March, 2005

Surveillance and the Self: Privacy, Identity, and Technology

Richard Warner, *Chicago-Kent College of Law*

SURVEILLANCE AND THE SELF: PRIVACY, IDENTITY, AND TECHNOLOGY

*Richard Warner**

INTRODUCTION

Advances in surveillance techniques have greatly increased the power of others to eavesdrop on our lives. Both government and private business have eagerly availed themselves of these advances; so have terrorists, organized crime, and other wrongdoers. New technologies help them conceal their activities as well as increase their scope and effectiveness.[1] Governments and private businesses have responded with sophisticated surveillance technologies. In the latter case, new data collection and analysis techniques not only protect against wrongdoers, but they also greatly increase efficiency. The price is a significant loss of privacy. Is the price too high? To what extent—if any—should we trade privacy for protection and efficiency?

Finding an acceptable tradeoff requires a proper appreciation of the value of privacy, an appreciation we currently lack. Yet, this may seem obviously wrong. After all, political philosophy, for the last three hundred years, has emphasized the critical role of privacy in limiting the power of the state, and, although we may disagree about how to protect privacy, by now we surely all agree that allowing the state to reach too deeply into its citizens' lives puts freedom at risk. However, serving as a shield against an overintrusive state is not the only reason privacy matters. It also matters to the self; sufficient control over what others know about us is essential to realizing our identities as persons. This aspect of privacy has received insufficient attention.[2]

---

* Professor, Chicago-Kent College of Law; Professor, Chair of American and Comparative Law, Catholic University of Lublin, Poland. This Article is based upon a presentation given at the DePaul University College of Law Symposium: *Privacy and Identity: Constructing, Maintaining, and Protecting Personhood* held on Saturday, March 13, 2004.

1. *See generally* Louise I. Shelley, *Organized Crime, Terrorism and Cybercrime*, *in* SECURITY SECTOR REFORM: INSTITUTIONS, SOCIETY AND GOOD GOVERNANCE 303–12 (Nomos ed., 2003).

2. The link between privacy and self has been much discussed. *See generally* Stanely I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XIII: PRIVACY (J. Ronald Pennock & J.W. Chapman eds., 1971); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Jeffrey H. Rieman, *Privacy, Intimacy, and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 300 (Ferdinand David Schoman ed., 1984); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

I focus exclusively on the relation between privacy and the self, and I also narrow my focus in two other ways. First, I confine this Article primarily to privacy threats created by the Internet. The Internet is the nerve center of the technological innovations that create privacy concerns. Much of what this Article argues, however, will generalize to non-Internet contexts. Second, I consider only non-governmental threats to privacy. The governmental threat is increasingly worrisome. However, the chorus of concern in that case is already large and strong, and the threat from private business merits consideration on its own. In analyzing the business threat, I concentrate on the gain in efficiency from surveillance technology, not its use to prevent wrongdoing.

The aspect of privacy with which I am concerned is what Jerry Kang labels "informational privacy."[3] Professor Kang distinguishes three types of privacy rights: spatial, decisional, and informational.[4] Spatial rights define a physical zone of control over intrusions by others; decisional rights protect an individual's freedom of choice; informational rights demarcate an ability to determine what others know about us and what they do with that knowledge. I focus on informational rights, and when I refer to "privacy" I mean primarily the power to control what others can learn about us and what they can do with what they learn. To ensure sufficient power in this regard, businesses should be required to obtain our consent before they collect certain types of information about us. Current privacy law does not impose such a requirement.[5] I also argue that the "consent requirement" is insufficient on its own to protect privacy adequately.

Part II reviews the important link between advertising and market efficiency, a link often overlooked in discussions of privacy. Part III explains the role of privacy in the construction of our identities. Part IV introduces the "consent requirement," the requirement that businesses obtain consent before collecting certain types of information; this Part also considers and answers objections based on the claim that the requirement treats privacy as if it were property. Part IV concludes by contending that the major issue in regard to the consent requirement is whether it really succeeds in protecting privacy against technological threats. Part V identifies the threats. Part VI contends

---

My view is that these discussions overlook the critical place of "social roles" in development of the self and the relation between the self and privacy. *See infra* Part III.C.

3. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1205–12 (1998).

4. *Id.* at 1202–05.

5. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003) (analyzing and criticizing the current state of privacy law).

that the consent requirement provides important protection but is not a complete solution, and calls for additional statutory protection.

II. Efficiency, Information, and Technology

When considering business threats to privacy, it is easy, in the eagerness to protect privacy, to overlook the critical role that information plays in enabling the market exchanges that provide us with goods and services.[6] Consequently, I begin with a reminder of the remarkable cooperation that the market makes possible.

A. Information and Market Efficiency

Charles Lindblom's engaging example illustrates the coordination involved in a typical sequence of market exchanges:

> During the course of a morning, a number of people step into a Milan café for an espresso. They do not doubt that it will be available. What justifies their confidence? Making the coffee available rests on a great deal of cooperation, specifically, the assignment to many people of performances that together accomplish a feat far beyond the capacity of any one person alone. It is accomplished by market transactions that assign and link both multiple performances and multiple chains of them. Farmers cooperate in growing and harvesting the coffee beans. Truck drivers or locomotive engineers transport the beans to a seaport on highways or railroads that have been constructed by many kinds of cooperating laborers. At the seaport, longshoremen and ships' crews join the chain. At a dock in Genoa, shipping the beans on to Milan calls again on performances from longshoremen, warehousers, and truckers. Somewhere along the chain, some people roast the beans, and others fabricate bags for carrying them. Think of other participating cooperators: insurers and inspectors, wholesalers and retailers. . . . However great their distance from Milan, innumerable people play their roles in cooperation, and no less so than the surly or obliging waiter in the café.[7]

Information, not centralized planning, is the thread that ties the individual efforts together. The farmers growing coffee beans estimate the volume buyers will want to purchase. Coffee manufacturers and

---

6. *See, e.g.*, Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. Rev. 633 (2000). In her interesting essay, Bartow complains that "[d]ocilely, we allow corporate entities to monitor our online efforts to educate and inform ourselves, support each other, and purchase goods and services for our families and ourselves. This data is then used to more efficiently separate us from our money." *Id.* at 636. Bartow's exclusive focus on the negative aspects of business data overlooks the fact that more efficient provision of goods and services lowers costs.

7. Charles E. Lindblom, The Market System: What It Is, How It Works, and What to Make of It 36–37 (2001).

wholesalers coordinate their efforts through communication with each other and with those who transport the beans from the fields. Wholesalers estimate the demand from retailers, who in turn estimate the demand of consumers, like the café in Milan, which estimates the demand from its customers. In general, market economies depend on a flow of information. The more accurate and less costly the information, the more efficient the economy. It is more efficient in the sense that we spend less time and effort to achieve the same results; the savings can be used for other purposes—education, relief of poverty, improved health insurance, and so on.

I focus on the flow of information from individual consumers to businesses. This is an area in which technology has greatly reduced privacy; the immediate point, however, is not the privacy loss, but the efficiency gain. Technology has improved efficiency by making it cost-effective to collect, analyze, and use vast amounts of data about consumers' preferences. The increase in efficiency comes from the increased ability to determine what products and services consumers want, and from the increased ability to target advertising.[8] Targeted advertising is the process of matching advertising to recipients in ways that maximize the likelihood that recipients will purchase in response.[9] When "two marketers are competing for the same customer's business, all other things being equal, the marketer with the greatest scope of information about that particular customer [and hence the more targeted advertising] . . . will be the more efficient competitor."[10] Targeting does not merely benefit businesses; it also benefits consumers by reducing the amount of irrelevant information that bombards them.

One way in which technology has greatly increased the ability of businesses to target advertising is by increasing the ability to aggregate information. Aggregation is perhaps the most serious technol-

8. These observations about advertising and efficiency assume that advertising conveys information. Some may rightly object that advertising is often highly manipulative because it is designed to *create* perceived needs for products and services of doubtful value. *See* HERBERT MARCUSE, ONE DIMENSIONAL MAN: STUDIES IN THE IDEOLOGY OF ADVANCED INDUSTRIAL SOCIETIES 5 (1968) (emphasizing that advertising manipulates consumers by creating needs). *See also* LINDBLOM, *supra* note 7, at 188–89 (emphasizing the same point). It is nonetheless true that advertising informs consumers that certain products are available from particular sources.

9. *See* http://dbay.ndsu.edu/~dollarbay/howtoplay/howto.definitions.php.

10. DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE: BUILDING RELATIONSHIPS ONE CUSTOMER AT A TIME 138 (1st Currency paperback ed. 1996). Originally published in 1993, *The One to One Future* is one of the classics of direct marketing literature. Published before the explosion of e-commerce on the Internet, its focus on fax machines and computerized databases make it a fascinating read. Substitute "Internet" for "fax machine" and one would think one was reading a contemporary commentary on the Internet.

ogy-created threat to privacy. Information is aggregated from two sources—private and public. *In re DoubleClick Inc. Privacy Litigation*[11] illustrates the former. The court noted that DoubleClick "compiles user profiles . . . from over 11,000 web sites for which and on which it provides targeted banner advertising."[12] DoubleClick used cookies to collect "e-mail addresses, home and businesses addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect."[13] The court observed that "[o]nce DoubleClick collects information from the cookies on users' hard drives, it aggregates and compiles the information to build demographic profiles of users. Plaintiffs allege that DoubleClick has more than 100 million user profiles in its database."[14]

Public records are also a rich source for constructing profiles. They "contain a great deal of information about individuals, often very sensitive information."[15] The information includes the following: Social security numbers; financial account numbers; family law files may contain information about children as well as allegations of wrongdoing; insurance litigation files may contain details of medical conditions and other highly personal information (about the effect of the condition, preexisting conditions, or information relevant to supporting an allegation that the claims are exaggerated); sexual harassment files may contain allegations about lifestyle and sexual history; and criminal files may contain very sensitive personal information.[16] Businesses like Classified^3.com[17] and Accurint[18] aggregate such information to produce remarkably detailed descriptions of people's lives. Classified^3.com claims it

> has the capabilities to search, gather and report detailed intelligence on almost anyone or anything on the planet. With access to more than 425 billion records in 100+ countries, cutting edge access to

11. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

12. *Id.* at 502.

13. *Id.* at 503.

14. *Id.* at 505.

15. Beth Givens, *Public Records on the Internet: The Privacy Dilemma* (Apr. 19, 2002), http://www.privacyrights.org/ar/onlinepubrecs.htm.

16. *Id.*

17. See Classified^3.com: Global Intelligence Agency, Home Page, *at* http://www.classified3.com (last visited Mar. 28, 2005).

18. Accurint's sales pitch states: "Use the world's most comprehensive and accurate locate and research tool to achieve better results at a lower cost. Find people, businesses and their assets. Obtain deep background information. Uncover bankruptcies and criminal histories. Accurint makes your search easy by providing instant access to billions of linked records." *See* Accurint Home Page, *at* http://www.accurint.com (last visited Feb. 9, 2005).

updated databases, and the advantage of having trained experts performing your research, Classified[3].com has the tools and expertise to make intelligence gathering easier than ever before.[19]

B. *Two Regulatory Approaches*

Protecting privacy means constricting the flow of information that is the lifeblood of market efficiency.[20] There are two regulatory approaches to finding the appropriate tradeoff between privacy and efficiency: Top-down and bottom-up regulation. "Top-down" regulation imposes central planning through legislation and court decisions. It regulates commerce directly by defining what, when, how, and/or with whom market participants may buy and sell. "Bottom-up" ordering occurs via property rights and non-legal norms, which define a general framework within which market participants—not central planners—decide what, when, how, and with whom they buy and sell.[21] The difference between the two approaches is a matter of degree. The more an ordering leaves decisions in the hands of market participants, the more bottom-up it is; the more it takes decisions out of market hands, the more top-down.

C. *Bottom-Up Planning Is More Efficient, Other Things Being Equal*

Other things being equal, letting market participants decide what, when, and with whom they buy and sell is more efficient than taking

19. *See* Classified[3].com, *supra* note 17.

20. It is clear that restricting the flow of data tends to reduce efficiency. *See* Michael A. Turner, *The Impact of Data Restrictions on Consumer Distance Shopping*, http://www.privacyalliance.org/resources/turner.pdf (last visited Feb. 8, 2005).

21. Professors Margaret Jane Radin and R. Polk Wagner have a narrower conception of bottom-up regulation. They explain that the terms "top-down" and "bottom-up" refer to "Hayek's stylized distinction between bottom-up and top-down ordering . . . . Cyberlibertarians identify Hayek's top-down central planning with state-backed law and his bottom-up private ordering with regimes of non-legal customary norms." Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1297 (1998). Cyberlibertarians certainly did use "bottom-up" in this fashion. This conception of bottom-up ordering is not particularly useful. The reason is that, as Julie Cohen emphasizes, "[m]arket ordering and government oversight are complementary, not mutually exclusive choices. Market ordering presupposes some ex ante distribution of entitlements." Julie E. Cohen, Lochner *in Cyberspace: The New Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462, 492 (1998). *See also* Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1259 (1998) (noting the need for an initial distribution of entitlements). In general, property rights play an essential role in placing market decisions in the hands of market participants. Not only do they define who is entitled to exchange what, but also enable sellers to control with whom they share business resources and to whom they will sell, as well as where, when, and how they do so. The distinction between bottom-up and top-down ordering is a question of the *degree* of government control.

these decisions out of their hands.[22] There are two ways in which "other things" may not be "equal." First, leaving decisions in the hands of market participants sometimes leads to inefficiency.[23] Leaving decisions about the extent of automobile generated air pollution in the hands of automobile manufacturers, for example, leads to the degradation of the environment, health problems, and other negative consequences that impose costs far exceeding what the manufacturers save by not investing in pollution control systems.[24] Privacy may involve similar inefficiencies. Consider, for example, the damage caused by the errors that inevitably occur as information is entered into databases and as it is used and analyzed. Errors can lead to serious consequences such as the denial of employment.[25] It may well be that businesses inefficiently underinvest in error prevention and detection; it is possible that an increased investment would reduce the damage by far more than the amount of the investment. The possible inefficiencies in ways businesses deal with personal data merit close attention.

My focus here, however, will be on the second reason for top-down regulation: Namely, that leaving decisions in the hands of market participants may fail to realize values that we, as a society, want realized. Laws prohibiting the exploitation of child labor are one example.[26] Even if they reduce efficiency, we would impose them nonetheless in order to protect children. Similarly, even at the expense of efficiency,

---

22. Arthur Okun summaries the efficiency claim:

> The case for efficiency of capitalism rests on the theory of the "invisible hand," which Adam Smith first set forth two centuries ago. Through the market, greed is harnessed to serve social purposes in an impersonal and seemingly automatic way. A competitive market transmits signals to producers that reflect the values of consumers. If the manufacture and distribution of a new product is profitable, the benefits it provides to buyers necessarily exceed the costs of production. And these costs in turn measure the value of the other outputs that are sacrificed by using labor and capital to make the new product. Thus, profitability channels resources into more productive uses and pulls them away from less productive ones. The producer has the incentive to make what consumers want and to make it in the least costly way. Nobody is asked to evaluate what is good for the system or for the society; if he merely pursues his own economic self-interest, he will automatically serve the social welfare.

ARTHUR M. OKUN, EQUALITY AND EFFICIENCY: THE BIG TRADEOFF 50 (1975).

23. *See, e.g.*, LINDBLOM, *supra* note 7, at 147–48.

24. *See generally* RICHARD C. PORTER, ECONOMICS AT THE WHEEL: THE COSTS OF CARS AND DRIVERS (1999).

25. *See* Givens, *supra* note 15 and accompanying text (discussing the adverse effects of negative information in public records).

26. Child Labor is regulated under the Fair Labor Standards Act of 1938, 29 U.S.C. §§ 201–219 (2000). *See* U.S. Department of Labor, Youth and Labor, *at* http://www.dol.gov/dol/topic/youthlabor/index.htm (last visited Feb. 8, 2005). The Department of Labor emphasizes that the purpose of regulating child labor is to protect the health and safety of children and to ensure that they have sufficient educational opportunities. Economic efficiency is not the point.

top-down regulation is desirable to ensure that society provides the degree of privacy necessary to allow individuals to enjoy sufficient freedom for adequate self-realization. We should, however, deploy top-down regulation only where it is really required; otherwise we unnecessarily sacrifice the efficiency that bottom-up regulation promotes. To see what type of regulation is needed where, we need to understand the threats technology creates, and to understand the threats, we need to understand the relation between privacy, freedom, and the self.

I am not claiming that these relations are the *only* reason (apart from restraining government) to protect privacy. It may well be, for example, that some control over what others know about us is essential to our psychological well-being in ways that are independent from the considerations that follow about freedom and the self. These considerations are just one central and important reason to protect privacy.

III. PRIVACY, FREEDOM, AND THE SELF

William James captures the relevant concept of the self. "I am," James writes,

> often confronted by the necessity of standing by one of my empirical selves and relinquishing the rest. Not that I would not, if I could, be both handsome and fat and well dressed, and a great athlete, and make a million a year, be a wit, a *bon vivant*, and a lady killer, as well as a philosopher, and a philanthropist, statesman, warrior, and African explorer, as well as a 'tone poet' and saint. But the thing is simply impossible. The millionaire's work would run counter to the saint's; the *bon vivant* and the philanthropist would trip each other; the philosopher and the lady killer could not well keep house in the same tenement of clay. Such characters may at the outset of life be alike *possible* to a man. But to make anyone of them actual, the rest must be more or less suppressed. So the seeker of his truest, strongest, deepest self must review the list carefully, and pick out the one on which to stake his salvation. All other selves thereupon become unreal, but the fortunes of this self are real, its failures are real failures, its triumphs real triumphs, carrying shame and gladness with them.[27]

You make yourself the person you are by what you "stand by," by the commitments you strive to realize. This conception of personhood underlies political philosophy from John Stuart Mill[28] to John Rawls[29]

27. WILLIAM JAMES, 1 THE PRINCIPLES OF PSYCHOLOGY 309–10 (1980).

28. *See generally* JOHN STUART MILL, ON LIBERTY (David Bromwich & George Kateb eds., Yale University Press 2003) (1859).

and Joseph Raz,[30] and I assume that it is uncontroversial that we are typically as James describes.[31]

A. Complexity and Contradiction

The Jamesian conception requires one emendation. James exaggerates when he suggests that "the seeker of his truest, strongest, deepest self must review the list carefully, and pick out the one on which to stake his salvation."[32] Our identities are composed of multiple roles: spouse, parent, professor, friend, applicant for insurance, heir to this or that religious tradition, product of southern Californian culture, and so on. In general,

> [w]e are none of us defined by membership in a single community or form of moral life. We are . . . heirs of many distinct, sometimes conflicting, intellectual and moral traditions. . . . The complexity and contradictions of our cultural inheritance give to our identities an aspect of complexity and even of plurality which is not accidental, but (if we may use such a term) essential to them. For us . . . the power to conceive of ourselves in different ways, to harbour dissonant projects and perspectives, to inform our thoughts and lives with divergent categories and concepts, is integral to our identity as reflective beings.[33]

In general, we spread out along a continuum: Harmonious selves with little conflict occupy one extreme; tortured, conflict-ridden selves, the other. Most of us most likely occupy a position somewhere in the middle.

B. Social Roles

An essential step in understanding the link between privacy and the self is appreciating the function in the development of the self of what I will call "social roles."[34] The basic point: We adopt the plans and projects we "stand by" from roles recognized and understood *by the society in which we live.* We do not, as a rule at least, invent a role or type of activity that society has not already recognized in some form

---

29. *See generally* JOHN RAWLS, POLITICAL LIBERALISM (1993); JOHN RAWLS, A THEORY OF JUSTICE (1971).

30. *See generally* JOSEPH RAZ, THE MORALITY OF FREEDOM (1986).

31. One important philosophical task is showing that what is typically true is also necessarily true, that our Jamesian nature is inescapable. On the issue of necessary truth, see RICHARD WARNER, FREEDOM, ENJOYMENT, AND HAPPINESS (1987).

32. JAMES, *supra* note 27, at 310.

33. John Gray, *The Politics of Cultural Diversity*, *in* POST-LIBERALISM: STUDIES IN POLITICAL THOUGHT 253, 262–63 (1993).

34. RAZ, *supra* note 30, at 311 (emphasizing the importance of social roles—what he calls "social forms"—to the development of the self).

or other. We choose our roles from those already recognized and understood by the society in which we live. These are the roles I label "social roles." Being a bird watcher is an example. You could not be a bird watcher in a society that does not recognize that role. Trying to imagine the opposite shows why—and in what sense—the claim is true.

Imagine a primitive tribe whose sole use for animals is to hunt and eat them; you are the lone anomaly who spends hours tracking down birds merely to look at them.[35] Although you watch birds, you are not a bird watcher in the sense that a member of the Audubon Society is. The Audubon member's bird-watching behavior fits a recognized social pattern. Our society recognizes that people enjoy bird-watching, and the bird watcher understands himself or herself, and is understood by others, as someone who enjoys watching birds. To call yourself a bird-watcher is not just to say you watch birds; it is also to ascribe to yourself a recognized role. In the primitive tribe, your anomalous bird gazing does not fit any recognized pattern of behavior; hence, you lack reference to such a pattern as a way of understanding yourself and explaining yourself to others.

We define ourselves in large part by the social roles we play, roles provided by the society—or perhaps better, the societies—in which we live. Those roles define the possibilities open to us. You cannot, for example, be a lawyer except in a society governed by law; practice medicine unless the society you are in recognizes the practice; be a professional race car driver except in a community that recognizes the sport.[36] The point extends even to being a parent, child, lover, or spouse. Being a parent is a relationship that takes on different meanings and definitions depending on the society in which the relationship is realized. Our conception of these roles is formed in part by ideals, values, and expectations shared by those in the society in which we were raised, educated, and in which we live.

C. Social Roles and Privacy

Privacy is essential if a self, defined by multiple roles, is to fulfill all those roles successfully. The reason lies in the fact that social roles not only provide a framework for understanding and explanation, but also for evaluation. Social roles typically incorporate evaluative standards. Standards of professional conduct for lawyers are one such ex-

35. The example is adapted from *id.* at 310.

36. *Id.*

ample; standards for teachers are another.[37] We also—and this is the crucial point for privacy—evaluate the ways in which we *combine* roles in a single self. In our society, for example, bird-watching is regarded as an avocation. If one was a monomaniacal bird watcher devoting virtually every waking hour to bird-watching to the exclusion of other pursuits, one would provoke questions. We would want to know why that person would build a whole life around watching birds. It would be eccentric at best; at worst, an unhealthy obsession that wastes one's life.

Most would likely concur with this assessment. Other examples, however, are much more controversial. Some think that it is wrong to combine being gay or lesbian with being a parent; others sharply disagree. Exploring sexuality in sex clubs is, in the eyes of many, unacceptable in a candidate for political office.[38] Many parents would have qualms about an exemplary elementary school teacher who at night drinks himself or herself into oblivion, or indulges a passion for pornography. An associate in a traditional, conservative law firm might face strong disapproval and even termination of employment if the senior partners discovered the associate's anonymous calls for radical reform of the legal profession. A thirty-five-year-old man who has lived a law-abiding and exemplary life as a pediatrician, husband, and parent may face family turmoil and employment problems when the hospital in which he works and his family learn of his arrest for possessing an ounce of marijuana at nineteen and his violation of sodomy laws in his one homosexual relationship at twenty-two. In general, the expectations we create in others when we are in one role may be deeply disappointed when they find us in what they regard as an incompatible role. The consequences can range from disapproval and dislike to loss of employment and ostracization. Indeed, it is possible that

> our society will see a growing number of individuals who are disenfranchised for life. Large numbers will not be able to find employment because of negative information . . .—whether true or not—from years gone by. Or they will be relegated to lower-paying jobs in the service industries, unable to bring their true abilities into the employment marketplace. We [www.privacyrights.org] have been contacted by many such individuals in our ten-year history. I believe, sadly, we will be contacted by many more.[39]

---

37. *Id.*

38. *See, e.g.*, Sarah Hall, *Jeri Ryan Sex-Club Scandal* (June 22, 2004), *available at* http://movies.eonline.com/News/Items/0,1,14366,00.htm.

39. Givens, *supra* note 15.

We cannot rely on tolerance and reasoned discussion to protect us. Our disagreements are too sharp and fundamental and too resistant to rational resolution. As John Rawls notes,

> [L]ong historical experience suggests, and many plausible reflections confirm, that . . . reasoned and uncoerced agreement are not to be expected. . . . Our individual and associative points of view, intellectual affinities and affective attachments, are too diverse, especially in a free democratic society, to allow of lasting and reasoned agreement. Many conceptions of the world can plausibly be constructed from different standpoints. Diversity naturally arises from our limited powers and distinct perspectives; it is unrealistic to suppose that all our differences are rooted solely in ignorance and perversity, or else in the rivalries that result from scarcity. [The appropriate view of social organization] takes deep and unresolvable differences on matters of fundamental significance as a permanent condition of human life.[40]

Privacy—in the sense of the ability to control what others do and do not know about us—serves as an essential sanctuary. It allows the exemplary elementary school teacher to combine that activity with whatever private passions the teacher wishes to indulge. When sodomy laws were still enforced, privacy allowed gay men to conduct their sexual lives as they wished.

D. The Technology Threat

Technology threatens to destroy the ability of privacy to play its sanctuary-providing role. A comparison with the past reveals the present danger. Fifty years ago it was much easier for privacy to play its sanctuary-providing role. The reason was that we could, through our own efforts, ensure that the zone of privacy we thought we *ought to* have, more or less coincided with the zone of privacy we *in fact* had.[41] Suppose, for example, that you and I wished to communicate without others eavesdropping. We could do so by finding a place to converse out of earshot of others. Even if we suspected sophisticated surveillance, we could defeat such attempts much more easily a half a century ago than we can now. In short, we could—much more so than today—ensure that what we thought ought to be private would in fact be private. This is what technology has changed. It has greatly curtailed our ability to ensure that what we think ought to be private really is concealed from unwanted eyes.

---

40. John Rawls, *Kantian Constructivism in Moral Theory*, 77 J. PHIL. 515, 542 (1980).

41. The security expert Bruce Schneier emphasizes this point. *See* BRUCE SCHNEIER, SECRETS AND LIES 30 (2000).

E. Irony and Regulation

There is an irony here worth noting. Consider that the technological threats to privacy and the self are a product of developments in democratic nation-states and their market economies.[42] Technological innovation has flourished in this environment, producing, among other things, the surveillance technologies that now threaten privacy. The irony is that we owe the freedom to construct a multifaceted self in large part to the same sources that have produced the threat—democratic institutions and the market economy. As analysts as diverse as the nineteenth century sociologist Georg Simmel and the twentieth century economist Fredrick Hayek have emphasized, by replacing feudal forms of organization and production and by promoting mobility and communication,

> the development of capitalism creates more complex forms of individuality, since individuals can pursue a wider range of unconnected interests and belong to multiple associations without being defined (or swallowed up) by anyone. Those associations create linkages across borders, which means, for example, that two chamber music enthusiasts, one in Peoria, the other in Pretoria, may have more in common with one another than each has with his more immediate neighbors. Under such circumstances individual identity arises from the set of one's interests and associations, a set different, in theory at least, for each individual and valued precisely because it is voluntarily chosen.[43]

If we are to retain our freedom, we need to regain the control that technology has taken from us. To preserve the efficient functioning of the market—the very market that has played a central role in giving us our freedom—we should use top-down regulation sparingly in our efforts to regain control over our personal information. We should opt for bottom-up regulation whenever doing so is consistent with the value we place on privacy.

IV. THE "CONSENT REQUIREMENT"

An attractive, bottom-up way to regulate privacy is to impose a "consent requirement." That is, we pass a statute that requires businesses to obtain our consent before they collect certain types of information about us. The more types of information businesses cannot

42. Market economies and democratic institutions foster technological innovation by providing the freedom to experiment and rewarding successful entrepreneurs. *See generally* JERRY Z. MULLER, THE MIND AND THE MARKET: CAPITALISM IN WESTERN THOUGHT 400 (2002).

43. For a discussion of the theories of the scholars Simmel and Hayek, see *id.* at 242–52, 347–87.

collect without consent, the greater privacy protection the statute provides.[44]

The consent requirement is a "bottom-up" approach because it leaves the decision about when to disclose information in the hands of individual consumers. If businesses desire information consumers loathe to disclose, businesses can encourage disclosure by offering discounts on purchases or other forms of compensation. The resulting pattern of interactions among consumers and businesses determines the tradeoff between privacy and efficiency. The absence of inflexible, top-down planning allows innovation and experimentation, and history shows that, in times of technological change, economies flourish best when regulation does not stifle inventiveness.[45]

The consent requirement appears to solve with one stroke the privacy problem technology creates. The problem is that technology greatly reduces our ability to control what others know about us.[46] The consent requirement appears to return, by law, the control that technology has stolen. The requirement ensures a zone of privacy, which others may not—other things being equal—invade without our explicit, prior consent. In effect, this is to treat privacy like property. The consent requirement gives us a right to exclude others from personal information, but the right is not inalienable. We can, if we so wish, grant third parties a license to use our personal information.

There are two types of objections to the consent requirement. Some object because it treats privacy like property; others object that the requirement fails to adequately protect privacy. This section considers the first objection. The next two sections discuss the second objection.

A. The Inalienability Objection

Some contend that privacy—or, at least certain aspects of it—should be inalienable. They see treating privacy as alienable as inconsistent with the role privacy plays in protecting our freedom to develop our identities.[47]

One difficulty is to identify the relevant aspects and explain why we should not have the right to disclose them. Imagine I write an autobi-

44. I will bypass the question of what types of information should be included; my focus is on the requirement of consent itself, not on the types of information involved.

45. *See generally* Benn Steil et al., *Introduction and Overview*, *in* TECHNOLOGICAL INNOVATION & ECONOMIC PERFORMANCE 3 (Benn Steil et al. eds., 2002).

46. *See supra* Part II.A.

47. *See generally* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 136 (1988).

ography that reveals the most intimate aspects of my marriage in great detail. Why should I not have the right to sell it to a publisher? If the answer is that the intimate details of my marriage do not qualify as an inalienable aspect of privacy, then what does? A second difficulty is that we should be quite uncomfortable with the idea that the state should define what we can and cannot disclose about ourselves. To do so is, in part, to define the sort of relations we are allowed to have with others, and constraining those relations is a substantial interference with our freedom of association. The better course is to leave decisions about what to disclose up to individuals.

B. The Commodification Objection

Some object that treating privacy like property "commodifies" privacy. An item is commodified to the extent that we are willing to exchange it for a price in the market.[48] Commodification is objectionable when it leads us to value improperly the items we exchange. Imagine that both the Mona Lisa and chewing gum discarded by Britney Spears are for sale on eBay; suppose the chewing gum sells for a higher price. If we conclude that the Mona Lisa has less value—not market value, but cultural and aesthetic value—than Britney's gum, we improperly value the items in question. Critics of the market—including Adam Smith and John Maynard Keynes—have complained that commodification does indeed lead us to value items improperly.[49] Keynes hoped that increasing affluence would cure the ills he saw in a market economy:

> When the accumulation of wealth is no longer of high social importance, there will be great changes in the code of morals. We shall be able to rid ourselves of many pseudo-moral principles which have hag-ridden us for two hundred years, by which we have exalted some of the most distasteful of human qualities into the position of the highest virtues. We shall be able to afford to dare to assess the money motive at its true value. The love of money as a possession—as distinguished from the love of money as a means to the enjoyments and realities of life—will be recognised for what it is, a somewhat disgusting morbidity, one of those semicriminal, semi-pathological propensities which one hands over with a shudder to the specialists in mental disease.[50]

---

48. *See, e.g.*, Margaret Jane Radin, *Compensation and Commensurability*, 43 DUKE L.J. 56, 57 (1993); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849, 1855 (1987).

49. *See* MULLER, *supra* note 42, at 317–22 (offering an illuminating historical discussion of this theme, including commentaries on Smith and Keynes).

50. *Id.* at 319.

The "love of money as a possession"[51] leads many people to assess the true value of an item in light of its exchange value in the market, and it would be foolish to ignore this fact, which critics have warned of since the rise of capitalism.[52]

There are, however, two reasons not to be particularly concerned about improperly valuing privacy as a result of commodification. First, we routinely exchange highly personal aspects of ourselves for money without ceasing to value them properly. Like every other employed educator, I exchange my intellectual abilities for money, yet—and I doubt I am atypical—I still see significant non-market value in intellectual activity. Indeed, I pursue intellectual projects primarily because of their non-market rewards. It is an unavoidable aspect of a market economy that we all have to strike some balance between the freedom to pursue whatever ends we regard as worthwhile and the need to make money. Merely "to survive in market one must make a particular kind of contribution—a marketable one. No other alternative is open; no choice. Most adults, then, in a market system work or perish."[53] Each of us decides how we want to use our freedom: more work, more money, less leisure; or, less work, less money, more leisure. The consent requirement provides a similar choice in the case of privacy.

Second, treating privacy as property can *promote* valuing privacy properly. Indeed, the *point* of treating privacy as property is not so much to make it exchangeable as to allow us to protect it, to define a zone of privacy that businesses cannot invade without consent. Treating privacy as property highlights its proper value.

None of this is intended to deny that commodification is worrisome. My contention is that, in the case of the consent requirement, it is not a sufficiently pressing worry to deter us from imposing that requirement. The critical question about the consent requirement is, instead, whether it can actually succeed in adequately protecting privacy? To answer, we need to identify the threats that reduce our ability to control what others know about us.

---

51. *Id.*; *see also* JOHN MAYNARD KEYNES, *The General Theory of Employment, Interest, and Money*, *in* THE COLLECTED WRITINGS OF JOHN MAYNARD KEYNES 376 (Donald Moggridge ed., 1973).

52. *See* MULLER, *supra* note 42, at 319.

53. LINDBLOM, *supra* note 7, at 187 (noting that "[t]he classical economists applauded the market system because it coerced the masses to work, doing so by the 'silent, unremitted pressure' of hunger, as one of them, William Townsend, put it").

V. THE THREATS

The threats divide into two categories: Lack of consent and technological inadequacies.

A. Lack of Consent

Businesses deny us control over what others know about us when they collect information about us without our consent. Lack of consent is common on the Internet. When one visits a website, the visit typically triggers the deposit on a computer hard drive of programs, called "cookies," that garner information and return it to advertisers.[54] It is arguable that one gives implied consent to the use of cookies since it is possible to change a computer's Internet browser settings to prevent their use. However, many sites will refuse access to Internet users who block cookies, so the implied consent you give by not blocking cookies does not necessarily represent a truly meaningful choice among viable options. In addition, consent to cookies is often less than fully informed; many are unaware of just how much information the cookies collect and who receives that information.[55]

Even when websites do attempt to obtain consent to collect and use information, the "consent" they obtain is often defective. Many websites offer a privacy policy that informs users about what information the business collects and what it does with that information.[56] Unfortunately, policies are often written in a confusing and deceptive fashion to suggest that the business offers more privacy protection than it really does.[57] Moreover, the mechanisms by which consumers indicate consent often defeat, rather than promote, the attempt to give free and informed consent. Consent is often solicited through the request to check a box if one agrees to let the business collect information and use it in certain ways. The box is often checked by default; this means one must notice the box and uncheck it to avoid giving "consent." In many cases, if one returns to the page to correct erroneously entered information or for some other reason, the box is again checked by default, one must notice that and uncheck it again.

---

54. *See* Definitions of Cookie on the Web, *at* http://www.google.com/search?hl=en&q=define%3A+cookie (last visited Feb. 8, 2005).

55. *See* Wayne Porter, *Internet Cookies–Spyware or Neutral Technology*, *available at* http://www.spywareguide.com/articles/internet_cookies_spyware_or_ne_57.html (last visited Mar. 28, 2005).

56. *See* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1099 (1999).

57. *Id.*

Even when a consumer has given free and informed consent to the disclosure of information, data aggregation may extend the effects of that disclosure in ways the consumer did not contemplate and to which he or she would not have given consent. As Professor Daniel Solove explains,

> [a]n individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information. It is the totality of information about a person and how it is used that poses the greatest threat to privacy. . . . From the standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision. The potential future uses of that information are too vast and unknown to enable individuals to make the appropriate valuation.[58]

Suppose, for example, that Jones, whose best friend is struggling with depression, has spent considerable time on websites and in Internet discussion groups devoted to clinical depression. The sites and discussion groups keep a record of these activities. Jones is aware of the data collection activities and, by his use of the sites and groups, gives implied consent to the data collection. Unfortunately, a summary of the recorded information appears in a background check, run by a potential employer, who denies Jones a job on this basis. Jones would never have consented to the potential employer's possession and use of the information. The Jones example is an instance of private data collection. In the case of public records, we generally do not even have the option of withholding consent to the initial disclosure of information. Indeed, "in the majority of situations, providing personal information to government agencies and courts is *mandatory*. Individuals have no choice in the matter."[59]

B. Inadequate Technology

Inadequate technology threatens privacy in three ways. The first way in which inadequate technology threatens privacy is improper "anonymization." Information is anonymized when all references have been removed that would allow one to identify the individual the information describes. Anonymization provides an important degree of control over what others know about us; a guarantee of anonymization allows you to be sure that the information you release will not be used to construct a picture of *you*. The protection anonymization pro-

58. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1452 (2001).

59. Givens, *supra* note 15.

vides can be illusory, however. Anonymization, if not properly performed, leaves a trail that can be traced back to personally identifying information.[60] Further, even properly anonymized data may be used to identify individuals. I am, for example, the only person in the category defined by the following two factors: (1) Has a Ph.D. in philosophy and (2) currently teaches at Chicago-Kent College of Law. Any information pertaining to the people in this category can only be about me. This problem arises in anonymizing health care data. There may, for example, be only one person treated in way *X* for disease *Y* in hospital *Z* in a given time period.[61]

The second way in which technology threatens privacy is inadequate error prevention. Errors in non-anonymized, personally identifying information decrease our control over what others know—or, better—*think* they know about us. Errors transform information we consented to disclose into a false and misleading picture, which we have not consented to make public.[62] The more inadequate error prevention and detection, the more control we lose.

Finally, "[s]ecurity and privacy are inextricably linked. The protection of information depends in large part on the existence of security measures to protect that information."[63] Unfortunately, security on many networks is quite poor.[64] The weaker security, the more unauthorized access to information; the more unwanted eyes obtain unauthorized access, the more information is distributed beyond the bounds of our consent and expectations.

VI. LIMITS OF THE CONSENT REQUIREMENT

To what extent does the consent requirement adequately meet the threats identified in the previous part? It fails to adequately address the threats posed by inadequate technology and by aggregation. It does adequately meet the problems posed by lack of consent in non-aggregation cases. The latter point is important because it shows that

60. *See, e.g.*, Richard Clayton et al., *Real World Patterns of Failure in Anonymity Systems* (2001), http://www.cl.cam.ac.uk/~rnc1/Patterns_of_Failure.pdf.

61. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 509 (1995) (noting the ease with which one can link information to specific individuals).

62. *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21st CENTURY 25–31 (2001).

63. Health Insurance Portability and Accountability Act, 45 C.F.R. pts. 160, 162, 164 (2003).

64. As security expert Bruce Schneier notes, "[t]oday there are no real consequences for having bad security. In fact, the market place rewards bad security." Bruce Schneier, Remarks at University of California, Berkeley Workshop on Economics and Information Security (May 16–17, 2002).

we only need top-down regulation to respond to the technology and aggregation threats.

A. Lack of Consent in Non-Aggregation Cases

The consent requirement can require that websites contain easily understandable, unambiguous privacy policies and can prohibit such practices as having check-boxes indicating consent obtained by default. The worry is whether privacy policies really produce adequately informed consent. Professor Solove raises this objection forcefully. He contends that a consumer "has difficulty assigning the proper value to personal information. It is difficult for the individual to adequately value specific pieces of information. . . . Because this value is linked to uncertain future uses, it is difficult, if not impossible, for an individual to adequately value her information."[65] Improper valuation means that consumers will sometimes make decisions about disclosing information that are the opposite of those that they would make if they were better informed. To the extent that consumers mistakenly impart information that they would withhold were they better informed, they impair their privacy. To the extent that they mistakenly withhold information that they would impart were they better informed, they impair market efficiency without any offsetting privacy gain. Is Solove correct? Is it difficult for consumers to value information because "this value is linked to uncertain future uses?"[66] The effects of data aggregation are a large part of Solove's basis for this claim, but we are considering aggregation separately. Let us ask whether, apart from aggregation, consumers have sufficient knowledge to determine whether to disclose information.

To take myself as an example, there are two instances in which I know enough to determine whether to disclose information even if I am uncertain about its potential uses. First, there is information so extremely personal that I will keep it absolutely private. I do not need to know proposed uses of this information to decide not to disclose it. Second, at the other extreme, there is information I will readily disclose no matter what use may be made of it (within broad limits; I will return to this qualification). Suppose, for example, I purchase toilet paper and a bottle of red wine at a grocery store, which retains a record that I purchased those items at a particular price on a particular day. I have no objection to the grocery store having that information. Indeed, I want the store to have it because it can use it to provide me

65. Solove, *supra* note 58, at 1452.
66. *Id.*

with products I want, run a more efficient store, and pass the efficiency savings on to me in the form of lower costs. I do not care what else they do with the information. As far as I am concerned, they can publish it on a billboard at the exit of the Lincoln Tunnel into New York City. There are limitations, of course. I would not want someone to compile a history of all of my purchases of wine during my lifetime and publish the information on a website asserting that my wine consumption was excessive.

I disclose information to the store against a background assumption that the uses that will be made of the information will stay within certain broad limits; however, I can be confident that the assumption is true. I am simply not important enough for anyone to go to the trouble of, for example, compiling a detailed picture of my purchases of wine. Of course, this could change. For example, insurance companies might become interested in patterns of alcohol consumption. In this regard, the invasion of my privacy arises from data aggregation. Adequately controlling data aggregation requires top-down regulation that restricts aggregation and the use of aggregated information; such regulation can prevent the invasions of privacy resulting from the aggregation of information that, bit by individual bit, poses no privacy threat.

In the intermediate cases between the two extremes, uncertainty about the use of information can be more of a concern. I may, for example, be reluctant to disclose my opinions and political allegiances to my local congressperson's re-election campaign unless I am assured that the information will not be passed on to the party's national committee.[67] However, uncertainty about this potential use does not mean I cannot make a rational decision about whether to disclose information. It just means I face a decision under uncertainty. If I do not want to run the risk of the unwanted use of my information, I simply do not disclose it. If businesses want me to disclose information that uncertainty makes me withhold, they simply have to eliminate the uncertainty by agreeing to limit their uses to those acceptable to me. They can do this, for example, through privacy policies.

Some will object that consumers do not take the time and trouble to read privacy policies,[68] and hence that it is simply naïve to think that

67. The consent requirement is consistent with granting a limited license. Professor Solove, however, assumes the opposite when he argues that "[s]ince the ownership model involves individuals relinquishing full title to the information, they have little idea how such information will be used when in the hands of others." *Id.*

68. *See* Kang, *supra* note 3, at 1248 (stating that "[f]or numerous reasons, such as transaction costs, individuals and information collectors do not generally negotiate and conclude express

detailed privacy policies are an effective method of communication. In response, we should distinguish between two cases. In the first, consumers do not read the privacy policy because they do not care sufficiently about what the business will do with the information they disclose—my lack of concern about my toilet paper and wine purchases illustrates the point. Here, the failure to read the privacy policy does not show that the consent requirement fails to protect privacy; it just shows that consumers do not pointlessly waste their time and effort.[69] In the second case, consumers who do not read the policy withhold information they would disclose if they read it and were reassured by the privacy protections offered. If businesses want the information consumers are not disclosing, they can find a way to present the relevant aspects of the privacy practices in a way that makes it more likely that consumers will become aware of them. If businesses fail to do so, then the cost of acquiring the information is not worth the cost of reaching out to the consumers. As a result, information remains private unless businesses find it sufficiently important to them to invest in encouraging its disclosure. Here the consent requirement works precisely as intended. The point is to allow consumers and businesses to strike a balance between privacy and efficiency.

To summarize, the consent requirement does appear to do just what we want: To strike an appropriate balance between privacy and efficiency. Two objections remain to this claim. First, the consent requirement cannot adequately address the technological threats to privacy. Second, it cannot adequately address the problems posed by aggregation.

B. Technical Requirements

It may appear that the consent requirement can adequately address the technological threats. Why not simply require that privacy policies include information about the adequacy of their anonymization, error prevention, and security provisions? The problem is that consumers could not properly evaluate this information. Anonymization, error

---

privacy contracts before engaging in each and every cyberspace transaction"). *See also* GARFINKEL, supra note 62; Sovern, *supra* note 56, at 1033.

69. Some may think that this attributes much too much rationality to consumers. The question of the degree of consumer rationality is an empirical one, of course. Methodologically, however, we are justified in assuming a fair degree of rationality. Democratic forms of political organization function properly only when citizens are sufficiently informed and sufficiently rational. The text pursues the question of how to legislate privacy protections in a properly functioning democracy. If the rationality of citizens as a whole falls below what a properly functioning democracy requires, then we have more serious problems than simply protecting privacy.

prevention, and security are technical and controversial topics; consumers generally lack the knowledge necessary to assess the adequacy of these procedures.

Protection here must come from market or legal incentives to adopt adequate measures. The current consensus is that market incentives fail to lead websites to adopt adequate measures.[70] Consequently, it appears that legal regulation is required. The Health Insurance Portability and Accountability Act (HIPAA) illustrates a detailed legislative approach to specifying technological requirements for protecting online medical information.[71] It is, however, far from clear that HIPAA's extensive requirements are appropriate in all cases of online data storage. The issue of appropriate technological requirements is a critical one that calls for detailed treatment.[72]

C. *Aggregation*

In the case of aggregation, the consent requirement fails to strike an adequate balance between privacy and efficiency. The essential difficulty is that data may be aggregated by a variety of third parties for a wide range of purposes over a number of years. Thus, when consumers divulge individual bits of information, it is virtually impossible for them to predict the ways in which that information will be aggregated and the uses to which the aggregated information will be put. Two results follow. First, concern for the unpredictable aggregation consequences will lead some consumers to withhold information that they would willingly disclose if they could predict its uses in future data aggregation. The result is that we forego the efficiency gain we would reap from disclosure without any offsetting privacy protection. Putting information about aggregation in privacy policies is not the solution. How is a business to cost-effectively obtain information about what any number of third-party aggregators are likely to do with information over a period of several years? Second, some consumers will fail to realize or misjudge the aggregation risk and disclose information they would withhold were they better informed. Here the efficiency gain from disclosure results from a failure properly to protect privacy. We see an extreme case of this failure in the case of public

70. *See infra* notes 71–75 and accompanying text.

71. *See* Health Insurance Portability and Accountability Act, 45 C.F.R. pts. 160, 162, 164 (2003).

72. *See* TECHNICAL STANDARDS AND COMMON CRITERIA TASK FORCE, NAT'L CYBER SECURITY P'SHIP, RECOMMENDATIONS REPORT app. D (Apr. 2004), *available at* http://www.cyberpartnership.org/TF4TechReport.pdf (rejecting a "one size fits all" approach to data protection and arguing that different standards are appropriate for different types of systems).

records when it is mandatory to divulge information to governmental agencies. The use of the information by private parties is completely *un*constrained by any consent requirement.

Excessive disclosure causes two types of harm—one private, one public. The private harm is a reduction in the freedom of specific individuals. Jones is denied employment as a result of depression-related Internet activities. Previous examples illustrate the point.[73] The thirty-five-year-old law-abiding, irreproachable pediatrician, husband, and parent faces family turmoil and employment problems when the hospital in which he works and his family learn of his arrest for marijuana at nineteen and his violation of sodomy laws at twenty-two. The exemplary elementary school teacher is exposed to public censure for indulging in his or her passion for alcohol or pornography. Fear of such exposure deters others from exploring roles that they would otherwise adopt.

The public harm is a harm to the social roles themselves. Aggregation can undermine the social roles that form frameworks in which we understand ourselves and through which we are understood by others. Businesses can use customer data in ways that alter this framework in objectionable ways. Ann Bartow argues that this is happening on the Internet with the "female" role.[74] She argues that businesses on the web are aggregating data to construct a profile of the typical female consumer, and she contends that "[d]atum by datum, woman by woman, the cyber-definition of 'female' is being constructed. . . . Derivative e-stereotypes, braced by a plenitude of personal information, will appear scientific and incontrovertible."[75] Bartow worries that both men and women will understand women through a business-constructed stereotype that distorts perceptions of women and limits their possibilities.[76] Whether or not Bartow is correct about this particular claim, it is certainly true that aggregation may create or reenforce pernicious stereotypes. Joel Reidenberg, for example, cites Acxiom, one of the largest information-selling companies, as an example of the use of data aggregation to engage in "invidious stereotyping."[77] He contends that "[t]he company offered 'a comprehensive ethnicity coding system' . . . [and] also proposed to clients coding that resembled Nazi Germany's Nuremberg laws."[78] We should certainly be concerned

73. *See supra* Part III.C.

74. Bartow, *supra* note 6, at 653–54.

75. *Id.*

76. *Id.* at 655–58.

77. Reidenberg, *supra* note 5, at 883.

78. *Id.* (quoting ACXIOM PRODUCT CATALOG 5 (1999)).

here that business-constructed stereotypes will distort our perceptions, create new prejudices, and feed existing ones.

Top-down regulation that restricts the use of aggregated information is required to prevent both the private and public harms aggregation causes. But it will prove difficult to find an appropriate approach. Aggregation plays an important role in improving economic efficiency by improving the ability of advertisers to target their message.[79] To protect privacy, we must sacrifice some efficiency, and the context in which we must do so is still one in which we are seeing rapid technological and economic innovation. Moreover, governments as a rule face considerable difficulty in centrally directing economies,[80] and, in this case, the task is made all the more difficult by the fact that we do not agree about the importance of various aspects of privacy.[81] What one person sees as an intolerable invasion, another finds entirely acceptable.

VII. CONCLUSION

To ensure the privacy necessary for the free realization of our identities, we must regain, through legal regulation, the control over personal information that we have lost through technological innovation. This requires a combination of bottom-up and top-down regulation. Top-down regulation requires that we arrive at a public consensus about the appropriate trade-off between efficiency and privacy. In a society marked by fundamental disagreement on moral and political matters, this will prove extraordinarily difficult. HIPAA's difficulties provide a glimpse of the problems to come.[82] Many complain that HIPAA is excessively burdensome on those subject to its requirements and that its privacy protection requirements block many legitimate and important uses of information.[83] Top-down privacy regulation presents a formidable challenge to democratic governments in massive nation-states characterized by widespread disagreement on fundamental moral and political matters. Meeting this challenge is a critically important task that urgently requires attention.

---

79. *See supra* Part II.A.

80. *Compare* MULLER, *supra* note 42 (offering an illuminating historical discussion of this fact), *with* LINDBLOM, *supra* note 7 (providing a non-historical defense).

81. *See generally* AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999) (discussing privacy controversies in a variety of contexts).

82. *See, e.g.*, Press Release, EurekAlert, Study: National Medical Privacy Law Makes Health Research Harder, More Expensive (Mar. 11, 2004), http://www.eurekalert.org/pub_releases/2004-03/uomh-snm031104.php.

83. *Id.*