing the sophistication of their database and learning more and more about what turns [users] on."[91]

Finally, it is worth noting that in at least some countries where pornography is more frowned upon than it is in the United States—to say nothing of sodomy or same-sex marriage—individuals still find a way to view porn online in droves. Pornography viewing in China, say, does not implicate quite the same privacy tradeoff as gay pornography viewing in the southern United States. It may have more in common with a classic black market; the government tries to crack down, but the market pops up again anyway because demand exists and people are willing to take risks to meet it. Still, it is probably fair to say that pornography viewers in China appreciate the ability to surf online for pornography, as opposed to having to look for it in more public settings. In any event, the market is thriving. A large-scale study of China[92] reveals that the accumulated number of pornography sites continues to rise, despite the government's efforts.[93] When the Chinese government issues anti-pornography campaign news, porn visits dip for a day but usually bounce back afterward.[94]

CONCLUSION

The key point here is not that big data does not have some, maybe many, negative consequences for privacy—some of them quite severe. It does, and we are not trying to argue that the privacy literature errs in drawing attention to those negative impacts. Our point, rather, is that the failure to keep a more complete roster of impacts gives a distorted sense of the aggregate privacy impact of new technologies and data aggregations. In fact, calculating the aggregate privacy impact of these developments is very complicated and the right answer will vary a great deal depending on the user and his or her circumstances. In many cases, the same technology will enhance privacy vis à vis some actors while eroding with respect to others, and the key question—about which reasonable consumers will differ—is which privacies to value more highly.

More generally, the literature is obsessed with tallying the loss of a particular type of privacy—a privacy that involves security from tracking by large, remote entities. This form of privacy receives endless attention from activists and academics. But it is not the only type of privacy. And many technologies, we have tried to show, even while eroding this form of privacy, may simultaneously enhance the privacy of individuals in interaction with the people around them—a form of privacy to which academics and activists often pay a great deal less attention.

Consumers, in very large numbers, seem to be making different judgments from these academics and activists. And it will not do to dismiss those differences as the mere indulging of convenience. For many people, it may be privacy values that *cause* them to use Kindles or highly-trackable condom vendors. It's just a different form of privacy than the one that concerns the Electronic Frontier Foundation and the ACLU.

90 *Id.*

91 *Id.*

92 Zhaohui Liu, Lu Jiant, Qinhua Zheng, Zhenhua Tian, Jun Liu, and Junzhou Zhao, *A Peep at Pornography Web in China*, Working Paper (2010), *available at* www.cs.cmu.edu/~lujiang/camera_ready_papers/WEBSI_2010.pdf.

93 Christopher Beam, *They Know It When They See It: Is All Pornography Banned in China?*, Slate (June 24, 2009), http://www.slate.com/articles/news_and_politics/explainer/2009/06/they_know_it_when_they_see_it.html (last visited Jan. 27, 2015).

94 *Id.*

One of the present authors recently asked both of his teenage children whether Google was good or bad for their privacy. One of them said bluntly: "Of course Google is good for my privacy. I don't care what some server knows about me. But I care a lot what *you* know about me."[95] The other remarked that the subject is complicated, because Google offers a number of different services and they have different privacy implications. What's more, he noted, different aspects of different Google services have different privacy implications. Asked for an example, he noted the new feature of Gmail that allows users to recall emails for a short time after they have been sent. This, he notes, is a big advance for his privacy.[96] The complexity reflected in these responses seems to us to point to a profound truth about the relationship between technologies commonly assumed to erode privacy and the lived experience of privacy in the real world. That is, the relationship is multivariate and highly individualized.

Our privacy debate too often ignores that fact when it treats privacy as a generic good that is either increasing or decreasing. It seldom works that simply. There's no correct answer to the question of whether Woody Allen would have had more or less privacy had he not had to suffer the disapproving gaze of the woman in *Bananas* or the indignity of a shop-clerk shouting about his porn purchases across a store but if, instead, PornHub had collected data about his viewing habits—data that could leak in a data breach, be subject to the subpoenas, or be used to market pornography to him. There's only personal preference. Our privacy debate does not pay much attention to aggregated consumer preferences as a metric against which to measure privacy.

Perhaps, we venture to suggest, it should.

GOVERNANCE STUDIES

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance.aspx

EDITING, PRODUCTION & LAYOUT

Beth Stone

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU

95 Conversation between Benjamin Wittes and Elishe Julian Wittes.
96 Conversation between Benjamin Wittes and Gabriel Saul Wittes.