

# Privacy, Ideology, and Technology: A Response to Jeffrey Rosen

JULIE E. COHEN\*

## I. WHY PRY?

Jeffrey Rosen's *The Unwanted Gaze*<sup>1</sup> is in some ways an extraordinarily perceptive work. Rosen offers a compelling (and often hair-raising) account of the pervasive dissolution of the boundary between public and private information. This dissolution is both legal and social; neither the law nor any other social institution seems to recognize many limits on the sorts of information that can be subjected to public scrutiny. The book also provides a rich, evocative characterization of the dignitary harms caused by privacy invasion. Rosen's description of the sheer unfairness of being "judged out of context" rings instantly true.<sup>2</sup> Privacy, Rosen concludes, is indispensable to human well-being and is at risk of being destroyed unless we act fast. I have no quarrel with either of these conclusions.

The book is far less convincing, however, when it moves beyond description and attempts to identify the causes of the destruction of privacy and propose solutions. *Why* is privacy under siege today? The incidents that Rosen chooses as illustrations both reveal and obscure. From Monica Lewinsky's unsent, deleted e-mails to the private online activities of corporate employees and the Dean of the Harvard Divinity School, the examples offer a rich stew of technology, corporate mind control, public scapegoating, and political intrigue. But for the most part, Rosen seems to think that it is sex that is primarily to blame for these developments — though how, exactly, Rosen cannot seem to decide. He suggests, variously, that we seek private information out of prurient fascination with other people's intimate behavior, or to enforce upon others authoritarian notions of "correct" interpersonal behavior, or to inform moral judgments about others based on a hasty and ill-conceived equivalence between the personal and the political. Or perhaps Rosen is simply upset about the loss of privacy for a specific sort of (sexual or intimate) behavior, whatever the origin of society's impulse to pry.

Yet there are puzzling anomalies in Rosen's account. Most notably, appended to Rosen's excavation of recent sex-related privacy invasions is a chapter on privacy in cyberspace. This chapter sits uneasily in relation to the rest of the book. Its focus is not confined to sex-related privacy, and Rosen does not explain how the more varied information-gathering activities chronicled there bear on his earlier analysis.

---

\* Associate Professor, Georgetown University Law Center. Internet: jec@law.georgetown.edu. I thank Kristina Aberg for her able research assistance. © 2001, Julie E. Cohen. Permission is hereby granted for copies of this Review Essay to be made and distributed for educational use, provided that: (i) copies are distributed at or below cost; (ii) the author and *The Georgetown Law Journal* are identified; and (iii) proper notice of copyright is affixed to each copy.

<sup>1</sup> Jeffrey Rosen, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* (2000).

<sup>2</sup> *Id.* at 8-9.

Rosen acknowledges as much and offers, instead, the explanation that intimate privacy and cyberspace privacy are simply two examples of the same problem: the risk of being judged out of context in a world of short attention spans, and the harms to dignity that follow.<sup>3</sup> I find this explanation far too simple, and more than a bit circular. *Why* this rush to judge others out of context? Necessity is one answer — if attention spans are limited, we cannot avoid making decisions based on incomplete information — but where does the necessity to judge come from? And what do computers and digital networking technologies — factors that recur not only in the chapter on cyberspace privacy, but also in most of Rosen’s other examples — have to do with it?

This Review Essay offers some rather different answers to these questions. I shall argue, first, that the use of personal information to sort and classify individuals is inextricably bound up with the fabric of our political economy. As Part II explains, the unfettered use of “true” information to predict risk and minimize uncertainty is a hallmark of the liberal state and its constituent economic and political markets. Not sex, but money, and more broadly an ideology about the predictive power of isolated facts, generate the perceived necessity to judge individuals based on incomplete profiles. The harms of this rush to judgment — harms not only to dignity, but also to economic welfare and more fundamentally to individual autonomy — may undermine liberal individualism (as Rosen argues), but they are products of it as well. Part III argues, further, that the problem of vanishing informational privacy in digital networked environments is not *sui generis*, but rather is central to understanding the destruction of privacy more generally. This is not simply because new technologies reduce the costs of collecting, exchanging, and processing the traditional sorts of consumer information. The profit-driven search for personal information via digital networks is also catalyzing an erosion of the privacy that individuals have customarily enjoyed in their homes, their private papers, and even their thoughts. This process is transforming not only the way we experience privacy, but also the way we understand it. Privacy is becoming not only harder to protect, but also harder to justify protecting. Part IV concludes that shifting these mutually reinforcing ideological and technological vectors will require more drastic intervention than Rosen suggests.

## II. IDEOLOGY: PRIVACY, UNCERTAINTY, AND RISK

At bottom, *The Unwanted Gaze* is a work of political theory. Rosen’s ultimate focus, and his rallying point, is the role of the liberal state as guarantor of individual privacy. He argues that a liberal society should respect privacy because it is essential for individual dignity. Therefore, the liberal state should reject legal rules that create incentives to pry into private (especially sexual) matters, and should support legal rules that protect people’s desire to be left alone.<sup>4</sup> Unfortunately for this theory, however, the evidence is very much to the contrary. The liberal state, and the twin principles of Enlightenment scientism and market-based rationality upon which it rests, are centrally implicated in the destruction of

---

<sup>3</sup> *Id.* at 222-23.

<sup>4</sup> *Id.* at 211, 218-19.

privacy. Recourse to foundational principles of liberalism is far more likely to exacerbate the privacy problem than to solve it.

I will begin where Rosen begins, by focusing on the motives of those who collect personal information from individuals. As I have noted, Rosen focuses primarily on the problem of intimate information. This approach, however, begs important questions about the treatment of personal information more generally. Many studies have shown, and Rosen's own discussion of cyberspace privacy suggests, that contemporary American society now sanctions a greater degree of access to all sorts of information about individuals.<sup>5</sup> To understand why this is so, it would seem helpful to explore why those who collect personal information, both intimate and nonintimate, want it, and what they intend to use it for.

The answers to these questions suggest that sexual privacy is an incidental casualty of a different and far more comprehensive desire to know. Within the private sector, the impetus for the destruction of privacy is not prurience or prudishness, but core values that animate the rational marketplace behavior of profit-seeking entities. Americans are obsessed with sex, true, but we are even more obsessed with money. Our concern with private information is not its privateness or its prurience, but its potential to be converted into profit. Within society more broadly, the impetus for the destruction of privacy is a perceived equivalence between information processing and truth. We value information, including personal information, because we believe it will bring us omniscience, and with it the ability to predict preferences, behaviors, and needs and the opportunity to shape public (or private) policies accordingly. If Rosen is really concerned about the destruction of privacy in America, it is Adam Smith, René Descartes, and Jeremy Bentham, not Sigmund Freud or Catharine MacKinnon, with whom he must contend.

Employers are a case in point. Rosen posits that employers who want to shield themselves from sexual harassment liability will increase monitoring of interactions among employees.<sup>6</sup> This seems clearly right, but incomplete. There are lots of other things that employers want to know about both current and prospective employees: how hard they work, whether they will be expensive to insure, whether they pose risks to the safety of other employees or to the security of company property and trade secrets, and so on.<sup>7</sup>

---

<sup>5</sup> See, e.g., FED. TRADE COMM'N, *PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS* 15-18 (2000) [hereinafter FED. TRADE COMM'N, *PRIVACY ONLINE*]; OSCAR H. GANDY, JR., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* 53-94 (1993); SIMSON GARFINKEL, *DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY* 125-75 (2000); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1034-43 (1999).

<sup>6</sup> See ROSEN, *supra* note 1, at 81-90.

<sup>7</sup> See Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 3, 25-30 (1997); Philip M. Berkowitz, *Employee Privacy in the Age of Electronic Communications*, N.Y. L.J., Oct. 14, 1999, at 5; Charles Morgan, *Canada: Employer Monitoring of Employee E-Mail and Internet Use*, MONDAQ BUS. BRIEFING, July 30, 1999, available at 1999 WL 8711311; Joao-Pierre S. Ruth, *Careful . . . Your Boss May Be Watching*, BUS. NEWS N.J., Sept. 12, 2000, at 24; *Survival Guide: Small Fix-its for Work's Frustrations: On-Job Violence Is Preventable*, NEWSDAY, July 19, 1999, at C2; George B. Yancey, *The Predictive Power of Hiring Tools*, CREDIT UNION EXECUTIVE, July

Similar reasoning animates other marketplace actors, who want to know things that will help them structure investment risk, broadly defined. Insurers want to gauge the likelihood and magnitude of claims requiring payment, so that they can price policies accordingly.<sup>8</sup> Lenders want to assess the risk of default, so that they can set interest rates and collateral requirements.<sup>9</sup> The list goes on; it is easy to posit ways in which additional information might bear on the uncertainties that confront businesses. It is easier still to conform firm behavior to perceived correlations drawn from customer databases, with the result that hypotheses about risk become self-fulfilling prophecies. Those deemed unemployable or uninsurable may find it difficult to rehabilitate themselves when no one will employ or insure them.

In the realms of advertising and marketing, businesses want personal information not so much to minimize probable loss, but to structure expected gain. The “risk” to be minimized is the omnipresent, unquantifiable risk of making a lower profit than one might otherwise make. Access to consumer information reduces the sense of uncertainty that inevitably accompanies any venture because the information provides a vocabulary with which to talk about risk and profit potential. Information, including consumer information, transforms guesses into their more respectable cousins, estimates and projections. Estimates and projections, in turn, become predictions, imbued with a flavor of certainty that is no less real for being wholly unjustified.<sup>10</sup>

These beliefs about the relationship between information, risk, and profit are not anomalies within the liberal state, but rather are among its central pillars. Within a liberal market economy, it is an article of faith that both firms and individuals should be able to seek and use information that (they believe) will make them economically better off.<sup>11</sup> It follows that firms should be entitled to use personal information to minimize (projected) risk and to maximize (expected) profits, and should be entitled to demand this information as one condition of a consensual transaction. According to this view, privacy allows the

---

1, 2000, at 12.

<sup>8</sup> See *Financial Privacy: Hearing on H.R. 10 Before the Subcomm. on Fin. Inst. & Consumer Credit of the House Comm. on Banking & Fin. Servs.*, 106th Cong. 176-77(1999) (statement of Roberta B. Meyer, Senior Counsel, Consumer Affairs Unit, Amer. Council of Life Ins.); Schwartz, *supra* note 7, at 3, 26-28, 36-38; Anne Eisenberg, *Insurance-by-Mile Tested*, COM. APPEAL (Memphis, TN), Apr. 21, 2000, at C1; Matt E. Thatcher & Eric K. Clemons, *Managing the Costs of Informational Privacy: Pure Bundling as a Strategy in the Individual Health Insurance Market*, J. MGMT. INFO. SYS., Oct. 1, 2000, at 2957.

<sup>9</sup> See FED. TRADE COMM’N, FTC FACTS FOR CONSUMERS: CREDIT SCORING (Aug. 1998), available at <http://www.ftc.gov/bcp/online/pubs/credit/scoring.htm>.

<sup>10</sup> See, e.g., Nina Munk, *How I Started a Dot-Com for Dogs*, N.Y. TIMES, Oct. 15, 2000, § 6 (Magazine), at 82 (describing the process of creating a business plan as an “imaginary numbers game”).

<sup>11</sup> See Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 397 (1978); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 628-33 (1980); see also GANDY, *supra* note 5, at 95-122 (discussing documentary, anecdotal, and survey evidence about “corporate perspectives” on the collection and use of personal information).

individual to engage in a sort of arbitrage, by obtaining something she values highly at a lower rate than she could obtain in a world with less privacy.<sup>12</sup> In turn, the exposure gained by access to private information minimizes another sort of exposure — that of contracting parties to financial risk. Individuals are exposed so that other parties need not be.

This conflation of information with certainty and projections with predictions is not confined to markets. The destruction of privacy is the necessary byproduct of a particular set of beliefs about the predictive power of information that operate in both market and government spheres. Within this belief structure, nothing is random. Success in markets, politics, and policymaking can be predicted, and failure avoided, using the proper algorithms and the right inputs.<sup>13</sup> The ideology of the algorithm — of “more is better” — restores certainty, or at least cabins uncertainty, both in commerce and in public debate. In legal disputes, where uncertainty complicates questions of responsibility and remedy, every piece of information is presumptively relevant to the calculus of liability or guilt.<sup>14</sup> In addition, as Ms. Lewinsky’s case demonstrates, data collected and systematized by the private sector are then readily accessible for state compulsion, so that government need not confront the troublesome question of its power to compel the information directly from the affected individuals.<sup>15</sup>

The interests and practices implicated in the informational privacy debate, in short, are at once quotidian and deeply ideological. The need to judge others out of context is the logical product of rational self-interest when it occurs in markets and of rationalism, more broadly defined, when the agent is the state. Such a regime literally cannot operate without a constant supply of new information, and to suggest placing some of these inputs off limits merely because they are “personal” is to propose the ultimate heresy.

---

<sup>12</sup> See Posner, *supra* note 11, at 399-400; Stigler, *supra* note 11, at 628-33.

<sup>13</sup> See, e.g., ALBERT BORGMANN, *CROSSING THE POSTMODERN DIVIDE* 34-37, 68-71 (1992) (discussing “methodical universalism” and role that information processing plays in sustaining it); JACQUES ELLUL, *THE TECHNOLOGICAL SOCIETY* 79-147 (John Wilkinson trans., 1954) (describing the “modern technique” as a self-contained system of social ordering in which individual idiosyncrasies and moral considerations are subordinated to the demands of rationalizing methods and processes).

<sup>14</sup> The rules of evidence reflect this presumption. The standard of relevance is broad and lenient, while the standards for exclusion are for the most part narrow and specific. See FED. R. EVID. 401, 402; *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 587-88 (1993). Those who would exclude particular items of information under the catch-all “more prejudicial than probative” standard face an uphill battle. See FED. R. EVID. 403; *Heyne v. Caruso*, 69 F.3d 1475, 1480-81 (9th Cir. 1995); *Ballou v. Henri Studios, Inc.*, 656 F.2d 1147, 1153-55 (5th Cir. 1981); *United States v. Day*, 591 F.2d 861, 877-78 (D.C. Cir. 1978).

<sup>15</sup> See ROSEN, *supra* note 1, at 4 (discussing government subpoenas to Kramerbooks bookstore for records of Lewinsky’s book purchases); Michael Janofsky, *Police Seek Record of Bookstore Patrons in Bid for Drug Charge*, N.Y. TIMES, Nov. 24, 2000, at A37 (describing dispute between drug enforcement agents and bookstore over search warrant for sales records for books on methamphetamine manufacture).

To observe that the harvesting of private information is driven by both market and Enlightenment ideologies does not, of course, suffice to establish that it should trouble us. (For many, it will tend to suggest the opposite.) Yet data privacy regulation would not be the first instance in which society has determined that the common good requires limits on the profit-seeking behavior of private entities.<sup>16</sup> To decide whether society should set limits on the collection and use of personal information, and if so, how, one must consider what harms these behaviors cause and decide whether the harms outweigh the benefits that information processing produces.

Here it becomes important to understand exactly what “judged out of context” means, and what harms it signifies.<sup>17</sup> Rosen argues that even though such judging causes dignitary injury, people are still free to think and act as they please.<sup>18</sup> This explanation, too, seems incomplete. Judging others is not simply an idle pastime. Commercial actors judge in order to determine the commercial treatment (including prices and terms) that an individual will receive. State actors judge in order to allocate public resources and to mete out (or withhold) civil or criminal sanctions. These are decisions with concrete consequences. This is not to say that dignity is unimportant or undeserving of legal protection. Rather, it is to argue that privacy invasion also produces other, arguably more significant effects.

These third-party judgments, moreover, necessarily affect both the process of individuation and the limits of autonomy. Autonomy is inescapably a function of context and a matter of degree.<sup>19</sup> In particular, Rosen’s rejection of arguments from autonomy gives insufficient weight to the ways in which individuals’ thoughts, beliefs, and actions are shaped by the actions of others around them. We may think what we please, but we respond to the information that we are shown and to the ways that others treat us. Over time, this dynamic constructs and modifies habits, preferences, and beliefs. For this reason, commercial risk management and marketing practices focused on prediction shade imperceptibly, but inexorably, into attempts to mold individual behavior. As marketers and risk managers use past acts to shape future

---

<sup>16</sup> I use the term “regulation” loosely here to encompass any legal limitation (whether statutory, regulatory, or judge-made) on the gathering and use of personal information.

<sup>17</sup> It is worth noting here that Rosen’s characterization of the harm caused by privacy invasion necessarily implies a definition of “private” that extends far beyond sex-related activities and information.

<sup>18</sup> ROSEN, *supra* note 1, at 166-67.

<sup>19</sup> See Yochai Benkler, *Siren Songs and Amish Children: Autonomy, Information, and Law*, 76 N.Y.U. L. REV. (forthcoming 2001); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-25 (2000); Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 877, 885-90 (1994); cf. Martha C. Nussbaum, *Human Functioning and Social Justice: In Defense of Aristotelian Essentialism*, 20 POLIT. THEORY 202, 216-22 (1992) (developing a list of “basic functional human capabilities” and the circumstances that are necessary for humans to enjoy them); Martha C. Nussbaum, *Aristotelian Social Democracy*, in LIBERALISM AND THE GOOD 203, 219-25 (R. Bruce Douglass et al. eds., 1990) (same).

preferences and opportunities, prediction and control become inextricably linked.<sup>20</sup> As I have argued at greater length elsewhere, there is a very real risk that, over time, the market-driven culture of exposure may come to undermine the very qualities of individualism, entrepreneurship, and independence of thought that it professes to value.<sup>21</sup>

These are strong reasons that a society that values individual autonomy and strong citizens might want to set limits on the collection and use of personal information. Appealing to foundational principles of liberal individualism, however, does not (and cannot) tell us how to set about this task. Liberal ideology got us into this mess; it will not get us out. The conversation must proceed in some other way.

I do not mean to suggest that the law should compel businesses to throw caution to the winds and abandon any attempt to identify customers or project income streams, or that the law should abandon the use of circumstantial evidence to assess guilt or liability. Many of the purposes for which market and government entities seek personal data are entirely appropriate. Employers should be entitled to expect that their employees not engage in insider trading or misappropriation of trade secrets and should be entitled to adopt reasonable safeguards against such conduct. Lenders should be entitled to some information about borrowers' credit histories. Legal and policy disputes require resolution, and sometimes (though not always) personal information will bear on the appropriate outcome.

I also do not intend to suggest that rationalized information processing practices lack redeeming *social* value. To the contrary, the culture and practices of rationalized information processing serve important intrinsic and instrumental values relating to freedom of thought, inquiry, and expression. Thus, there are also strong arguments *against* placing limits on the collection and use of information. These arguments are familiar, and I will not belabor them here.

What I wish to argue, instead, is that in debates about privacy law and policy, ideology and necessity blur in important and outcome-determining ways, and that this blurring makes resolution of informational privacy issues extraordinarily (and unnecessarily) difficult. We profess to believe that individuals should be subjects and not objects of information. This belief springs from another foundational principle of liberal individualism: the notion that respect for individual autonomy requires individualized

---

<sup>20</sup> Cohen, *supra* note 19, at 1403-08. This dynamic suggests, as well, that Rosen's cry for "context" conceals a danger. More context would not change the fact that profiling reduces and constructs. Cognitively, making sense of any context requires a sorting algorithm that treats some information as more important than other information. *See generally* GEOFFREY C. BOWKER & SUSAN LEIGH STAR, *SORTING THINGS OUT* (1999). Even as profiles grow more and more detailed, the act of classification and its consequences still may cause harm.

<sup>21</sup> Cohen, *supra* note 19, at 1406-08, 1424-27. In his concluding observations, Rosen appears to recognize that scrutiny will affect behavior, but resists the conclusion that it therefore affects autonomy, or produces lasting changes in individual personality. ROSEN, *supra* note 1, at 210-18.

treatment.<sup>22</sup> Even so, the rationale for considering particular items of personal information rapidly devolves into an argument in favor of collecting and using every piece of information that can be obtained. Then, because technologies for collecting information do not readily distinguish between legitimate and illegitimate purposes, a legitimate reason for monitoring can be used to bootstrap a comprehensive monitoring regime. Meanwhile, the ideology of the algorithm diverts attention away from other possible ways of designing information tools and collecting information while minimizing the privacy harms to individuals. But a world in which more information is known and processed is a world that treats individuals as (manipulable) objects for more and more purposes.<sup>23</sup>

A world where information-processing practices are a matter of ideology is a very difficult place to have a conversation about limits, or about the impact of data processing rules and practices on the lived experience of ordinary people. It is important to understand that this dynamic arises within and because of liberal ideology, not despite it. Addressing the informational privacy problem requires pragmatic balancing of competing values. To proceed with this project in any meaningful way, one must first acknowledge that competing values exist. The belief that more personal information always reveals more truth is ideology, not fact, and must be recognized as such for informational privacy to have a chance.

### III. TECHNOLOGY: PRIVACY, PROPERTY, AND LICENSE

Still unexplored is the role that digital network technologies play in facilitating the profit-driven search for personal information and extending the underlying ideology of rationalized information processing. Both in his chapter on internet privacy and elsewhere throughout the book, Rosen makes clear his belief that digital technologies are implicated in the destruction of privacy. If one is concerned about reversing the destruction of privacy, however, it is important to specify the relationship between technology and privacy more precisely. Information technology is not simply a passive conduit for preexisting social values. The capabilities (and disabilities) of artifacts also shape social practices and priorities. The capabilities and limits of digital information technologies are changing not only the amount of privacy we enjoy, but also the ways in which we think about the privacy to which human beings are entitled.

One possible explanation for the relationship between digital technologies and privacy is that technology is a simple multiplier. Digital technologies reduce the costs of privacy invasion, and this reduction causes significant quantitative shifts in the behavior of both commercial and government actors. Commercial actors can amass and process a greatly increased volume and variety of data about their customers, and governments about their citizens. On this theory, though, digital processing of transactional and official data does not move new sorts of information into the public arena. Increased data collection

---

<sup>22</sup> Think, for example, of the due process clauses. U.S. CONST. amends. V, XIV.

<sup>23</sup> The result is, as Robert Post so aptly describes in this Symposium, a clash of two social structures, but the clash is increasingly one-sided. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001).

and processing capacity simply generates more — more detailed, more permanent records of more activities that were always, in some sense, open to public view.<sup>24</sup>

Many commentators, however, reject this view of the interaction between technology and privacy as too simplistic. As early as the 1970s, a majority of the Supreme Court suggested that the ready availability of “vast amounts of personal information” in digitized form might pose a qualitatively new sort of privacy threat.<sup>25</sup> More recent commentators have argued that the threat lies not merely in the ease of access to digitized data, but also in the new and more complex permutations and profiles that interlinked digital databases enable.<sup>26</sup> To similar effect, a strand of the philosophical literature on privacy argues that new “data mining” practices violate the customary presumption that individual behavior will be noted, and its consequences felt, only in the particular “discrete social sphere” that the individual intended.<sup>27</sup> Still others have observed that digital data processing technologies also collect new, formerly unavailable data about individuals’ activities, including browsing and (virtual) window-shopping activities, reading and listening habits, and (by implication) ideological preferences.<sup>28</sup> In aggregate, these different accounts and approaches suggest persuasively that digital technology does not simply gather more of the same data, but that it also collects more kinds of data and is employed to generate far more comprehensive “truths.”<sup>29</sup>

---

<sup>24</sup> Conversely, digital technologies do not nullify the privacy protections afforded by the federal Freedom of Information Act, 5 U.S.C. §552a (2000), and analogous state laws just because they make it easier for the government to collect information.

<sup>25</sup> *Whalen v. Roe*, 429 U.S. 589, 605 (1977).

<sup>26</sup> See, e.g., A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 479-505 (1996).

<sup>27</sup> See Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559, 581-86 (1998); Jonathan Schonsheck, *Privacy and Discrete “Social Spheres,”* 7 ETHICS & BEHAV. 221, 222-24 (1997). Rosen appears to concur in this view. See ROSEN, *supra* note 1, at 197-210.

<sup>28</sup> Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 CONN. L. REV. 981, 983-86 (1996); Jerry Kang, *Informational Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198-99, 1223-30 (1998).

<sup>29</sup> The modern direct marketing industry is predicated on this belief (though not disturbed by it); more information is collected and treated as a valued asset precisely because it is thought to generate better, more accurate insights about human character, behavior, and preferences.

But these synergistic, or “panoptic,” theories of privacy invasion still do not go far enough.<sup>30</sup> Digital technologies do more than shrink experienced privacy. The interaction between monitoring technologies and behavior is dynamic. The design of technologies is driven, in the first instance, by (conscious and unconscious) decisions about what values are important and what results the technology should produce. The resulting technologies, however, then structure not only behavior, but also behavioral and policy norms. Technologies (human-designed artifacts) produce feedback loops.<sup>31</sup> For at least the past several decades, firms and governments have been designing information systems to enable the inexpensive accumulation and seamless combination and recombination of collections of personal information. Systems designed to smooth the way for large-scale collection and processing of personal information also affect prevailing understandings of the privacy to which individuals are or should be entitled and the basis on which they might be entitled to claim it.

The profit-motivated search for predictive information is transforming the design of living and work spaces and of structures for delivering intellectual goods, and at the same time it is transforming the conceptualization of these spaces and activities. In the process, traditional distinctions between private and public spaces, and between private and public realms of activity, are collapsing. In their place is emerging a very different conception of the boundary between public and private and its implications for privacy law and policy. Within this vision, neither places nor thoughts are sacrosanct. Instead, privacy is an inverse function of the extent to which licensed chattels and information goods require, and consumers “consent” to, information collection.

To see how digitization drives this conceptual shift requires careful attention to the historical and theoretical roots of privacy protection. Historically, both place and autonomy have been central to judicial elaboration of privacy rights. Nowhere has the freedom from outside scrutiny been greater than in spaces traditionally considered private — for example, living spaces — and in activities strongly linked to autonomy: one’s private papers, thoughts, and interpersonal associations.<sup>32</sup> Other physical spaces, such

---

<sup>30</sup> Jeremy Bentham theorized a prison, the Panopticon, built in concentric rings of cells around a central guard tower, from which a guard could observe the occupants of each cell at any time. He argued that the potential for visibility at all times would be a powerful and efficient instrument of social control. Modern privacy theorists have observed that Bentham’s insight about the link between visibility and control extends far beyond prisons. *See, e.g., GANDY, supra* note 5, at 21-23 (discussing Bentham’s Panopticon); ROSEN, *supra* note 1, at 213-14 (same).

<sup>31</sup> *See, e.g., DONALD MACKENZIE, KNOWING MACHINES: ESSAYS ON TECHNOLOGICAL CHANGE* (1997); LANGDON WINNER, *AUTONOMOUS TECHNOLOGY: TECHNICS-OUT-OF-CONTROL AS A THEME IN POLITICAL THOUGHT* (1977).

<sup>32</sup> *See, e.g., Wilson v. Layne*, 526 U.S. 603, 609-13 (1999) (holding that inviting newspaper reporter to witness arrest violated Fourth Amendment protection of privacy of the home); *Minnesota v. Olson*, 495 U.S. 91, 97-100 (1990) (holding that Fourth Amendment protects privacy of overnight guest in private home); *Stanley v. Georgia*, 394 U.S. 557, 565-66 (1969) (holding that law criminalizing private possession of obscene reading materials violated the First Amendment); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 466 (1958) (holding that First Amendment forbids compelled disclosure of membership records of private organization); *Mas v. Perry*, 489 F.2d 1396, 1398 (5th Cir. 1974) (enforcing common-law privacy rights of residential tenant in rented apartment).

as work spaces, have been held to afford an intermediate degree of privacy.<sup>33</sup> Public streets are not private at all, but enclaves within otherwise public space — for example, public bathrooms and telephone booths — may generate legally cognizable expectations of privacy because of the nature of the activities that take place there.<sup>34</sup> Thus, Rosen quite logically organizes his discussion of privacy first around physical location — privacy at home, at work, in court, online — and to a lesser extent around privacy of thought.

At a theoretical level, however, the precise nature of — and justification for — privacy remains unclear. Descriptively, privacy has been defined as freedom from scrutiny, control, or intrusion by others.<sup>35</sup> This understanding of privacy as freedom-from implies a correlative freedom-to: Absent external scrutiny, control or intrusion, one may behave as one wishes. Yet this formulation leaves unaddressed some rather important questions about the location and nature of the boundary between privacy and freedom. Is the freedom that “privacy” guarantees best characterized as a privilege with which others have no right to interfere? If so, is the privilege rooted in formal, relatively immutable notions of physical place, or in a broader and more flexible conception of autonomy? Alternatively, is the “privacy” of private spaces and thoughts simply contingent — a Hohfeldian liability that is subject to erosion as technology evolves?<sup>36</sup>

These questions have moral as well as jurisprudential valence. Modern privacy advocates, including both Rosen and myself, conceive of privacy as a species of constitutive freedom and view that freedom as both intrinsically and instrumentally valuable. Some critics, however, have viewed privacy (or at least some kinds of it) disparagingly, as license. On this view, privacy betokens a dangerous absence of moral constraints, and too much privacy is as great an evil as too little.<sup>37</sup> Privacy also has relational implications; some feminist theorists have argued that traditional place- and family-centered notions of

---

<sup>33</sup> See, e.g., *O'Connor v. Ortega*, 480 U.S. 709, 716-18 (1987) (desk in employee's private office); *Dawson v. Texas*, 868 S.W.2d 363, 370-71 (Tex. Ct. App. 1993) (private locker in employee dressing room).

<sup>34</sup> See, e.g., *Katz v. United States*, 389 U.S. 347, 353 (1967) (telephone booth); *Haley v. State*, 696 N.E.2d 98 (Ind. Ct. App. 1998) (tent at public campground); *People v. Kaslowski*, 608 N.W.2d 539, 541 (Mich. Ct. App. 2000) (wrapped package delivered by private freight carrier); *Harkey v. Abate*, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (public bathroom).

<sup>35</sup> See, e.g., Kang, *supra* note 28, at 1202-04 (surveying the case law and literature and identifying three “clusters” of privacy values: spatial, decisional, and informational); Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA CPTR. & HIGH TECH. L.J. 27, 30 (1995) (“[P]rivacy is the condition in which others are deprived of access to you.” (emphasis omitted)).

<sup>36</sup> See Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 28 YALE L.J. 16, 32-54 (1913).

<sup>37</sup> Cf., e.g., *Bowers v. Hardwick*, 478 U.S. 186, 195-96 (1986) (refusing to recognize a fundamental constitutional right to engage in consensual homosexual sodomy).

privacy may reinforce and perpetuate inequality, subordination, and violence.<sup>38</sup> A society's definition of the scope and limits of privacy says much about its theoretical or intellectual understanding of concepts such as freedom and equality, but also much about its normative or moral understanding of these concepts.

The lack of clarity at the theoretical and normative roots of privacy doctrine matters because the traditional legal and behavioral barriers that have demarcated private space and private conduct have come under pressure as the material conditions of privacy shift.<sup>39</sup> A shift in the material conditions of privacy can be architectural in the traditional sense; apartment dwellers enjoy less privacy than residents of single-family homes. But such shifts also can be caused by other kinds of design choices. Historically, private property has served as the primary barrier to privacy invasion. The primary agent of privacy invasion was the state, and important constitutional protections constrained the state's ability to enter and search private premises. Now, however, monitoring and data collection capabilities are routinely embedded in the design of spaces, tools, network protocols and applications, and even documents. Smart microchips in homes, appliances, and cars can monitor use and report via digital networks to utilities, equipment lessors, toll collectors, and other third parties.<sup>40</sup> "Cookies" and "web bugs" can generate records of internet browsing activities.<sup>41</sup> Documents and other digital files can be designed to report to software manufacturers, or to allow only

---

<sup>38</sup> See, e.g., ROBIN WEST, PROGRESSIVE CONSTITUTIONALISM 58-65, 118-21 (1994); Mary E. Becker, *The Politics of Women's Wrongs and the Bill of "Rights": A Bicentennial Perspective*, 59 U. CHI. L. REV. 453, 508-09 (1992); Catharine A. MacKinnon, *Reflections on Sex Equality Under Law*, 100 YALE L.J. 1281, 1311-24 (1991); Reva B. Siegel, "The Rule of Love": *Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117, 2154-74 (1996); Malinda L. Seymore, *Isn't It a Crime: Feminist Perspectives on Spousal Immunity and Spousal Violence*, 90 NW. U. L. REV. 1032, 1072-73 (1996); Nadine Taub & Elizabeth M. Schneider, *Women's Subordination and the Role of Law*, in THE POLITICS OF LAW: A PROGRESSIVE CRITIQUE 328, 331-35 (David Kairys ed., 3d ed. 1998).

<sup>39</sup> See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 143-57 (1999); Reiman, *supra* note 36, at 43-44.

<sup>40</sup> See GARFINKEL, *supra* note 5, at 82-84; Eisenberg, *supra* note 8; Susan Gregory Thomas, *The Networked Family*, U.S. NEWS & WORLD REPORT, Dec. 1, 1997, at 66, available at <http://www.usnews.com/usnews/issue/971201/1futu.htm> (last visited Mar. 26, 2001); David Lammers, *Smart Appliances Hit the Net*, TECHWEB NEWS, at <http://www.techweb.com/wire/story/TWB20000118S0032> (Jan. 18, 2000).

<sup>41</sup> See U.S. Dept. of Energy, Computer Incident Advisory Capability, *Information Bulletin I-034: Internet Cookies* (Mar. 12, 1998), available at <http://www.ciac.org/ciac/bulletins/i-034.shtml> (last visited Mar. 26, 2001); Adam Cohen, *Paranoia: Spies Among Us*, TIME DIGITAL, July 2000 at 32, available at <http://www.time.com/time/digital/reports/paranoia/index.html> (last visited Mar. 26, 2001); Neil J. Rubenking, *Who's Watching You Surf?*, PC MAG., June 26, 2000, available at <http://www.zdnet.com/pcmag/stories/solutions/0,8224,2586415,00.html> (last visited Mar. 26, 2001); Roger Clarke, *Cookies*, at <http://www.anu.edu.au/people/Roger.Clarke/II/Cookies.html> (last modified Jan. 13, 2001); *Emails Can Betray Personal Info*, WIRED NEWS, at <http://www.wired.com/news/print/0,1294,32857,00.html> (Dec. 3, 1999); Paul Festa, *IE Hole Exposes Web Surfers' Private Data*, CNET NEWS.COM, at <http://news.cnet.com/news/0-1005-202-1857707.html> (May 11, 2000); Chris Oakes, *Mouse Pointer Records Clicks*, WIRED NEWS, at <http://www.wired.com/news/print/0,1294,32788,00.html> (Nov. 30, 1999); Richard M. Smith, *Web Bug Basics*, at <http://www.privacyfoundation.org/education/webbug.html#1> (last visited Mar. 26, 2001).

certain actions but not others.<sup>42</sup> Incorporation of persistent identifiers into personal computer microprocessors and internet addressing protocols is a recurring possibility.<sup>43</sup>

The rationale for these new kinds of privacy invasion is consent as incident to a commercial transaction between equal parties. In some cases, consent to collect information is presumed, and technologies are designed surreptitiously (or simply without comment) to enable it.<sup>44</sup> The degree of privacy actually experienced becomes a function of self-help; users can defeat these functions, but only if they can figure out how. In other cases, formal contractual provisions govern data collection and use. Inanimate objects formerly conceived as personal property — software, telecommunications equipment, and even temporary electronic copies of Web content — are distributed under licenses that require individuals to consent to data collection. “Privacy policies” attached to these items often simply serve to notify individuals of the control that they do not have.<sup>45</sup> Effectively, these digital technologies and information goods have become the data processor’s agents rather than the individual’s chattels.

Once again, none of this, or at least very little of it, is about sex. The increased monitoring of private spaces drives toward quite a different end. The colonization of private spaces by cookies, web bugs, smart microchips, and self-enforcing licenses is an entirely predictable consequence of the market-driven search for more and better information. If information is money, there is no reason to expect that the desire for more information should stop politely at the residential doorstep or its virtual equivalent. And if the state wants this information, or if a third party wants to use state process to compel its production, it is harder to argue against that result if the information, presumptively relevant, is already there.

This spatial and legal reconfiguration inverts privacy at the most fundamental, epistemological level. In a world where objects carry license to invade privacy, whether one is “at home” or “at work” becomes increasingly irrelevant. Similarly, privacy of thought becomes substantially less relevant in a world where documents can report on their owners and where digital networks can create large databases of people’s

---

<sup>42</sup> See Lee A. Bygrave & Kamiel J. Koelman, *Privacy, Data Protection and Copyright: Their Intersection in the Context of Electronic Copyright Management Systems*, in COPYRIGHT AND ELECTRONIC COMMERCE 59, 60-63, 108-09 (P. Bernt Hugenholtz ed., 2000); Associated Press, *Mattel Removes Software Feature Over Privacy Concerns*, CNET NEWS.COM, <http://news.cnet.com/news/0-1006-202-2152384.html> (June 26, 2000); Daniel J. Gervais, *Electronic Rights Management and Digital Identifier Systems*, J. ELECTRONIC PUB. (Mar. 1999), at <http://www.press.umich.edu/jep/04-03/gervais.html>; Mike Ricciuti, *Microsoft Admits Privacy Problem, Plans Fix*, CNET NEWS.COM, at <http://news.cnet.com/news/0-1006-202-339622.html> (Mar. 7, 1999); Richard M. Smith, *The RealJukeBox Monitoring System*, at <http://users.rcn.com/rms2000/privacy/realjb.htm> (last visited Mar. 26, 2001).

<sup>43</sup> See Shawn C. Helms, *Translating Privacy Values with Technology*, 7 J. SCI. & TECH. L. (forthcoming 2001) (discussing Intel’s Processor Serial Number project and the Internet Engineering Task Force project to design permanent addressing features for the sixth version of the Internet protocol TCP/IP).

<sup>44</sup> See Rubenking, *supra* note 41; Clarke, *supra* note 41; Oakes, *supra* note 41. The surreptitiousness, of course, belies the presumption of consent.

<sup>45</sup> See, e.g., FED. TRADE COMM’N, PRIVACY ONLINE, *supra* note 5, at 10-16.

reading, viewing, and listening habits. Rights (and thus expectations) are defined by instrumentality rather than by location, and by (fictional) consent rather than by any sense of the inherent inviolability of private papers and thought processes. Privacy is still about license, but now in a wholly different sense than the debate about privacy and morality once presupposed. The locus of license-as-freedom has shifted to the designers of artifacts and tools. Increasingly, individual users of these artifacts will enjoy only whatever privacy the data collectors have not seen fit to take.

If privacy constructs personality, moreover, the shift to a consent-based understanding of privacy cannot simply be a neutral matter. Here, Rosen's plea for recognition of private zones even within nominally public spaces, such as the workplace, does not go far enough. Drawing on the work of Erving Goffman, Rosen posits that employees require a "backstage" so that they can do their jobs effectively.<sup>46</sup> If this is true, though, the argument for a backstage in our own homes and our own thoughts is even more compelling. Once again, the argument flows not only from dignity, but more fundamentally from autonomy. What violates dignity may also construct behavior, preferences, opinions, and beliefs, as individuals strive to minimize the real (or imagined) harms that may flow from being watched. Rather than presuming we can do what we please in private spaces, we may come to presume that we can do only what others permit and read only what others approve.

In sum, networked digital technologies do not simply make the privacy problem more acute. They make it different. In a very literal sense, technology is displacing privacy. Privacy in formerly private places or spheres of activity can no longer be presumed, or even presumed to be good. The (re)design of information technologies to facilitate the profit-driven pursuit of personal information increasingly forecloses not only the experience of privacy, but also alternative, place- or autonomy-centered understandings of privacy. Any prescription for reversing the destruction of privacy must consider, and address, this dynamic and the combination of ideology and technology that has produced it.

#### IV. BREAKING THE CYCLE

Rosen argues that reversing the destruction of privacy is, first and foremost, a matter of wanting to do so.<sup>47</sup> It is difficult to quarrel with this general statement, but equally difficult to glean any specific direction from it. At different points in the book, however, Rosen also suggests that invasion of privacy lawsuits or widespread adoption of privacy self-help technologies might remedy specific privacy problems.<sup>48</sup> We are now in a position to evaluate these recommendations. Although I would like Rosen to be right about the ready availability of tools for reversing the destruction of privacy, I suspect that his

---

<sup>46</sup> ROSEN, *supra* note 1, at 122-27 (citing ERVING GOFFMAN, *THE PRESENTATION OF SELF IN EVERYDAY LIFE* 128-30 (1954)). I leave aside Rosen's apparent belief that sexual advances toward fellow workers belong backstage.

<sup>47</sup> *See* ROSEN, *supra* note 1, at 194-95.

<sup>48</sup> *Id.* at 117-23, 173-77.

proposed strategies are too reactive to dislodge the mutually reinforcing ideological and technological vectors that shape contemporary information processing practice.

First, it is becoming increasingly clear that the common law invasion of privacy torts will not help to contain the destruction of informational privacy.<sup>49</sup> Lawsuits by individuals outraged at the unauthorized sale and use of their personal information have been uniformly unsuccessful. Courts have responded to these novel informational privacy claims (based on the “unauthorized appropriation of name or likeness” branch of privacy doctrine) as if inspired by Lewis Carroll’s Red Queen: Personal information is only valuable in aggregate, so individuals have no basis to claim injury against those who wish to sell their information for value;<sup>50</sup> personal information has not been “appropriated” unless the entity that has collected it to use and exchange for value also releases it to the general public;<sup>51</sup> personal information including correct, current address information is not the individual’s if the name is slightly misspelled.<sup>52</sup> While courts have recognized a privacy interest in sexual or intimate information (pursuant to the “embarrassing facts” branch of privacy doctrine), they are unlikely to hold that, for example, processing and sale of routine transactional data constitutes an embarrassing disclosure of private facts.<sup>53</sup>

It is, of course, an overstatement to say that the common law is incapable of change. The hallmark of the common law is gradualism, and it is possible that judicial resistance to informational privacy claims might gradually weaken to accommodate emerging societal preferences for more privacy.<sup>54</sup> Where

---

<sup>49</sup> To be fair, Rosen does not argue this, but argues instead that the common-law tort of intrusion upon seclusion might usefully be adapted to redress (some instances of) workplace harassment. This may or may not be right (I have my doubts); the implicit suggestion, however, is that a combination of inquisitorial self-restraint, individual self-help, and judicious application of the common law will be sufficient to cure society’s privacy woes.

<sup>50</sup> *Dwyer v. American Express, Inc.*, 652 N.E.2d 1351, 1353 (Ill. App.Ct. 1995). *But see* *Weld v. CVS Pharmacy*, 1999 WL 494114 (Mass. Super. Ct. June 29, 1999) (declining to grant summary judgment for defendant on invasion of privacy claims similar to those brought in *Dwyer*).

<sup>51</sup> *Shibley v. Time, Inc.*, 341 N.E.2d 337 (Ohio Ct. App. 1977).

<sup>52</sup> *See* GARFINKEL, *supra* note 5, at 178-81 (discussing Virginia trial court’s dismissal of lawsuit by Ram Avrahami against U.S. News & World Report, Inc.)

<sup>53</sup> With respect to sexual privacy in particular, Rosen suggests that many invasions shouldn’t be cognizable at law, but only in the court of public opinion. ROSEN, *supra* note 1, at 117-27, 219-22. To divorce norms and market practices from law in this fashion, however, is profoundly disingenuous. As Rosen himself recognizes in his discussion of the employer incentives created by sexual harassment law, law and norms, or more broadly “culture,” are mutually constituting. *See* Naomi Mezey, *Law as Culture*, 13 YALE J.L. & HUMAN. 101 (forthcoming 2001). It is quite likely that contemporary norms about acceptable workplace behavior derive in part from internalization of the mandates of sexual harassment law, and would not have developed without this impetus.

<sup>54</sup> *Cf.* Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003 (2000) (arguing that the common law is better suited than constitutional law to develop the right balance between disclosure and privacy norms).

informational privacy is concerned, however, the common law also contains within it the seeds of powerful resistance. In particular, if licensed access to privately provided resources is the engine of privacy invasion, it seems wishful to think that the common law — the law of contract and private property — will divert it. In a world of digital networks and embedded microprocessors, private property and private contract become barriers to effective public protection of individual privacy. Paired with thin conceptions of consent, private property rights signify *carte blanche* to collect information about readers and listeners, and to demand changes in the design of networks that will eliminate anonymity for consumers of information services and intellectual goods.

Second, even if widely adopted, privacy self-help technologies face significant external limitations. These technologies are relatively effective at defeating casual monitoring of internet browsing, but (so far, at least) much less effective once the individual becomes a customer or licensee.<sup>55</sup> In such cases, the amount of privacy protection available will depend in large part on the systems in use for approving and processing consumer transactions and on the underlying technical standards that support the systems.<sup>56</sup> Privacy self-help technologies do not alter these commercial and technological infrastructures, nor do they alter the process by which technical standards enter the commercial mainstream.<sup>57</sup> Wanting more privacy is a start, and taking measures to protect one's own privacy is even better, but a massive commercial, technological, and contractual infrastructure designed to facilitate data collection and processing cannot just be wished away.

The call for greater informational privacy is, fundamentally, a critique of the political economy of information markets. To produce meaningful changes in the culture and practice of information processing, reforms must operate at both structural and ideological levels. At the structural level, firms and governments must be willing to fund research on privacy-enhancing technologies and to integrate these technologies into commercial and official information systems and practices once they have been developed. At the ideological level, firms and governments must learn to accept that perfect control of

---

<sup>55</sup> See Daniel Tynan, *Privacy 2000: In Web We Trust?*, PC World, June 2000, <http://www.pcworld.com/features/article/0,aid,16444,pg,1,00.asp> (last visited Mar. 26, 2001); see also *On Internet Privacy and Profiling: Hearing Before the Senate Comm. on Commerce*, 106th Cong. (2000) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center) (arguing that effective privacy protection requires the development of privacy-protective technologies for electronic commerce and that this will not happen without legislation), available at <http://www.epic.org/privacy/internet/senate-testimony.html> (last visited Apr. 9, 2001). Companies like Zero Knowledge Systems are attempting to develop anonymous transaction protocols, but there is little evidence of mainstream commercial interest in these systems. See Tynan, *supra*.

<sup>56</sup> See Helms, *supra* note 43; Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶¶ 62-98 (Feb. 2001), at [http://stlr.stanford.edu/STLR/Articles/01\\_STLR\\_1](http://stlr.stanford.edu/STLR/Articles/01_STLR_1).

<sup>57</sup> Consumer protests might affect these processes, as might legislation or judicial recognition of a privacy interest in personal information. Whether market pressures alone will suffice is the subject of a vigorous debate, and is beyond the scope of this Review Essay.

2001]

PRIVACY, IDEOLOGY, AND TECHNOLOGY

uncertainty and risk cannot be achieved even with limitless information, and that limiting access to and use of personal information also may promote important social values. These are not easy projects, but these are not minor changes. To the extent that *The Unwanted Gaze* contributes to a more serious, sustained conversation about the importance of privacy, it sets us on the path, and that is no small accomplishment.