Reasonable Expectations and the Erosion of Privacy

SHAUN B. SPENCER*

TABLE OF CONTENTS

* Climenko/Thayer Lecturer on Law, Harvard Law School. The author is grateful for the contributions of Nolan Bowie, Lawrence Friedman, Frederick Schauer, and Richard Sobel.

I. INTRODUCTION

This Article examines how the prevailing legal conception of privacy facilitates the erosion of privacy. The law generally measures privacy by reference to society's reasonable expectation of privacy. If we think of the universe of legally private matters as a sphere, the sphere will contract or (at least in theory) expand in accordance with changing social expectations. This expectation-driven conception of privacy in effect establishes a privacy marketplace, analogous in both a literal and metaphorical sense to a marketplace of ideas. In this marketplace, societal expectations of privacy fluctuate in response to changing social practices. For this reason, privacy is susceptible to encroachment at the hands of large institutional actors who can control this marketplace by affecting social practices.

This Article also identifies two essential elements of the erosion of privacy: embedded imprecision and internalization. We find imprecision embedded in the expectation-driven conception of privacy because of the inevitable gray area between what society clearly expects to be protected (that is, private), and what it clearly understands to be unprotected. Effective encroachment occurs through incremental incursions into this gray area of unsettled expectations. Moreover, individuals internalize each incremental step of encroachment, and thereby lose any sense that privacy was once possible in the encroached upon area. Because of this internalization, the expectation-driven privacy test cannot account for the cumulative effect of successive encroachments. Instead, its focus on the current level of expectations facilitates the incremental erosion of privacy.

Finally, this Article examines pervasive failures in the literal and metaphorical privacy marketplaces. Given the expectation-driven

vulnerability discussed above, preservation of privacy depends upon the individual's ability to resist encroachment into the private sphere. However, informational asymmetry, unequal bargaining power, and collective action problems conspire against them in both the economic and political marketplaces. Equally problematic are the inevitable unintended consequences that flow from any single encroachment. These phenomena stack the deck against those who would preserve the private sphere, and in favor of those who benefit from its erosion. Without some structural changes to restore the balance, the erosion of privacy may be a foregone conclusion.

Several caveats are appropriate at the outset. First, the term "privacy" means different things to different people. To clarify, this Article refers to what many call "information privacy," rather than the fundamental personal autonomy to which others have affixed the privacy label.[1] Alan Westin provided the classic definition of information privacy—the claim of individuals or groups to determine the conditions under which information about themselves is communicated to others.[2] Furthermore, the terms "public sector" and "private sector" risk introducing the notion of information privacy where it does not belong. This Article therefore

1. For discussions of information privacy, see Hyman Gross, *Privacy and Autonomy*, *in* NOMOS XIII: PRIVACY 169, 170 (J. Roland Pennock & John W. Chapman eds., 1971) (suggesting that privacy includes limits on what is known and who may know about one's personal affairs); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968) (stating that privacy is control over personal information about oneself); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000) [herinafter Froomkin, *Death of Privacy?*] (suggesting that privacy is "the ability to control the acquisition or release of information about oneself"). Others consider privacy a broader interest that includes informational privacy but encompasses far more. *See* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 91 (1992) (explaining that privacy is control over one's intimate decisions, including decisions about physical access to oneself, cognitive access to oneself, and intimate behaviors); A. Michael Froomkin, *Regulation and Computing and Information Technology: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 493 (1996) ("The constitutional right to privacy, such as it is, is frequently described as having three components: (1) a right to be left alone; (2) a right to autonomous choice regarding intimate matters; and (3) a right to autonomous choice regarding other personal matters."). The United States Supreme Court noted two senses of privacy in its own decisions. *See* Whalen v. Roe, 429 U.S. 589, 599–600 (1977) (noting that the Court had applied the "privacy" label to two different kinds of interests: (1) the "individual interest in avoiding disclosure of personal matters," and (2) the "interest in independence in making certain kinds of important decisions").

2. WESTIN, *supra* note 1, at 7.

avoids the terms wherever possible.[3]

This Article sometimes refers to a "sphere" of privacy that can expand or contract, while recognizing that one cannot formally quantify privacy in this fashion, because the term "privacy" lacks substance when divorced from a specific social context. Terms suggesting a measurable sphere of privacy that we can observe expanding or shrinking are intended only to convey the sense that matters once considered private can subsequently lose that status, and vice versa.

Finally, the purpose here is not to argue for or against specific practices.[4] Although many specific surveillance techniques or data collection practices are mentioned, this is primarily to illustrate their role in shaping expectations of privacy. Many of the practices mentioned below will find proponents and opponents, each with differing views on whether the practices invade a reasonable expectation of privacy. In fact, that split of opinion illustrates the imprecision embedded in the expectation-driven conception of privacy. Society will inevitably disagree about whether certain matters should be protected as private, and the incremental erosion of privacy occurs in this gray area of unsettled expectations.

II. THE EXPECTATION-DRIVEN CONCEPTION OF PRIVACY

The following Section discusses the role of social expectations in privacy law. Courts protect privacy mainly in the invasion of privacy torts and the Fourth Amendment search and seizure jurisprudence. In each area, courts define privacy by reference to society's prevailing understanding of what is a reasonable expectation of privacy. Because this conception of privacy tracks societal expectations, what is protected as private will vary in accordance with relevant social changes. For example, we generally expect that what we do and say in our homes

3. This linguistic contrast between public and private may trace its roots to the Greek and Roman distinctions between the public sphere (affairs of state) and the private sphere (affairs of domestic life). *See* JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE 3–4 (Thomas Burger trans., 1989) (contrasting the Greek political sphere of the polis, where citizens pursued freedom, honor and virtue, with the domestic sphere of the oikos, to which the labor of slaves and the service of women were consigned); *see also* HANNAH ARENDT, THE HUMAN CONDITION 38 (1958) (explaining that for the Greeks and Romans the private sphere connoted incompleteness and deprivation from the fulfillment of the public realm).

4. This Article proceeds on the assumption that, in many contexts, we ought to protect privacy against encroachment. Not everyone shares that assumption. *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393–99 (1978) (arguing that personal privacy is generally inefficient because it allows people to conceal "discreditable information" from others and to shift the cost of information acquisition to those who are not the least-cost avoiders). Enough commentators have come to the defense of privacy, however; this Article needs not join that debate.

remains private. If, however, people outside our homes were free to use devices that could sense our body heat through our walls or amplify sound waves bouncing against our windows, we might have a very different expectation of privacy in our homes.[5] The final Section in this Part examines how successive, incremental encroachments gradually erode societal expectations of privacy.

A. The Judicial Conception of Privacy

In the United States, judicial protection of privacy depends on whether an individual has a reasonable expectation that the information in question will remain private. Stated another way, the question is whether society recognizes the individual's claimed expectation of privacy as reasonable. Courts apply this reasonableness standard in the two broad areas of judicial privacy protection: the Fourth Amendment protection against unreasonable search and seizure, and the invasion of privacy torts.

1. Fourth Amendment Protection of Privacy

The Fourth Amendment's protection against unreasonable search and seizure incorporates societal expectations. In *Katz v. United States*,[6] the Supreme Court held that a person speaking on a public telephone had a justifiable expectation of privacy in his conversation, and that the government violated his expectation by wiretapping the telephone.[7] In an oft-cited concurrence, Justice Harlan explained that "reasonableness" entailed a two-part, expectation-driven test. First, the defendant must have an actual or subjective expectation of privacy. Second, the expectation must be "one that society is prepared to recognize as 'reasonable.'"[8]

---

5. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that law enforcement's use of a thermal imaging device to scan heat radiating from the defendant's home violated a reasonable expectation of privacy because technology was not in general public use); JARVIS INT'L INTELLIGENCE, INC., LASER MICROPHONE, *at* http://www.jarvisinternational.com/lasermic.htm (offering a "short range laser microphone that allows you to listen in on certain rooms and buildings from 150 yards away" by using lasers and receivers to amplify sound waves reflected against interior windows) (last visited Apr. 10, 2002).

6. 389 U.S. 347 (1967).

7. *Id.* at 353.

8. *Id.* at 361 (Harlan, J., concurring).

The Supreme Court elaborated on this expectation-driven conception of privacy in *O'Connor v. Ortega*.[9] A state hospital searched a doctor's desk drawers and personal file cabinets during a sexual harassment investigation. Investigators seized the doctor's personal letters and photographs.[10] The doctor filed a claim under 42 U.S.C. § 1983 against the hospital, and alleged violation of his Fourth Amendment rights.[11] Justice O'Connor wrote the plurality opinion, which held that the plaintiff presented sufficient evidence to survive summary judgment.[12] Discussing the Fourth Amendment "reasonable expectation" test, Justice O'Connor wrote:

> The operational realities of the workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.[13]

By positing actual official practices and procedures and operational realities of the workplace as limits on whether an expectation of privacy was reasonable, the Court recognized the role of social context in determining the scope of privacy. As Frederick Schauer observed, the Fourth Amendment test does not involve a fixed moral conception of what ought to be private, nor does it involve application of a formal legal test. Instead, courts "look at society as it is and . . . look at what society now thinks of as an area that is understood as a sanctuary."[14] *Ortega* shows that this social understanding "is itself inevitably dependent on changing social values and changing social expectations."[15]

The Court's reasoning in *Kyllo v. United States*[16] illustrates how changing technology can dictate the reasonable expectation of privacy. The Court held that law enforcement's warrantless use of a thermal imaging device to scan the defendant's house constituted a presumptively unreasonable search under the Fourth Amendment.[17] Scanning the defendant's home from across the street revealed that portions of the house were unusually hot, which was consistent with the use of heat

---

9. 480 U.S. 709 (1987).
10. *Id.* at 713.
11. *Id.* at 714.
12. *Id.* at 728–29.
13. *Id.* at 717.
14. Frederick Schauer, The Social Construction of Privacy, Discussion Draft 10 (Mar. 20, 2000) (unpublished manuscript, *at* http://www.ksg.harvard.edu/presspol/publications/pdfs/schauer1.PDF).
15. *See id.*
16. 533 U.S. 27 (2001).
17. *See id.* at 40.

lamps to grow marijuana.[18] Relying in part on the thermal imaging scan, the law enforcement officer obtained a search warrant and found that the defendant was, in fact, growing marijuana in his house.[19] The district court denied the defendant's motion to suppress the evidence found in his house, and the Ninth Circuit affirmed.[20]

Writing for the Court, Justice Scalia held that the use of the thermal imaging device constituted a presumptively unreasonable search within the meaning of the Fourth Amendment.[21] Scalia relied heavily on the fact that thermal imaging technology was "not in general public use."[22] He contrasted the thermal imaging device with widely used technologies such as airplane and helicopter flight, which have opened to public view areas of the "house and curtilage that once were private."[23] The logical conclusion of this reasoning is that, if thermal imaging technology finds its way into general public use, there may no longer be a reasonable expectation of privacy against such technology.[24]

Several United States Supreme Court decisions rest on the assumption that individuals cannot reasonably expect privacy in information they share voluntarily with others, like their bank[25] or their telephone

18. *Id.* at 30.

19. *Id.*

20. *Id.* A divided panel of the Ninth Circuit originally reversed the district court, *see* United States v. Kyllo, 140 F.3d 1249, 1250 (9th Cir. 1998), but on rehearing the still divided panel (after a change in composition) affirmed the district court, *see* United States v. Kyllo, 190 F.3d 1041, 1043 (9th Cir. 1999). The second panel reasoned that the defendant had no subjective expectation of privacy because he did not try to conceal the heat radiating from his home. 190 F.3d at 1046.

21. *Kyllo*, 533 U.S. at 40.

22. *See id.* at 34.

23. *See id.* at 34. For cases finding no unreasonable search based on warrantless aerial observations, see Florida v. Riley, 488 U.S. 445, 445 (1989) (observation of partially exposed residential greenhouse from helicopter at altitude of 400 feet); Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986) (aerial photography of industrial plant from between 1200 and 12,000 feet); California v. Ciraolo, 476 U.S. 207, 209 (1986) (surveillance of fenced-in backyard from helicopter at altitude of 1000 feet).

24. Some may consider it unlikely that such a highly specialized technology would become widely used. The same might have been said of global positioning system (GPS) technology when it was a purely military application, or of long distance laser microphones that amplify sound waves radiating against the inside of a window. Today, GPS technology has widespread public applications, and laser microphones are available for sale to the public. *See* Sabra Chartrand, *Patents: Tapping Global Positioning Technology to Send an S.O.S., Raise Drawbridges and Monitor Workouts*, N.Y. TIMES, Mar. 5, 2001, at C6; Jarvis Int'l Intelligence, Inc., *Laser Microphone*, *at* http://www.jarvisinternational.com/lasermic.htm (offering laser microphone for sale) (last visited Apr. 10, 2002).

25. United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that a bank

company.[26] Some state courts, however, have disagreed with this assumption. In *Burrows v. Superior Court*,[27] the California Supreme Court held that customers had a reasonable expectation that information shared with their bank would remain private. The court based its holding in part on testimony by bank officials and customers that customers expected their bank records to be used for internal bank purposes only.[28]

The *Burrows* court and the United States Supreme Court applied similar tests but reached different results concerning bank customers' expectations of privacy. This could reflect the California Supreme Court's greater emphasis on empirical evidence of expectations than the Supreme Court.[29] On the other hand, it may be appropriate for the expectation-driven conception of privacy to vary from state to state, presumably reflecting the different customs or norms in each state.

In this regard, the expectation-driven conception of privacy places the Supreme Court in a rather difficult position. On Fourth Amendment privacy questions, the Court must discern (or declare) the values and expectations of the national community. Any statement of the prevailing values and expectations will inevitably conflict with the values and expectations held in a minority of state and local communities. Perhaps the best way to deal with this problem is for the Supreme Court's privacy jurisprudence to serve merely as a baseline, recognizing only the

---

depositor had no reasonable expectation of privacy in bank records because depositor voluntarily conveyed checks and deposit slips to bank employees).

26. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that a telephone customer had no reasonable expectation of privacy in the numbers he dialed because the act of dialing exposes those numbers to the telephone company); *see also* United States v. White, 401 U.S. 745, 751–52 (1971) (finding no legitimate expectation that the defendant's accomplices would not report the defendant's statements to the police).

27. 529 P.2d 590 (Cal. 1974).

28. *See id.* at 593 ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."); *accord* Charnes v. DiGiacomo, 612 P.2d 1117, 1120–21 (Colo. 1980) (finding a reasonable expectation of privacy in bank records under the Colorado constitution); Commonwealth v. DeJohn, 403 A.2d 1283, 1291 (Pa. 1979) (finding a reasonable expectation of privacy in bank records under the Pennsylvania constitution).

29. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*," 42 DUKE L.J. 727, 737 (1993). Slobogin and Schumacher surveyed nearly two hundred individuals about their expectations of privacy. They asked citizens to rank fifty government searches in ascending order (one being least offensive and fifty being most offensive) of how much the searches intruded on their expectation of privacy. The results placed "perusing bank records" in thirty-eighth place, more intrusive than such searches as using a chauffeur or secretary as undercover agents, and slightly less intrusive than urinalysis. *Id.* at 737–38 tbl. 1, 742.

most broadly accepted privacy expectations. This approach would then allow states to build additional privacy protection upon that foundation, when local values and expectations dictate greater protection than the Supreme Court has established. Such a model depends on state supreme courts treating their constitutional protections against unreasonable search and seizure as truly independent from the federal provision, rather than interpreting their constitutional protections as duplicative of the federal protection.[30] Without this independent state protection, the Supreme Court's nationally applicable definition of what is private will serve as a ceiling rather than a floor, and will therefore diminish the expectation of privacy in those communities whose expectations differ from the majority. One alternative is for the Supreme Court to import a "contemporary community standards" test into its already involved interpretation of the Fourth Amendment's prohibition against unreasonable search and seizure.[31] Such an approach would either make the Court an arbiter of local norms in hundreds or even thousands of localities, or would relegate the Court to a minor role at best in Fourth Amendment jurisprudence.

2. Tort Law Protection of Privacy

The invasion of privacy tort traces its roots to Warren and Brandeis' seminal law review article.[32] In response to the late nineteenth century

30. *See, e.g.*, Lawrence Friedman, *The Constitutional Value of Dialogue and the New Judicial Federalism*, 28 HASTINGS CONST. L.Q. 93, 97 (2000) (arguing that the values of federalism and dialogue support independent state court interpretation of state constitutional provisions that parallel federal constitutional provisions).

31. *See, e.g.*, Miller v. California, 413 U.S. 15, 30 (1973):

> Under a National Constitution, fundamental First Amendment limitations on the powers of the States do not vary from community to community, but this does not mean that there are, or should or can be, fixed, uniform national standards of precisely what appeals to the "prurient interest" or is "patently offensive." These are essentially questions of fact, and our Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 States in a single formulation, even assuming the prerequisite consensus exists. When triers of fact are asked to decide whether "the average person, applying contemporary community standards" would consider certain materials "prurient," it would be unrealistic to require that the answer be based on some abstract formulation . . . . To require a State to structure obscenity proceedings around evidence of a *national* "community standard" would be an exercise in futility.

32. Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890), *reprinted in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 75, 76 (Ferdinand David Schoeman ed. 1984) [hereinafter PHILOSOPHICAL DIMENSIONS

version of tabloid journalism, Warren and Brandeis argued for explicit common law recognition of an invasion of privacy tort to "protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[33] Over the next seven decades, most states adopted some version of Warren and Brandies' privacy tort.[34] In 1960, Prosser's article reshaped the law of privacy. Prosser examined the common law privacy decisions in the wake of the Warren and Brandeis article, and argued that the decisions in fact dealt with invasions of four different interests.[35] Prosser's four interests are codified in the *Restatement (Second) of Torts* §§ 652B-652E.[36]

OF PRIVACY]. W. A. Parent suggests, as have many others, that Warren and Brandeis equated privacy with the right to be let alone. W. A. Parent, *Recent Work on the Concept of Privacy*, 20 AM. PHIL. Q. 341, 341 (1983). In fact, Warren and Brandeis described privacy as merely a part of a larger right, which they referred to alternately as the "right to be let alone," and the "more general right to the immunity of the person,—the right to one's personality." Warren & Brandeis, *supra*, at 75, 83.

33. Warren & Brandeis, *supra* note 32, at 82.

34. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960), *reprinted in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 32, at 106, 106.

35. Prosser, *supra* note 34, at 107.

36. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (1977). Omitted from this discussion are the torts for misappropriation of name or likeness and "false light" invasion of privacy, sections 652C and 652E, because neither implicates information privacy. As defined by the *Restatement (Second) of Torts*, the misappropriation tort is more accurately characterized as protecting an interest in property or reputation, rather than privacy. *See id.* § 652C, cmt. c (stating that to be liable for misappropriation, "the defendant must have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness . . . . Until the value of the name has in some way been appropriated, there is no tort."); *accord* Prosser, *supra* note 34, at 104, 116–17 (arguing that the appropriation tort protects a proprietary interest in the exclusive use of one's name or likeness). Some commentators argue that misappropriation implicates privacy interests, but those arguments rest on the assertion that misappropriation can effect the same type of dignitary harm as invasion of information privacy. *See, e.g.*, Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964), *reprinted in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 32, at 156, 175, 178–79 (arguing that appropriation of one's name or likeness has the same tendency to degrade and humiliate the victim as the publication of private facts, and that the privacy torts all protect human dignity and individuality); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34 (1967) (arguing that the gravamen of the appropriation tort is not harm to a proprietary interest, but harm to the victim's sensibility). Though I agree that misappropriation and invasions of information privacy can effect similar dignitary harm, they do so through quite different mechanisms. Misappropriation involves neither an intrusion into an area from which the victim reasonably expected to exclude others, nor a disclosure of information that the victim kept secret from others. *See* RESTATEMENT (SECOND) OF TORTS § 652C, cmt. d (1976).

> No one has the right to object merely because his name or his appearance is brought before the public, since neither is in any way a private matter and both are open to public observation. It is only when the publicity is given for the purpose of appropriating to the defendant's benefit the commercial or other values associated with the name or the likeness that the right of privacy is invaded.

The *Restatement (Second) of Torts* claims protect against intrusion and eavesdropping on one's "seclusion,"[37] and disclosure of one's private information.[38] These claims are based expressly on what constitutes reasonable behavior. Intrusions on seclusion are not actionable unless the intrusion "would be highly offensive to a reasonable person."[39] Conduct is highly offensive when a reasonable person "would strongly object" to the conduct.[40] Similarly, a disclosure of private facts is not actionable unless it "would be highly offensive to a reasonable person."[41] The *Restatement (Second) of Torts* commentary specifies that the disclosure is not actionably offensive unless the disclosure "is such that a reasonable person would feel justified in feeling seriously aggrieved by it."[42] The reasonableness test is to be judged "relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens."[43]

The reasonable person standard incorporates society's expectations of what matters should be protected as private. As Frederick Schauer observed, the harm that underlies the privacy torts is a socially constructed harm.[44] The law cares not about harm to the plaintiff's own sensibilities. Instead, the actionable harm is "a function of going beyond what most of the people in the society have come to expect, so if those expectations change, then so too does the conception of harm that is based upon them."[45] Similarly, Robert Post conceived of the reasonable person standard as "a genuine instantiation of community norms" which does not focus on injuries to specific individuals' personalities, but

---

Id. Indeed, torts such as battery and defamation inflict dignitary harms, but that does not render them privacy torts.

Similarly, the "false light" tort protects against harm to reputation and largely overlaps with defamation. *See* Prosser, *supra* note 34, at 114; *cf.* Bloustein, *supra*, at 156, 178–79 (agreeing that false light cases involve reputation, but arguing that the slur on reputation involves a slur on individual integrity characteristic of the other privacy torts). Indeed, nothing in the *Restatement (Second) of Torts* formulation of the false light tort requires the disclosure of any private information. RESTATEMENT (SECOND) OF TORTS § 652E & cmt. a (1977).

37. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).
38. *See id.* at § 652D.
39. *Id.* at § 652B.
40. *Id.* at § 652B cmt. d.
41. *Id.* at § 652D(a).
42. *Id.* at § 652D cmt. c.
43. *Id.*
44. Schauer, *supra* note 14, at 3.
45. *Id.* at 10.

instead upholds social rules of "deference and demeanor," which Post called "civility rules."[46] Both Schauer and Post recognized, then, that the tort law conception of privacy incorporates society's expectation of privacy.

Courts applying the expectation-driven privacy test focus on the context of the alleged intrusion and the social norms and customs that determine whether an expectation of privacy is reasonable. In *Shulman v. Group W Productions, Inc.*,[47] a helicopter medical crew rescued the plaintiffs from a car that drove off a highway. Accompanying the crew was a television cameraman. The cameraman filmed the medical team rescuing the plaintiffs from the car and transporting them to the hospital in a rescue helicopter, and a helicopter nurse's microphone recorded conversations with one of the plaintiffs. The videotape and soundtrack were used months later in a television show. The plaintiffs never consented to the broadcast and sued the television producers for invasion of privacy.[48] Specifically, the plaintiffs sued under California's common-law equivalent of *Restatement (Second) of Torts* § 652B, intrusion on seclusion.[49]

To evaluate the plaintiffs' privacy claims, the court examined the prevailing social practices and legislative expressions relevant to the expectation of privacy under the circumstances.[50] First, the court examined current media practices and rejected the plaintiffs' claim that filming them at the accident scene was an intrusion on seclusion. The plaintiffs could not have reasonably expected that the media would be prevented from filming the accident scene, because journalists commonly film accident scenes and rescues.[51] The court supported this conclusion by citing California statutes that exempt the press from certain emergency closure orders.[52] Apparently, the court interpreted this exemption as an expression of societal approval for the media

46. Robert C. Post, *The Social Foundations of Privacy: Community and the Self in the Common Law Tort Law*, 77 CAL. L. REV. 957, 961–63 (1989); *accord* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2393 (1996) ("The [privacy] tort invokes objective norms of civility and punishes breaches of civility.").

47. 955 P.2d 469 (Cal. 1998).

48. *Id*. at 475–76.

49. *Id*. at 489–90. The plaintiffs also sued for public disclosure of private facts. The court rejected this claim because the published sounds and images were of legitimate public concern and therefore could not support a claim for disclosure of private facts. *Id*. at 488–89; *see* RESTATEMENT (SECOND) OF TORTS § 652D (1977) (stating that there is no liability for publicizing private facts if the facts are of legitimate concern to the public).

50. *Shulman*, 955 P.2d at 488–89.

51. *Id.* at 490.

52. *Id*. (citing CAL. PEN. CODE §§ 409.5(d)–.6(d) (West 2002)).

reporting on and broadcasting scenes of accidents.

Next, however, the court held that filming the plaintiffs inside the rescue helicopter could constitute an intrusion upon seclusion.[53] The court based its decision on both law and custom. "Although the attendance of reporters and photographers at the scene of an accident is to be expected, we are aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent."[54] The court noted that it was "neither the custom nor the habit of our society that any member of the public at large or its media representatives may hitch a ride in an ambulance and ogle as paramedics care for an injured stranger."[55]

The court also held that recording the plaintiffs' communications with the rescue nurse could constitute an intrusion upon seclusion, and therefore denied the defendants' motion for summary judgment on that claim.[56] The court again based its conclusion on social customs and norms reflected in existing law. Because the accident occurred "in a ditch many yards from and below the rural superhighway," it was extremely unlikely that any passersby on the road could have overheard the conversations.[57] The court also noted "existing legal protections for communications could support the conclusion that [the plaintiff] possessed a reasonable expectation of privacy in her conversations with [the nurse] and the other rescuers."[58] The court cited the physician-patient privilege codified in the California Evidence Code and the Confidentiality of Medical Information Act, as well as the California Invasion of Privacy Act's prohibition of recording any confidential communication without the consent of all parties.[59]

The court considered the implications of established custom and norms on whether the intrusion could be highly offensive to a reasonable person. The court contrasted established reporting techniques, such as questioning people who know confidential information, with techniques

53. *Id*.
54. *Shulman*, 955 P.2d at 490.
55. *Id*. at 491 (quoting the court of appeal decision, 59 Cal. Rptr. 2d 434, 453 (Ct. App. 1996)).
56. *Id*.
57. *Id.*
58. *Id*.
59. *Id*. at 491–92 (citing California Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56–56.37 (West 2002); CAL. EVID. CODE §§ 990–1007 (West 2002); California Invasion of Privacy Act, CAL. PEN. CODE §§ 630–637.6 (West 2002)).

that intrude upon "well-established legal areas of physical or sensory privacy—trespass into a home or tapping a personal telephone line."[60] The latter are much more likely to be highly offensive to a reasonable person because they are substantially harder to justify.[61] The court also noted that courts should consider the purpose of the intrusion, and suggested that a reasonable person's measure of offensiveness might depend on whether the intruder was a reporter or a debt collector.[62] This evaluation reflects a social judgment about the relative importance of the functions that different social actors serve.[63] Thus, the *Shulman* court relied heavily on social norms, as reflected in custom and law, to apply the expectation-driven privacy test.

The Idaho Supreme Court undertook a similarly expectation-based inquiry in *Hoskins v. Howard*.[64] The plaintiffs sued for invasion of privacy based on interception of their cordless telephone conversation.[65] Vacating the district court's entry of summary judgment for the defendants, the Idaho Supreme Court held that there was a genuine issue as to whether the plaintiffs had a legitimate expectation of privacy.[66] The court reasoned that an Idaho antiwiretapping statute established society's desire to preserve an expectation of privacy in wire communications, including cordless telephone conversations.[67]

Finally, in *Lewis v. Dayton Hudson Corp.*,[68] a Michigan court found no reasonable expectation of privacy where a sign notified shoppers in retail store fitting rooms that they were under surveillance. An

---

60. *Shulman*, 955 P.2d at 494.
61. *Id*.
62. *Id.* at 493.
63. *See id*. at 493–94. The court held that "a reasonable jury could find highly offensive the placement of a microphone on a medical rescuer in order to intercept what would otherwise be private conversations with an injured patient." *Id*. at 494. The court reasoned:

> [T]he patient would not know her words were being recorded and would not have occasion to ask about, and object or consent to, recording. Defendants, it could reasonably be said, took calculated advantage of the patient's "vulnerability and confusion." Arguably, the last thing an injured accident victim should have to worry about while being pried from her wrecked car is that a television producer may be recording everything she says to medical personnel for the possible edification and entertainment of casual television viewers.

Id. (citation omitted) (quoting Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668, 679 (Ct. App. 1986)).
64. 971 P.2d 1135 (Idaho 1998).
65. *Id*. at 1140.
66. *Id*. at 1141–42.
67. *See id*. at 1138–39, 1142 (holding that the cordless telephone conversation constituted a "wire communication" under the statute) (citing the Idaho Communications Security Act, IDAHO CODE § 18-6701–18-6709 (Michie 1997)).
68. 339 N.W.2d 857 (Mich. Ct. App. 1983).

undercover police officer, who happened to be shopping in the store, entered the fitting room to try on clothes, and put down his gun while he was changing. A security guard monitoring the room saw the gun and the police were called.[69] The court rejected the undercover officer's invasion of privacy claim because a sign in the fitting room warned that the area was under surveillance, and removed any reasonable expectation of privacy in the dressing room.[70]

B. The Legislative Conception of Privacy

From one perspective, the legislative approach to privacy seems quite different from the judicial conception. For the most part, legislatures pass specific statutes that fix particular matters or circumstances as private. Once such a statute exists, there is no need to refer to social expectations to determine whether matters encompassed by the statute should be private.[71] For example, in the wake of the controversial

69. *Id*. at 858.

70. *Id*. at 860; *see also* Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971).

> One who invites another to his home or office takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves. But he does not and should not be required to take the risk that what is heard and seen will be transmitted by photograph or recording, or in our modern world, in full living color and hi-fi to the public at large . . . .

Id.; Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir.1969) (finding that the intrusion tort protects against intrusion "whether by physical trespass or not, into spheres from which an ordinary man in a plaintiff's position could reasonably expect that the particular defendant should be excluded"); Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1135–36 (Alaska 1989) ("[T]here is a sphere of activity in every person's life that is closed to scrutiny by others. The boundaries of that sphere are determined by balancing a person's right to privacy against other public policies."); Sanders v. Am. Broad. Co., 978 P.2d 67, 72 (Cal. 1999) ("There are degrees and nuances to societal recognition of our expectations of privacy."); Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1068–71 (Colo. Ct. App. 1998) (holding that a medical intern had areasonable expectation of privacy against a hospital performing an unconsented-to HIV test on a blood sample (given for purpose of testing for rubella), because of the generally recognized privacy interest in information concerning one's health, Colorado statutes restricting access to one's medical records, and Colorado statutes requiring express consent before testing for HIV); People of Colorado v. Lesslie, 939 P.2d 443, 446 (Colo. Ct. App. 1996) (stating that a reasonable expectation of privacy requires balancing a person's actual expectation of privacy in an area against society's willingness objectively to recognize the reasonableness of that expectation).

71. Some statutes, however, explicitly incorporate the expectation-driven conception of privacy. *See, e.g*., California's so-called anti-paparazzi legislation, CAL. CIV. CODE § 1708.8(b) (Deering 1994 & Supp. 2002).

> A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any

conformation hearings over Judge Robert Bork's Supreme Court nomination, Congress passed the Video Privacy Protection Act of 1988.[72] During the hearings, many were shocked to learn that a journalist from Washington, D.C.'s, *City Paper* had obtained a printout of the movies Judge Bork rented from his neighborhood video store.[73] Today, the Video Privacy Protection Act allows civil suits against any video tape service providers who knowingly disclose the titles of videos rented by their customers.[74] The Act provides for statutory damages of $2500, plus punitive damages and reasonable attorney's fees.[75] We need not consult society's expectation concerning whether video stores will disclose the movies that we rent. Congress has already answered that question. Moreover, by prohibiting disclosure, Congress has either created or reinforced a reasonable expectation of privacy in the video rental records.

We cannot ignore, however, the role of social expectations in the legislative process. As the branch most directly representative of the people, legislatures play a unique role in articulating public norms and values, including norms and values about privacy.[76] Indeed, Congress

---

> type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy . . . .

Id.; WASH. REV. CODE ANN. § 9A.44.115 (West 2000) (prohibiting photographing a person without his or her consent "in a place where he or she would have a reasonable expectation of privacy").

72. 18 U.S.C. § 2710 (2000).

73. *See* SIMSON GARFINKEL, DATABASE NATION 72 (2000). Though many remember the controversy over a journalist obtaining Judge Bork's video rental records in the hope of demonstrating that he rented of pornographic films, fewer remember that the records revealed nothing controversial. As it turned out, most of the 146 movies were Disney movies and Hitchcock films. *Id.*

74. 18 U.S.C. § 2710(b)(1) (2000). Videotape service providers may, however, disclose the names of videos to law enforcement agencies pursuant to a warrant, grand jury subpoena, or court order. *Id*. § 2710(b)(2)(C). They may even disclose consumers' names, addresses, and the "subject matter" of the videos they rent, so long as (1) they provide consumers the chance to opt-out of such disclosures, and (2) the subject matter information is used solely to market goods "directly to the consumer." *Id.* § 2710(b)(2)(D)(ii).

75. *Id.* § 2710(c). The Act also forbids the use of any improperly obtained video store information in any state or federal judicial, administrative, or legislative proceeding. *Id.* § 2710(d).

76. *See, e.g.*, Frank Michelman, *Bringing the Law to Life: A Plea for Disenchantment*, 74 CORNELL L. REV. 256, 256 (1989) ("Politics, I contend, is the only avenue by which public values (insofar as we can speak at all of such matters) might possibly be determinable and accessible."); Cass R. Sunstein, *Beyond the Republican Revival*, 97 YALE L.J. 1539, 1545 (1988) (The function of politics "is to select values, to implement 'preferences about preferences,' or to provide opportunities for preference formation rather than simply to implement existing desires.") (citations omitted) (quoting Cass R. Sunstein, *Legal Interference with Private Preferences*, 53 U. CHI. L. REV. 1129, 1140 (1986); *see also* LANI GUINIER, THE TYRANNY OF THE MAJORITY: FUNDAMENTAL

has on occasion taken a different view than the Supreme Court concerning what is a reasonable expectation of privacy in particular circumstances. In the 1928 case *Olmstead v. United States*, the Court had to decide whether wiretapping a telephone line was a search under the Fourth Amendment.[77] Despite Justice Brandeis' famous defense of privacy in his dissent, the Court held that the wiretap was not a search, based on the suspect and literal-minded reasoning that the wiretap did not involve any physical intrusion into the house.[78] In the wake of *Olmstead*, Congress blunted the effect of the Court's ruling by enacting section 605 of the Federal Communication Act, prohibiting intercepting and revealing telephone communications without the sender's consent.[79]

Obviously, existing social norms are not the sole influence on legislation. Special interests wield tremendous influence on the legislative agenda, and often produce legislation that under protects privacy, compared with the level of protection contemporary social norms would support.[80] In theory, Congress could blaze a trail that it felt was required as a matter of policy or morality, but that the prevailing norms of the time rejected. Were Congress to blaze such a trail in the privacy area, it would be

FAIRNESS IN REPRESENTATIVE DEMOCRACY 186 (1994) ("[L]egislative bodies offer a more public, more participatory forum within which to debate and shape collective values.").

77. Olmstead v. United States, 277 U.S. 438, 462 (1928).

78. *Id.* at 466. In dissent, Justice Brandeis argued that the Court's interpretation of the Fourth Amendment should keep pace with developing technology. Though physical intrusion into a suspect's home was the way for government to invade privacy in the 1790s, the development of telephone communications made invasions of privacy possible even without a physical intrusion. *See id*. at 473–74. Justice Brandeis argued that the Court should extend the Fourth Amendment to telephone communications in order to protect the same amount of privacy that the framers intended to protect. *See id*. at 478–79. Alan Westin noted that Chief Justice Taft was determined that the *Olmstead* case, involving a bootlegger defendant, would not see law enforcement hindered by "bleeding hearts," and that Taft "saw the case as part of his struggle against the 'dangerous' liberal positions advocated on constitutional issues by Justices Holmes, Brandeis, and Stone." WESTIN, *supra* note 1, at 340.

79. 47 U.S.C. § 605 (2001); *see* Robert M. Pitler, *Independent State Search and Seizure Constitutionalism: The New York Court of Appeals' Quest for Principled Decisionmaking*, 62 BROOK. L. REV. 1, 59 (1996). Note that Chief Justice Taft, in the majority opinion, invited Congress to pass legislation to address the wiretap issue. *See Olmstead*, 277 U.S. at 465–66.

80. *See generally* Center for Public Integrity, *Nothing Sacred: The Politics of Privacy* (1998) (examining how special interest groups and corporations opposed to privacy legislation have influenced the legislative decisionmaking process on privacy protection), *available at* http://www.public-i.org/dtaweb/downloads/nothing_sacred.pdf (last visited July 21, 2002) [hereinafter *Nothing Sacred*].

creating a reasonable expectation of privacy where none had existed before—or where one had once existed but had since disappeared.

The unlikelihood of such trailblazing highlights the role of societal expectations in privacy legislation. Given the powerful influence of various lobbies opposed to strong privacy protection,[81] that role may best be described as a sine qua non. That is, unless the public has a strong desire for privacy in a particular area, attempts to pass legislation establishing that area as a private sphere are doomed to fail. The mere existence of public support, however, does not guarantee passage of the legislation. To the extent that legislatures base privacy legislation on social values and norms, they necessarily rely on the same changing expectations as the judicial conception of privacy. The following Section examines the mechanism by which powerful industries and institutions can gradually erode society's expectation of privacy.

C. Encroachment on the Expectation-Driven Conception of Privacy

This expectation-driven conception of privacy is vulnerable to encroachment. Actors and groups powerful enough to influence social behavior can change society's expectation of privacy, and thereby change what the law will protect as private. They do so by changing their own conduct or practices, by changing or designing technology to affect privacy, or by implementing laws that affect society's expectation of privacy.

Jeffrey Rosen recognized the vulnerability of the expectation-driven conception of privacy. "People's subjective expectations of privacy tend to reflect the amount of privacy they subjectively experience; and as advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protections."[82] So, for example, if employers monitor their employees' telephone or e-mail use while they are in the workplace, they diminish the expectation of privacy in the workplace. If merchants routinely sell consumers' personal data, they diminish the expectation of privacy in one's transactional information. And if the Supreme Court holds that law enforcement may review citizens' bank records without a warrant, it diminishes the societal expectation of privacy in one's bank records.[83]

---

81. *Id.* (noting the influence of groups and corporations opposed to privacy through such means as campaign contributions and lucrative employment offers to senior congressional staffers).

82. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60–61 (2000).

83. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (holding that bank

The encroachment proceeds so gradually as to seem to be the inevitable price of progress. An important precursor to resisting the process of encroachment is to recognize its cyclical and self-perpetuating nature. To examine where the process begins,[84] I shall use an example in the context of workplace privacy. In recent years, employers have become increasingly concerned about employee Internet use. Employers express two concerns: first, that employees may visit and share Web sites that are sufficiently offensive to raise potential hostile work environment claims; and second, that employees may waste too much work time surfing the Web.[85]

Suppose that when these concerns first emerged, employers had a variety of options at their disposal. On one end of the spectrum were relatively noninvasive responses. For example, they could focus on productivity statistics, which presumably would reflect Internet abuse as well as other inefficient habits. Or they could ask supervisors to meet more frequently with their employees to keep tabs on both their productivity and their interactions with other employees. On the other end of the spectrum were quite invasive responses. For example, employers could install surveillance software on each employee's computer to monitor every keystroke the user enters.[86] Or they could

---

depositors have no reasonable expectation that the bank will keep their records private from the government).

84. To say that the process begins is necessary for purposes of illustration, but is technically inaccurate because the process is ongoing. Society's expectations are constantly evolving in response to social changes.

85. *See* ROSEN, *supra* note 82, at 78–80 (discussing employer concern with sexual harassment liability resulting from employees' inappropriate Internet and e-mail use); Charles Waltner, *Tools that Monitor Employees' Net Surfing Save Companies Bandwidth and Time*, INFORMATIONWEEK, Apr. 27, 1998, at 121 (proposing that employers' frustration with non work related Internet use spurred growth of Web monitoring tools), *available at* 1998 WL 2359450. For example, in late 2001, the Director of the Administrative Office of the U.S. Courts activated filtering software that recorded all downloads of mpeg movie files and MP3 music files by federal judicial employees—including judges—accessing the Internet at work. Jeffrey Rosen, *Who's Spying on Judges?*, THE NEW REPUBLIC ONLINE, Sept. 10, 2001, *at* http://www.tnr.com/091001/rosen091001.html. The director justified the covert monitoring with slow Internet response times attributed to audio and video downloads. *Id.*

86. *See, e.g.*, Adavi, Inc., *Product Overview: Silent Watch 2.0* (2000), *at* http://www.adavi.com/ overview.cfm (describing Silent Watch, a surveillance software package that monitors and records every keystroke on an unlimited number of computers) (last visited Apr. 29, 2002). Adavi, Inc. describes Silent Watch as "ideal for businesses, schools, government entities and organizations with networked computers." *Id*. Silent Watch sells for $199.95. *Id.* Adavi, Inc. also offers a home version, Silent Guard, that monitors and logs keystrokes on a non-networked computer. Silent Guard

install software that logs every Web page the employee visits and the duration of each visit.[87] Still other responses lay somewhere in the middle ground, such as installing software to track the total time that each employee spends on the Web.[88]

Further suppose that few employers had any established policy or practice to address their concerns, and that most employers adopted the middle-of-the-spectrum response of tracking the total time each employee spent online. Before the employers took this step, many employees may have felt that the extent of their Internet use was not a matter that their employers should (or could) know. Afterward, however, employees could no longer expect their employers to remain unaware of how often or for how long they used the Internet. Although employers could expect some level of complaint from employees, they could probably rebut any minor opposition by justifying the measure as a moderate response to the efficiency and liability concerns discussed above. By choosing the moderate response, employers slightly diminished society's expectation of privacy in the workplace. Further development of this hypothetical will help illustrate the two elements of the incremental encroachment on privacy—embedded imprecision and internalization—which are discussed in the following Sections.

1. Embedded Imprecision

Effective encroachment occurs at the margins, in the imprecision embedded in the expectation-driven conception of privacy. This imprecision exists because there will always be a gray area between

---

can even take a screen snapshot when any word in the product's dictionary is typed or appears in any Internet traffic. *Id.* Silent Guard sells for just $49.95. *Id*.

For another example, see Spectorsoft's description of its product, "eBlaster." SpectorSoft.com, *eBlaster for Windows*, *at* http://www.spectorsoft.com/products/eblaster_windows/ (last visited Apr. 29, 2002).

> Are you concerned about what your spouse, employees or children do on the Internet while you're away? You can't always be around to watch over their shoulders, so hire a second pair of eyes with eBlaster.
>
> eBlaster monitors their PC and Internet Activity by recording every [W]eb site they visit, every program they run, every keystroke they type, and all popular instant messages and chats. eBlaster then sends the recorded activity to your e-mail address as frequently as every 30 minutes.

Id. The product even includes full transcripts of chat room and instant messaging sessions and is available for a special offer price of $69.95. *Id.*

87. *See* Adavi, Inc., *supra* note 86 (advertising that Silent Watch can sound an alarm to the system administrator "when users reach objectionable Web sites or inappropriate text content based on a dictionary of the user's choice.").

88. *See* Waltner, *supra* note 85, at 121 (describing Web monitoring software that can automatically e-mail to managers a list of the most active Web surfers and calculate the cost of employees' Web surfing by multiplying their online minutes by their per minute salary rate).

what society clearly expects to be protected (that is, private), and what it clearly understands to be unprotected. Had the employers in my example chosen the most invasive option first, they risked mobilizing serious opposition among employees. There would likely have been a consensus among employees that the most extreme option intruded on their privacy. Choosing the most extreme option would have reached beyond the gray area and offended society's expectation of privacy in the workplace. Rather than overreach with a single step, actors encroach in small increments, repeatedly claiming the gray area for themselves. They exploit the imprecision that pervades our expectation-driven conception of privacy by eroding privacy at the margins.

To further illustrate how embedded imprecision facilitates incremental encroachment, here are some possible next steps in my example. Employers could expand the monitoring of Internet usage to include the monitoring of which Web sites employees visit. Given that employees already expect some monitoring of their Internet use, employers may not face serious opposition to this expansion of their current policy. Some may voice complaints, but this small step probably would not offend any clearly understood expectation of privacy. Once the Web site monitoring policy has taken root and employees have again reshaped their expectations, employers may expand their monitoring to include the individual Web pages visited within each site. As that expansion and successive expansions are established, it may be only a matter of time before employers reach what at the outset had been the most extreme option—monitoring every keystroke on the company's computers.

2. Internalization

Critical to the incremental encroachment described above is that individuals internalize each successive encroachment. For example, in the workplace monitoring hypothetical discussed above, employees first internalized the idea that employers would (and could) monitor the total time they spent on the Internet. Once they accepted that practice, expectations shifted, so that the employers' next step—monitoring the particular Web sites that employees visited—then lay within the gray area of unsettled expectations. As each small step of encroachment becomes entrenched, individuals internalize the encroachment and lose any sense that privacy was once possible in the encroached-upon area. Because of this internalization, the expectation-driven privacy test cannot consider the effect of successive encroachments. Rather, by its

nature, the test can only evaluate the challenged practice in light of the current level of expectations.

Scholars have approached the phenomenon of internalization from many different perspectives and in connection with a variety of topics. Jeremy Bentham's concept of the Panopticon most directly illustrates internalization in the privacy context.[89] Bentham conceived his ideal prison, the Panopticon, in 1787.[90] Its purpose was to change prisoners' behavior through "the illusion of constant surveillance."[91] Bentham envisioned a central tower with windows on all sides, surrounded by a ring of cells occupied by the prisoners. The cells open inward, and an inspector in the central tower can monitor and speak to any prisoner at any time.[92] Critical to the panoptic effect is that the prisoners know their behavior can be constantly monitored, but cannot know when the inspector is monitoring them because they cannot see his face.[93] The mere possibility of being observed deters misconduct, even when the prisoners are not being observed.[94] The genius of Bentham's Panopticon is that people gradually internalize and comply with the rules, without remembering that the inspector's observation caused them to change their behavior.[95] Foucault captures the internalization of privacy invasions:

> He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he *inscribes in himself* the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection.[96]

Thus, the panoptic condition becomes part of the inmates' very identity.[97]

---

89. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195–308 (Alan Sheridan trans., Vintage Books 1977) (discussing Bentham's Panopticon at length).

90. *See* REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 32 (1999).

91. *Id*. at 33 (quoting JEREMY BENTHAM, THE PANOPTICON WRITINGS 16 (Miran Bozovic ed. 1995)). Bentham trumpeted his idea as a "new mode of obtaining power of mind over mind, in a quantity hitherto without example." *Id*. at 34 (quoting BENTHAM, *supra*, at 31). Reg Whitaker termed the modern state of widespread surveillance the "Participatory Panopticon." *Id*. at 139.

92. *Id*. at 32–33.

93. *Id*. at 33. An elaborate system of "lanterns and apertures" renders the Inspector a silhouette, so the prisoners cannot see his face. *Id*.

94. *Id.*

95. *See* Nicholas C. Burbules, *Privacy, Surveillance, and Classroom Communication on the Internet*, http://faculty.ed.uiuc.edu/burbules/ncb/papers/privacy.html (last visited Apr. 19, 2002).

96. FOUCAULT, *supra* note 89, at 202–03 (emphasis added).

97. *See* Burbules, *supra* note 95 (citing FOUCAULT, *supra* note 89, at 200).

In her extensive historical, sociological, and psychological study of information technology's influence in the workplace, Shoshanna Zuboff observed internalization in workers trying to cope with their disappearing privacy.[98] Workers whose conduct is exposed, especially in ways they might not choose to be, develop techniques to avoid the shame of disclosure.[99] Zuboff called one such technique "anticipatory conformity."[100] As surveillance becomes more pervasive, "the pressure of visibility begins to reorganize behavior at its source, shaping it in conformity with the normative standards of the observer."[101] Anticipatory conformity does not derive solely from the threat of shame before the employer, but also from the threat of shame before one's coworkers.[102]

The critical feature of the panoptic effect is that it becomes a way of life. Nicholas Burbules, writing about the panoptic effect and the vulnerable state of privacy, observed that people gradually come to accept established mechanisms of surveillance, such as the video cameras that track us in subways, banks, parking lots, stores, and elevators.[103] "As people accept the inevitability of being observed and recorded, their habits change; they change."[104] Not only do they change, but they lose sight of the external instrumentality that made them change in the first place. Burbles argues that the line between the public and private spheres may become meaningless as "people carry many of the attitudes and self-imposed restrictions of activity from the surveyed public into their private life—so in what sense is it still 'private'?"[105]

Burbules illustrated the panoptic effect in a familiar context: seating students in a circle, rather than row-by-row.[106] Because every student is continuously visible to the instructor and to the other students, every student must conform her behavior to what she considers acceptable to the others.[107] The insidious aspect of the panoptic effect is not merely the conformity. It is the fact that the students lose sight of *why* they have

98. *See generally* SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER (1984).
99. *Id.* at 342–45.
100. *Id.* at 345.
101. *Id.*
102. *Id.* at 346.
103. Burbules, *supra* note 95.
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id*. This illustrates how Zuboff's anticipatory conformity works horizontally, within a peer group, as well as vertically, within a hierarchy.

conformed their behavior—to conform with the perceived norms of others. The students gradually internalize those previously external norms, and superimpose them on their own.[108] Because of this internalization, each step of the incremental encroachment is tested only against the status quo, without consideration of what society considered private several steps before.[109]

3. Overreaching

Of course, not every attempted encroachment succeeds. Occasionally, industry or government overreaches the gray area, and so upsets settled societal expectations that it must retreat. Such steps were too drastic to remain hidden within the imprecision embedded in the expectation-driven conception of privacy.

One prominent example in cyberspace is DoubleClick's failed plan to create a vast database of personal profiles by merging its detailed but anonymous Internet profiles with a vast store of personally identified direct mail profiles owned by Abacus Direct. DoubleClick places ads from nearly 4500 companies on thousands of Web sites.[110] When

---

108. *See id*. Stanley Benn makes a similar point: "We act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change." Stanley Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XIII: PRIVACY, *supra* note 1, at 1, 24 (quoting Hubert Humphrey, *Forward* to EDWARD V. LONG, THE INTRUDERS (1967)).

109. Internalization theories appear in a variety of literature not dealing directly with privacy. Law and economics scholars have offered economic analyses to explain the internalization of social norms. *See, e.g.*, Robert Cooter, *Do Good Laws Make Good Citizens? An Economic Analysis of Internalized Norms*, 86 VA. L. REV. 1577, 1577–80 (2000). Elaborating on H.L.A. Hart's jurisprudential discussion of rule internalization, Frederick Schauer explains that an agent has internalized a rule when the agent treats the rule's existence as relevant to deciding what to do. *See* FREDERICK SCHAUER, PLAYING BY THE RULES: A PHILOSOPHICAL EXAMINATION OF RULE-BASED DECISION-MAKING IN LAW AND LIFE 121 (1991). Internalization also appears in behavioral and developmental psychology literature. *See, e.g.*, Joan E. Grusec & Jacqueline J. Goodnow, *Impact of Parental Discipline Methods on the Child's Internalization of Values: A Reconceptualization of Current Points of View*, 30 DEVELOPMENTAL PSYCHOL. 4, 17 (1994) (stating that internalization of a teacher's values occurs when the student "feel[s] the message has not been imposed but rather has been self-generated"); Dale L. Cusumano & J. Kevin Thompson, *Body Image and Body Shape Ideals in Magazines: Exposure, Awareness, and Internalization*, 37 SEX ROLES 701–21 (1997) (reporting that in a study of female college students, researchers found that internalization of social body type norms had substantially higher predictive value of body dissatisfaction, eating disturbances, and low self-esteem than mere awareness of or exposure to social body type norms); Mark E. Young, *A Classroom Application of Grusec and Goodnow's Discipline Model of Internalization of Values*, 115 EDUCATION 405, 405 (1995) ("Internalization of values is observed when acceptable behavior is generated from intrinsic factors and not from the anticipation of external consequences.").

110. John Schwartz, *Trade Commission Drops Inquiry of DoubleClick Inquiry*,

consumers pull up one of those Web sites, DoubleClick places cookies on their hard drives, and uses the cookies to track consumers' behavior as they surf the Web.[111] DoubleClick combines the data it gathers about each consumer's Web surfing habits into a profile, and delivers ads targeted to each consumer's profile.[112]

DoubleClick had always insisted that it collected consumer information anonymously.[113] That changed in 1999, after DoubleClick's $1.7 billion acquisition of Abacus Direct, which collects vast amounts of data on consumers' catalog shopping habits.[114] DoubleClick announced that it planned to merge its purportedly anonymous online information with Abacus Direct's personally identified data.[115] The public outcry proved too much for DoubleClick, whose public image and stock price suffered from inquiries by the Federal Trade Commission and several state attorneys general, and a complaint to the FTC by the Electronic Privacy Information Center.[116] The pressure prompted DoubleClick to change its privacy policies, and to announce in May 2000 that it would not merge DoubleClick and Abacus Direct data.[117]

N.Y. TIMES, Jan. 23, 2001, at C5.

111. *Id.*

112. Bob Tedeschi, *E-Commerce Report: DoubleClick Is Seeking Ways to Use Online and Offline Data and Protect Users' Anonymity*, N.Y. TIMES, Jan. 29, 2001, at C9; *DoubleClick Privacy Policy*, *available at* http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=& (last modified Nov. 19, 2001).

113. Schwartz, *supra* note 110.

114. *Id.*; *see* Ted Kemp, *Behind the DoubleClick Merger: Buying Behavior is Abacus' Key Asset*, DM NEWS, June 21, 1999, at 1, *available at* 1999 WL 21954252 (analyzing purchase by leading marketer of online advertisements of "a firm that manages the largest catalog of consumer catalog buying habits in the United States").

115. Schwartz, *supra* note 110, at C5.

116. *Id*.

117. *Id*. A California superior court judge recently found that DoubleClick's Web profiling practices intruded upon society's expectations of privacy. The court refused to dismiss a class action claim for invasion of privacy under the California Constitution because "[r]easonable people could find that the secret accumulation of such private information by an entity with whom they have no [sic] agreed to deal with is a serious invasion of privacy." *In re DoubleClick Cases*, No. JC4120 (Cal. Super. Ct. June 6, 2001), *available at* 2001 WL 1029646. The court upheld a claim under a statute prohibiting eavesdropping on "confidential communications" because, although any reasonably intelligent Internet user would be aware that e-mail and chat room messages are recorded, the "defendant has not shown that the same can be said of Web browsing activities." *Id.* (applying section 632(c) of the California Penal Code, CAL. PENAL CODE § 632(c) (Deering 1998), and defining "confidential communication" as "communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto"). Carried to its logical conclusion, the court's reasoning would require dismissal of the plaintiffs' claims if data

The government is not immune to such overreaching, as shown by the Johnson administration's failed effort to create a National Data Center. In 1965, the Bureau of the Budget proposed that the federal government create a National Data Center to centralize data processing and storage efforts by all federal agencies. The first step would be to store selected data from the Bureaus of the Census and Labor Statistics, the Internal Revenue Service, and the Social Security Administration. The original purpose was to cut costs, but proponents touted the potential benefits of cross-referencing data among all federal agencies, such as promoting efficient use of the data and improving data security. The concept "slowly evolved into that of a massive databank containing cradle-to-grave electronic records for every U.S. citizen."[118] The database would contain birth certificates, proof of citizenship, school records, draft and military service information, tax records, Social Security records, death records, and estate information.[119]

Once publicized, the plan was criticized in the press, and Congress held hearings on the threat of computer databases.[120] The House Special Subcommittee on Invasion of Privacy and the Senate Judiciary Subcommittee on Administrative Practices both heard testimony highly critical of the National Data Center plan.[121] Given the extreme negative response in the public and in Congress, the administration did not proceed with the plan.[122]

In a second example of government overreaching, the original draft of the Cyberspace Electronic Security Act could have been interpreted to allow law enforcement to remotely access and place "back doors" in suspects' computers.[123] A back door could give the government access to the suspect's every keystroke, allowing the government to learn passwords and decrypt otherwise uncrackable cryptography. Some even thought the draft Act might grant government permission to contract with software makers to embed those back doors in their systems, so that law enforcement could activate the back doors remotely. The clause in question "was quickly dropped in the face of furious opposition from civil liberties groups."[124]

---

profiling on the Web becomes well-known and commonplace.

118. GARFINKEL, *supra* note 73, at 13–14.

119. *Id.*

120. *Id*. at 14.

121. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 311 (2000); GARFINKEL, *supra* note 73, at 14.

122. GARFINKEL, *supra* note 73, at 14.

123. Froomkin, *Death of Privacy?*, *supra* note 1, at 1487–88 (citing the Draft Cyberspace Electronic Security Act Bill). A back door is a deliberate hole in system security. *See id.*

124. *Id.*

We must not be misled by these highly publicized incidents of overreaching. Although these examples demonstrate the potential to resist encroachment, they are rare exceptions. Most incremental steps of encroachment receive little, if any, public attention. The encroachment occurs below society's radar, so to speak.

In theory, the expectation-driven conception of privacy means that behavioral or technological changes in a society can not only diminish, but can also expand the scope of privacy.[125] For example, employers could pledge not to review medical information about prospective employees. The media could refrain from printing information about political candidates' personal lives. And Congress could pass legislation preventing merchants from using personal data about consumers without the consumers' specific, informed consent to each use. Each of these steps would tend to expand the societal expectation of privacy in the affected information.[126]

In reality, however, we rarely see such expansions of privacy, because the expectation-driven conception of privacy magnifies the effects of incremental encroachment, and because individuals trying to resist that encroachment face seemingly insurmountable obstacles. The next two Sections discuss how these incentives and obstacles facilitate the incremental erosion of privacy.

III. THE EXPECTATION-DRIVEN CONCEPTION OF PRIVACY AND THE FACILITATION OF INCREMENTAL ENCROACHMENT

The previous Part examined in broad terms how the expectation-driven conception of privacy is vulnerable to incremental encroachment. This Part examines how, at the level of particular transactions or practices, the expectation-driven conception of privacy magnifies the

125. *See id*. at 1523 ("Anything that increases a citizen's reasonable expectation of privacy will, under current doctrine, also increase the scope of Fourth Amendment protections.").

126. *See id*. at 1507–08.

> Prohibiting the use of technologies that are not already commonplace prevents the public from being desensitized, and it ensures a reasonable expectation of being able to walk in public without being scanned by them. Similarly, prohibiting the use of commonplace technologies also creates a (legally) reasonable expectation that others will follow the law, and that restricted technologies will not be used.

Id.

ultimate effect of encroachment. As each step of encroachment becomes magnified, individuals find it all the more difficult to resist encroachment on their privacy.

A. Intentional Exploitation of the Expectation-Driven Conception of Privacy

The expectation-driven conception of privacy creates a perverse incentive for businesses to diminish, *proactively*, individuals' expectations of privacy.[127] The logic is simple—one cannot be held liable for invading an expectation of privacy where none exists. We find an obvious example of this manipulation in the employment context, where lawyers routinely advise their clients to deny employees any expectation of privacy. According to Shanti Atkins of Employment Law Learning Technologies, which helps create corporate privacy policies, "Lowering expectation [sic] of privacy is the No. 1 thing they can do to protect themselves from privacy litigation."[128] One commentator advises that "[a]n employer should develop a policy that effectively lowers the expectation of privacy in advance . . . . This will greatly improve an employer's chances of tipping the privacy balance in its favor in future litigation challenging the surveillance or monitoring."[129] Another advises employers to issue written e-mail usage policies that put employees "on notice that the employer will monitor the use of its computer equipment and electronic services. This destroys any reasonable expectation of privacy an employee may have regarding e-mail or Internet usage."[130] He further advises requiring employees to sign forms consenting to the policy. "Although a signed consent form may not provide additional protection if not uniformly enforced, it still demonstrates employee awareness and may help to defeat a right to privacy claim."[131]

We have seen similar preemptive strikes in the area of medical privacy. Medical consumers have customarily been asked to sign broad releases that could justify almost any disclosure of medical data.[132] As a

127. *See* ROSEN, *supra* note 82, at 70.

128. Jeffrey Benner, *Privacy at Work? Be Serious*, WIRED NEWS, Mar. 1, 2001, *at* http://www.wired.com/news/business/0,1367,42029,00.html (last visited June 23, 2002).

129. Kevin J. Baum, *E-Mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1039 n.142 (1997).

130. Hall Adams, III, *et al.*, *E-Mail Monitoring in the Workplace: The Good, the Bad and the Ugly*, 67 DEF. COUNS. J. 32, 44 (2000).

131. *Id*.

132. Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 49 (1997). Schwartz calls this practice a "shallow consent process." *Id.*

result, medical consumers give consent without any meaningful information about what they are consenting to. The sweeping release insulates the health care provider against any claimed expectation that the provider would not share the data.[133] The medical privacy regulations promulgated at the end of the Clinton administration have taken a first step towards addressing this problem. Though they include a host of exceptions,[134] the regulations impose several requirements on providers attempting to gain patients' authorization to use or disclose health information for purposes other than treatment, billing and operations. Authorization forms must include, in plain language, a description "in a specific and meaningful fashion" of the information to be disclosed; the specific identification of the person or class of persons who may make the disclosure and who may receive the disclosure; and a date or event upon which the consent expires.[135]

Web sites commonly attempt to diminish consumers' expectations of privacy through their so-called privacy policies. It is *de rigueur* for a privacy policy to make very specific representations, only to nullify them with a broad disclaimer professing the right to change the policy without notice. Prior to August 31, 2000, Amazon.com's Privacy Notice stated that "Amazon.com does not sell, trade, or rent your personal information to others."[136] The policy continued, however: "We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com."[137] Amazon changed its policy on August 31, 2000, explaining that it was

133. *Id*.

134. Exceptions include disclosures in connection with the following: public health activities; abuse, neglect, or domestic violence victims; health oversight activities; judicial and administrative proceedings; law enforcement purposes; organ or tissue donation; research; veterans activities; national security and intelligence activities; protective services for the President and other officials; and workers' compensation claims. *See* 45 C.F.R. § 164.512(b)-(l) (2001). Nor do the detailed consent requirements apply to disclosures to be used for marketing purposes, s*ee id*. § 164.514(e), although the Department of Health and Human Services has proposed modifications that would apply those consent requirements to most marketing disclosures. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14776, 14815 (proposed Mar. 27, 2002) (proposing new section 164.508(a)(3)).

135. 45 C.F.R. § 164.508(c).

136. Letter from Mariam J. Naini, Associate General Counsel, Amazon.com, Inc. & David Gabrieli, Government Affairs Counsel, Amazon.com, Inc., to Donald S. Clark, Secretary, Federal Trade Commission (June 11, 1999), (attaching Amazon.com's Privacy Policy and customer "Bill of Rights"), *available at* http://www.ftc.gov/privacy/comments/amazoncom.htm (last visited May 17, 2002) .

137. *Id.*

simply clarifying the old policy by specifying that it might share personal information, without customers' consent, in limited circumstances, including the sale of Amazon.com to another company.[138] Of course, the new policy contains another broad exception, which renders' Amazon's restrictive language meaningless: "Our business changes constantly. This Notice and the Conditions of Use will change also, and use of information that we gather now is subject to the Privacy Notice in effect at the time of use."[139] So, at least according to the terms of the so-called Privacy Notice, Amazon.com customers have no expectation that Amazon.com will maintain their privacy.

The hard lesson learned by Toysmart.com should ensure that Web sites include such no privacy clauses in their privacy policies. Toysmart.com filed for bankruptcy and announced that it would sell its database of customer information.[140] Its privacy policy, however, promised unequivocally that customers' personal information "is never shared with a third party," and did not contain any catch-all reservation of the right to change the policy.[141] The FTC sued Toysmart.com for misrepresenting to consumers that it would never share personal information with third parties.[142] The FTC settled that lawsuit in exchange for Toysmart.com's agreement to sell the customer data only to a business that operated a similar Web site and agreed to honor all terms of Toysmart.com's Privacy Statement.[143] The FTC's decision drew protest from privacy advocates and many state attorneys general, who filed objections to the sale.[144] Eventually, the bankruptcy judge ordered the customer data destroyed as part of a settlement in which the Walt Disney subsidiary that owned the majority stake in Toysmart.com

138. Amazon.com, *Privacy Notice*, *available at* http://www.amazon.com/exec/obidos/tg/browse/-/468496/107-6519540-0867760 (visited Apr. 20, 2002); Tamara Loomis, *Amazon Revamps Its Policy on Sharing Data*, N.Y.L.J., Sept. 21, 2000, at 5. Notice that the new policy language also eliminated customers' ability to request that Amazon.com not share their data. *Id.*

139. *Id*.

140. *See* Stephanie Stoughton, *FTC: Toysmart.com Violated Kids' Privacy; Agency's Settlement on Data Rapped*, BOSTON GLOBE, July 22, 2000, at C1, *available at* 2000 WL 3335599.

141. Toysmart.com, *Privacy Statement*, *available at* http://www.toysmart.com/toysmart/ts_cs_privacy/policy.asp (last visited Apr. 26, 2001).

142. First Amended Complaint, Federal Trade Commission v. Toysmart.com, LLC, Civ. No. 00-11341-RGS (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm (last visited Apr. 20, 2002).

143. *See* Stipulation and Order Establishing Conditions on Sale of Customer Information, In re Toysmart.com, LLC, No. 00-13995-CJK (Bankr. D. Mass. July 20, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmarttbankruptcy.1.htm (last visited Apr. 20, 2002).

144. *See* Stephanie Stoughton, *States Weigh in on Toysmart Privacy Case; 38 Attorneys General Join Opposition to Sale of Data*, BOSTON GLOBE, July 26, 2000, at C1, *available at* 2000 WL 3336111.

paid the bankrupt company $50,000.[145] The lesson of the Toysmart.com saga may turn out to be that Web companies rely increasingly on no privacy policies like Amazon.com's.

B. Media Encroachment and Society's Diminution of Its Own Privacy Expectations

Today the media relentlessly appeal to and cultivate a voyeurism through which society unwittingly erodes its own expectation of privacy. The feeding frenzy yields television shows like *Big Brother* and *Survivor*, tabloid journalism in which no subject is too personal, and relentless investigation into the personal lives of public figures and their families. As we watch and read, we willingly delve into what we see as *other people's* privacy. However, because of the expectation-driven nature of privacy, we are simultaneously diminishing our own expectations of privacy.

Over a century ago, the problem of tabloid journalism prompted Warren and Brandeis to write their seminal article on privacy.[146] Today, we deal with problems similar in kind but far greater in degree. Extreme elements of the media seize upon and sell increasingly intimate details of people's personal lives, gradually dragging the mainstream media along for the ride once the prevailing expectations of privacy have sufficiently diminished that the public will accept more banal fare. For example, sensationalist journalism was not so long ago confined to supermarket tabloids. Now, such stories are reprinted in other newspapers, broadcast on television shows like *Inside Edition* and *Access Hollywood*, and spread across the Internet.[147] David Broder wrote that the print and broadcast versions of tabloid journalism "have demonstrated the capacity to 'launch' stories—often of the sleaziest kind—that the mainstream press feels necessary to follow."[148] Warren and Brandeis warned back in 1890 that tabloid journalism would erode social standards in gradual increments:

---

145. *See* Stephanie Stoughton, *Toysmart.com List to Be Destroyed*, BOSTON GLOBE, Jan. 30, 2001, at D7.

146. *See* Warren & Brandeis, *supra* note 32, at 76–77.

147. CHARLES J. SYKES, THE END OF PRIVACY 188 (1999).

148. *See* Andrea Sachs, *Mud and the Mainstream: When the Respectable Press Chases the National Enquirer, What's Going On?*, 34 COLUM. JOURNALISM REV., May/June 1995, at 33, 33 (quoting David S. Broder, *Junk Journalism*, WASH. POST, Feb. 23, 1994, at A17).

> Nor is the harm wrought by such invasions confined to the suffering of those who may be made the subjects of journalistic or other enterprise. In this, as in other branches of commerce, the supply creates the demand. Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation, results in a lowering of social standards and of morality. Each gossip apparently harmless, when widely and persistently circulated, is potent for evil.[149]

Recent decades have seen encroachment incentives at work in the media's coverage of public officials' personal lives. The press has a strong incentive to disclose potentially embarrassing private facts about public officials. For the shrinking number of corporations that own the media, the profit motive is obvious: sensational or salacious stories generate higher ratings and readership, which in turn generate more revenue.[150] Individual journalists have their own incentives, which include money, power, and celebrity.[151] They attempt to legitimize the intrusion on public officials' sex lives on the theory that a history of sexual indiscretions demonstrates bad character or judgment, both undesirable traits in political leaders.[152] The media use the mantra of the public's *right* to know as justification for serving or stimulating the public's voyeuristic *desire* to know.

In the past, public officials could expect a measure of privacy for their sexual affairs. Anita Allen wrote of a time when "family, friends, employees, and the press adhered to an unwritten code of privacy," and kept secret the "sexual intimacies of public officials and celebrities."[153] Allen cited as examples the rumored affairs of both President Franklin D. Roosevelt and First Lady Eleanor Roosevelt, and the extramarital sex lives of Presidents John F. Kennedy and Lyndon Johnson.[154] Today, however, public servants have internalized the media's encroachment on privacy. Public servants now believe that "what takes place in private, unless dull and routine, is likely to become public knowledge anyway."[155] Allen pointed out the change in how the media treated political figures' sexual conduct, from the Kennedy to the Clinton

149. Warren & Brandeis, *supra* note 32, at 77.

150. *See, e.g.*, David Shaw, *Two Impulses Drive the Mania: Prurience and Self-Preservation*, L.A. TIMES, Feb. 18, 1998, at B11; David Shaw, *The Simpson Legacy: Chapter Three: Tabloid Tornado; Mainstream Media; 'The Godzilla of Tabloid Stories'*, L.A. TIMES, Oct. 9, 1995, at S4; David Shaw, *Obsessed with Flash and Trash*, L.A. TIMES, Feb. 16, 1994, at A1.

151. Anita Allen, *Privacy and the Public Official: Talking About Sex as a Dilemma for Democracy*, 67 GEO. WASH. L. REV. 1165, 1165 (1999).

152. *Id*. at 1168. The *National Enquirer* established a measure of credibility among mainstream publications when it helped end Gary Hart's political career by publishing the infamous "Monkey Business" photo. Sachs, *supra* note 148, at 33.

153. Allen, *supra* note 151, at 1174.

154. *Id.*

155. *Id.* at 1165.

administrations.[156] Public officials' diminished expectations over those three decades are especially problematic because of the media's ability to resurrect indiscretions that political figures had considered ancient history. In 1998, when the House of Representatives impeached President Clinton for his conduct in the Lewinsky scandal, three different news outlets broke stories about decades-old extramarital affairs involving House Republicans. *Salon.com* exposed the thirty-year-old extramarital affair of Republican Congressman Henry Hyde, a House prosecutor in the Clinton impeachment trial.[157] Republican Congressman Dan Burton preempted impending press reports by admitting to the *Indianapolis Star and News* that he had fathered a child in an extramarital affair during the 1980s.[158] And the Internet site of Congressional newsletter *Roll Call* first published House Speaker-Elect Bob Livingston's admission, also to preempt forthcoming media reports that he had engaged in several extramarital affairs during his thirty-three years of marriage.[159] This unrelenting media coverage about public officials' personal lives feeds—or generates[160]—the public's desire for such salacious details. And as the increasingly intimate media coverage makes society come to expect such coverage, public officials gradually lose the expectation of privacy in their intimate relations.

Allen also addressed the more general erosion, over the last decades of the twentieth century, of the "expectations of personal privacy and of the

156. *Id.* at 1168–69.

157. David Talbot, *This Hypocrite Broke up My Family*, SALON.COM, Sept. 18, 1998 *at* http://www.salon.com/news/1998/09/cov_16newsb.html (last visited Mar. 29, 2001).

158. George Stuteville et al., *Burton Admits Affair*, INDIANAPOLIS STAR AND NEWS, Sept. 5, 1998, at 1; *see* Edward Walsh, *Burton Fathered Child in Extramarital Affair*, WASH. POST, Sept. 5, 1998, at A1.

159. Howard Kurtz, *White House Angry About GOP Charge*, WASH. POST, Dec. 18, 1998, at A40; *Text of Livingston Statement, Thursday, Dec. 17, 1998*, WASHINGTONPOST.COM, *at* http://washingtonpost.com/wp-srv/politics/special/clinton/stories/livingstontext121798.htm (last visited Mar. 29, 2001). This slew of exposed affairs may be attributable in part to *Hustler Magazine* publisher Larry Flynt, who in October 1998 offered up to $1 million for information about the sexual affairs of political leaders. Flynt accused Republicans pursuing the Clinton-Lewinsky affair of hypocrisy. *See Livingston Bows Out of the Speakership*, CNN.COM, Dec. 19, 1998, *at* http://www.cnn.com/ALLPOLITICS/stories/1998/12/19/livingston.quits/ (last visited Mar. 29, 2001).

160. For a critique of the notion that the media simply "give the people what they want," see ROBERT W. MCCHESNEY, RICH MEDIA, POOR DEMOCRACY: COMMUNICATION POLITICS IN DUBIOUS TIMES 32–33 (1999) ("As much as demand creates supply, supply creates demand.").

taste for personal privacy in the United States."[161] She speculated that possible causes include the prevalence of communication and surveillance-enhancing technologies, government surveillance practices, and commercial data collection techniques.[162] Further diminishing expectations of privacy are "opportunities to earn money and celebrity by giving up privacy voluntarily, and . . . opportunities to consume other people's privacy and private lives on the cheap."[163] We find often shocking exposés of personal lives in tabloids, television talk shows like *Oprah* and *Jerry Springer*, and so-called reality TV shows like CBS's *Big Brother* and *Survivor*, and MTV's *The Real World*. These tell-all stories and programs depend upon more than the exhibitionist few who participate; they depend upon a great silent majority of the public with a voyeuristic taste for peering into other people's privacy.

Allen noted perceptively that these genres of voyeurism quickly lose their shock value, and must continually be replaced by even more shocking manifestations, like using Internet Web sites that allow you to find detailed personal or financial information about others,[164] or "watch[ing] strangers on-line in real time as they groom themselves and interact with their intimates."[165] The market for private facts both feeds and constructs the taste for consuming other people's privacy.[166]

Allen harbored some hope that in the aftermath of the Clinton-Lewinsky ordeal our public officials' expectations of sexual privacy may wax in response to several decades of waning. There is a chance, she

---

161. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 729 (1999).
162. *Id.* at 730.
163. *Id.*
164. *See, e.g.*, Harris Digital Publishing Group, *NetDetective 7.0*, *at* http://www.netdetective2001.com (last visited July 15, 2002). The Net Detective's promotion speaks volumes about its intended audience:

> With Net Detective's exclusive BACKGROUND CHECKER™ YOU CAN [ ] Check Out new and old ROMANTIC interests; Dig up the dirt on your BOSS, co-workers, or neighbors; Verify EMPLOYMENT applications; check for bankruptcy, small claims, and TAX LIENS; Check death, MARRIAGE and PROPERTY records; Snoop for SECRETS your neighbors don't want you to know.

Harris Digital Publishing Group, *supra*, *at* http://www.netdetective2001.com/background_searches.html (last visited July 15, 2002). The site proudly displays the following testimonial:

> I have been telling my friends about NetDetective. I have also been snooping on my friends, and they don't even know it. I found out how much alimony and child support my next door neighbor gets, and that my neighbor across the street has some big credit problems. This is AWESOME!!!

Harris Digital Publishing Group, *supra*, *at* http://www.netdetective2001.com/court_records.html (last visited July 15, 2002). Net Detective 2001 sells for $29.00. Harris Digital Publishing Group, *supra*, *at* http://www.netdetective2001.com (last visited July 15, 2002).
165. Allen, *supra* note 161, at 731.
166. *Id.* at 735.

wrote, that the country "will begin a process of voluntary self-correction, shifting the balance toward greater respect for the privacy of public officials and aspiring officials."[167] This ray of hope implicitly recognizes that a diminution in society's self-perceived entitlement to the details of public officials' sex lives would yield a corresponding increase in the officials' expectation of privacy.

Such a renewed emphasis on privacy, however, may prove most difficult of all as it pertains to the media. Media encroachment is effectively sanctioned by the unique protection of the First Amendment. For example, the actual malice rule for defamation actions established by *New York Times v. Sullivan*[168] also applies to actions for false light invasion of privacy.[169] When the media reports on a matter of public concern, a plaintiff in a false light claim must prove not only that the publicity would be highly offensive to a reasonable person, but also that the publication contained a "knowing or reckless falsehood."[170] Similarly, the First Amendment prevents suits against the media for publication of private facts, so long as the facts were true and of public significance, and the press did not violate the law to obtain them.[171] In *Florida Star v. B.J.F.*, the plaintiff sued a newspaper for identifying her as a victim of a sexual assault.[172] Florida law prohibited police departments from allowing publication of sexual offense victims' names and prohibited the newspaper from publishing the names.[173] The police, however, mistakenly included the plaintiff's name in a copy of a police report sent to the pressroom, and the newspaper published her name.[174] The Court found for the newspaper because the report was true, the newspaper itself did not obtain the name illegally, and the statute prohibiting publication was not necessary to serve a compelling state interest.[175]

---

167. Allen, *supra* note 151, at 1181.
168. 376 U.S. 254 (1964).
169. Time, Inc. v. Hill, 385 U.S. 374, 390 (1967).
170. *Id*. at 390; *see also* RESTATEMENT (SECOND) OF TORTS § 652E (1977).
171. *See generally* Fla. Star v. B.J.F., 491 U.S. 524 (1989); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (holding that where a newspaper obtained rape victim's identity from publicly available judicial records, First Amendment barred invasion of privacy claim for publication of rape victims' identity).
172. *Florida Star*, 491 U.S. at 527–28.
173. *Id*. at 526. The newspaper's own internal policy also prohibited printing the names of rape victims. *Id*. at 528.
174. *Id*. at 527.
175. *Id*. at 537–40. Many commentators feel that the tort for public disclosure of private facts has been rendered a dead letter. *See, e.g.*, Rodney A. Smolla, *Privacy and the First Amendment Right To Gather News*, 67 GEO. WASH. L. REV. 1097, 1101 (1999)

The Court recently extended this rule even further. In *Bartnicki v. Vopper*, the Court held that the First Amendment prohibited a suit against a radio station that aired an illegally recorded tape of a cell phone conversation.[176] The Court held that the radio station merited First Amendment protection because, although it knew the tape had been illegally recorded, the station itself did not participated in or solicit the illegal recording.[177]

Some commentators suggest that the actual malice rule is unnecessary for defamation actions, and that revoking the rule's protection would not change the media's editorial decisions or reporter's conduct.[178] If special First Amendment protections are similarly unnecessary in invasion of privacy claims, then they serve only to subsidize the media's encroachment on privacy.

C. Unintended Consequences

In *The Economy of Ideas*, cyberspace visionary John Perry Barlow invoked the aphorism that "information wants to be free."[179] For Barlow, this positive affirmation recognized "the natural desire of secrets to be told."[180] His implication was that, as the Internet replaced the old world order of static media, copyright could have no hold on the "liquid works of the future," comprised purely of ideas that constantly

---

(stating that the tort "often seems to exist more 'in the books' than in practice"); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 351 (1983) ("The process of defining 'newsworthy' information has practically destroyed the private-facts tort as a realistic source of a legal remedy.").

176. Bartnicki v. Vopper, 532 U.S. 514, 535 (2001).

177. *Id.* at 525.

178. *See, e.g.*, Frederick Schauer, *Uncoupling Free Speech*, 92 COLUM. L. REV. 1321, 1328–34 (1992). Schauer questioned the empirical assumption on which the actual malice rule is based—without the heightened protection of the actual malice rule, the financial risk of defamation lawsuits will impair the media's editorial judgment. He also noted the distributional inequity of heaping upon a select few plaintiffs the cost of a social good like free expression, and explored ways to reallocate the costs of free speech. *Id*. at 1336–48.

179. John Perry Barlow, *The Economy of Ideas*, WIRED NEWS, Mar. 1994, *at* http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html (last visited March 29, 2001). Stuart Brand is credited with originating this maxim at the first Hackers' Conference in 1984, where he said:

> On the one hand information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So you have these two fighting against each other.

Id. Roger Clarke, *Information Wants to Be Free*, *at* http://www.anu.edu.au/people/Roger.Clarke/II/IWtbF.html (last modified Feb. 24, 2000).

180. Barlow, *supra* note 179.

"evolve to fill the empty niches of their local environments" and struggle to "be free."[181] Privacy advocates, however, may come to lament an important corollary to Barlow's axiom. Because of information's tendency toward expansion, its desire to be free, information collected by one person for one purpose will inevitably be used by others and for other purposes.

We can express information's desire to be free in economic terms. Information is nonrivalrous, so an actor that collects information can share that information with unlimited others and still use it for its original purpose.[182] Information is inexpensive to transmit, so an actor with large stores of data can share that data internally or externally at very low cost.[183] And information is nonexcludable, so an actor that maintains a database must expend substantial resources to prevent unauthorized parties from learning about the information.[184] Nonexcludability applies not only to outsiders, but also to insiders who are not authorized to access the information.[185]

The foregoing properties of information set the stage for unintended consequences that increase the ultimate effect of any particular encroachment. Information collected by one actor will inevitably find its way into someone else's hands, either through willful transfer of the information to a new use or a third party, or through accidental disclosure to a third party or unauthorized insider. We may think of these unintended consequences of data collection as externalities, which economists define as costs or benefits from an exchange that do not fall upon or accrue to the parties to that exchange.[186] The initial encroacher pays (in such currencies as money, political capital, or goodwill) only for the immediate cost of the encroachment, but does not bear the cost of subsequent unintended consequences. Because these unintended consequences are generally speculative at the time of the initial encroachment, individuals find it difficult to use the

181. *Id*.
182. *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 126 (3d. ed. 2000).
183. *See id*.
184. *See id*.
185. *See* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 632 (1980) ("Regulation of the information flows *within* an enterprise is difficult because of the very intangibility of many forms of information flows.").
186. *See* COOTER & ULEN, *supra* note 182, at 40; PINDYCK & RUBINFELD, MICROECONOMICS 592–93 (5th ed. 2001).

unintended consequences to argue against the encroachment.

1. Secondary Use

Secondary use occurs when an actor collects data or institutes a surveillance technique for one purpose, and the data or the surveillance technique are used by other actors or for other purposes. A classic example of secondary use is the proliferation of the Social Security number (SSN). Congress originally created the SSN in 1935 with assurances that it would be used solely to identify citizens' retirement accounts.[187] In 1943, the Roosevelt administration reasoned that it would be wasteful for other government agencies to develop their own identifying systems, and ordered agencies developing such systems to use the SSN.[188] By 1967 the Department of Defense, Internal Revenue Service, and Civil Service Commission all adopted the SSN to track people in their systems.[189] Starting in the 1970s, government use of the SSN exploded. By 1998 the Secretary of Health and Human services recognized that the SSN was "in such extraordinarily wide use as to be a de facto national identifier."[190]

Not only did the state and federal governments adopt the SSN, but private actors embraced the number as well. A vast array of businesses use the SSN, including information brokers, credit bureaus, collection agencies, banks, credit card companies, utilities, landlords, health care providers, and insurers.[191] As one commentator observed, "SSN use is so important to business and government in this country that a person who is assertive about their [sic] privacy rights may find herself in a position in which another will

---

187. H.R. REP. NO. 106-996(I) (2000), *available at* 2000 WL 1604000.

> The SSN was created in 1935 for the sole purpose of tracking workers' earnings so that Social Security benefits could be calculated upon retirement or disability. . . . Because a unique SSN is assigned to each individual, the number is commonly used as a personal identifier, although it was never intended for this purpose.

Id.; *accord* Charlotte Twight, *A Constitutional Counterrevolution*, IDEAS ON LIBERTY, Oct. 2000, at 15, 20.

188. GARFINKEL, *supra* note 73, at 20.

189. *Id*. at 33.

190. U.S. DEP'T OF HEALTH & HUMAN SERVS., UNIQUE HEALTH IDENTIFIER FOR INDIVIDUALS: A WHITE PAPER § III.A.1, *available at* http://www.epic.org/privacy/medical/hhs-id-798.html (July 2, 1998); *see also* Charlotte Twight, *Watching You*, 4 INDEP. REV. 165, 169 (1999).

191. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, PUB. NO. GAO/HEHS-99-28, REPORT TO THE CHAIRMAN, SUBCOMMITTEE ON SOCIAL SECURITY, COMMITTEE ON WAYS AND MEANS, HOUSE OF REPRESENTATIVES: GOVERNMENT AND COMMERCIAL USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD 3, 7–10 (1999), available by searching GAO reports *at* http://www.access.gpo.gov/su_docs/aces/aces160.shtml?/gao/index.html (last visited Apr. 28, 2001).

refuse to do business with her unless she furnishes her SSN."[192]

Driver's license databases further illustrate the secondary use problem. Although states undoubtedly have an interest in regulating their drivers, the mere act of creating a database of drivers' personal information inevitably spurs additional uses of that information. For example, the state of Missouri sells its automobile and driver's license information to about 400 companies, mostly for marketing purposes.[193] The companies include: eye doctors seeking a list of drivers with vision restrictions on their licenses; big and tall men's clothing stores seeking drivers over a certain height; medical insurers seeking drivers who are turning sixty-five and might be interested in supplemental Medicare insurance; and automobile insurers seeking drivers whose licenses are being reinstated after a suspension.[194] One driver who applied for license reinstatement reportedly received sixteen mail offers from "high-risk" automobile insurers.[195] Missouri reportedly earned $500,000 per year selling its drivers' license information.[196] Until a new state law took effect in 2000, Ohio earned about $3 million per year selling its driver's license data to marketing companies.[197] As of 2000, the Wisconsin Department of Transportation received approximately $8 million each year from the sale of motor vehicle information.[198]

Congress passed the Driver's Privacy Protection Act ("DPPA") in 1994 to curb the disclosure of personal information from state driver's records.[199] Although the DPPA prohibited states from releasing drivers' personal information for marketing purposes without their consent, the DPPA lacked real teeth until 1999, when Congress changed the act's protection scheme from "opt-out" to "opt-in."[200] Under the opt-out scheme, a state could assume it had drivers' permission to share their

192. Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 535 (1998).

193. Rick Desloge, *State Makes $500,000 a Year Selling Personal Information*, ST. LOUIS BUS. J., Oct. 16, 1998, *available at* http://stlouis.bizjournals.com/stlouis/stories/1998/10/19/newscolumn1.html (last visited Apr. 24, 2001).

194. *Id.*

195. *Id.*

196. *Id.*

197. Andrew Welsh-Huggins, *Ohio Limits Sale of Driver Data; Marketers Can No Longer Buy Lists of Names*, CINCINNATI ENQUIRER, July 6, 2000, at C10.

198. *See* Reno v. Condon, 528 U.S. 141, 144 (2000).

199. *See id*. at 143–44.

200. *See* Driver's Protection Act of 1994, Pub. L. No. 106-69, 113 Stat. 986, §§ 350(c)–(d) (codified at 18 U.S.C. § 2721(b)(11)–(12) (2000)).

information, unless the drivers negated that permission by opting out.[201] In contrast, the opt-in scheme requires a state to assume that it *does not* have drivers' permission to share their information unless the drivers provide express consent.[202] In the month after Ohio implemented its opt-in law, only a handful of drivers opted in.[203]

Some states use the existing infrastructure surrounding the driver's license to collect new types of information. As of May 2000, five states required a fingerprint when a person obtained a driver's license.[204] Missouri officials recently considered printing personal information, including medical and financial information, on the backs of driver's licenses.[205] Although the DPPA would restrict nonconsensual disclosure of such data for marketing purposes, the DPPA makes numerous exceptions for use by debt collectors, use in connection with a lawsuit, and use by a state, federal or local governmental agency "carrying out its functions."[206]

Whenever the government develops a new technology, secondary uses are sure to follow. A prime example is Global Positioning System (GPS) technology. The Department of Defense developed the GPS system in the early 1970s as a satellite-based positioning and navigation system.[207] The GPS system transmits precise information about three-dimensional position, velocity and time, and provides that information consistently to anyone equipped with a GPS receiver.[208] Additionally, military units using GPS can avoid detection because they need only receive the satellite signals, rather than transmit a signal of their own.[209] GPS can also provide precise guidance and targeting information for missiles.[210]

---

201. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099, Title XXX, § 300002(a), § 2721(b)(11) (1994).

202. *See* Driver's Privacy Protection Act of 1994, Pub. L. No. 106-69, 113 Stat. 986, §§ 350(c)–(d) (codified at 18 U.S.C. § 2721(b)(11)–(12)).

203. Welsh-Huggins, *supra* note 197, at C10.

204. *Morning Edition: Analysis: Missouri Proposal to Include Personal Information on Driver's Licenses Prompts Controversy* (National Public Radio, May 29, 2000) (Missly Shelton reproting), *available at* 2000 WL 21480377.

205. *Id.*

206. 18 U.S.C. § 2721(b).

207. DOD/DOT Task Force on Global Positioning System (GPS), *Increased Civil Participation*, § 1.2 [hereinafter DOD/DOT Task Force], *available at* http://www.fas.org/spp/military/program/nav/tf-rpt.htm (Dec. 21, 1993). For a brief but effective explanation of how the GPS system works, see Alan Zeichick, *GPS Explained; How the Global Positioning System Lets You Know Where You Stand*, RED HERRING, Jan. 30, 2001, at 80–81, *available at* 2001 WL 2879912.

208. Zeichick, *supra* note 207, at 80–81.

209. DOD/DOT Task Force, *supra*, § 1.4.1.

210. *60 Minutes: No Miss: Technology Enabling Missiles to Accurately Hit Targets Easily Available to Anyone Around the World* (CBS television broadcast, Dec. 26, 1993), *available at* LEXIS, News, CBS News Transcripts.

One can easily imagine a wide array of privacy-invasive GPS applications, and GPS is on the way to realizing that potential. GPS technology has made headlines for its use in cellular phones and other wireless devices. As of October 1, 2002, the FCC will require cellular telephone service networks to locate sixty-seven percent of all cellular phone calls within 100 meters, and ninety-five percent of calls within 300 meters.[211] The regulation was intended to allow tracing of emergency 911 calls and could have been satisfied by a system that required only that cellular providers design systems that tracked the user's location only when dialing 911.[212] Instead, cellular providers designed systems that broadcast the phone's location whenever the phone is turned on, turning cellular phones into continuous tracking devices that could generate substantial revenue from targeted advertising and other services. For example, as a user walked by a department store, their cellular phone could ring and deliver an ad for products in that store.[213] Or wireless users could subscribe to a service that directs them to the nearest restaurants or fast-food stores, with the restaurants paying the wireless provider for the right to be part of the service.[214] At least one cellular phone company in England is sending its subscribers special offers directing them to pubs in the area from which they are calling.[215] Law enforcement will also benefit from a requirement that cellular and other wireless carriers disclose the beginning and end call locations to law enforcement agents with wiretap authorization.[216]

GPS technology can spawn devices that monitor more than your location. A Florida company holds a patent on what it calls "Digital Angel" technology, which can track not only your location, but also your vital signs.[217] The Digital Angel runs on body heat, and could be worn as a bracelet or necklace, or even under the skin.[218] A Canadian company called AirIQ uses GPS devices to locate missing or overdue rental cars, but the company's Web site reveals far more intrusive

211. 47 C.F.R. § 20.18 (2000).
212. Froomkin, *Death of Privacy?*, *supra* note 1, at 1479.
213. Hiawatha Bray, *Something to Watch over You*, BOSTON GLOBE, Jan. 22, 2001, at C1.
214. *Id*.
215. Froomkin, *Death of Privacy?*, *supra* note 1, at 1480.
216. *Id.*
217. *All Things Considered, Commentary: Chipification,* (National Public Radio Broadcast, Jan. 25, 2001) (Katharine Mieszkowski reporting), *available at* 2001 WL 9433350.
218. *Id*.

uses.[219] "[A] vehicle can be disabled or enabled and the doors can be unlocked with the point and click of a mouse."[220] A Connecticut rental car company has been using AirIQ to track the driving speeds of its rental car customers and issuing fines to customers who speed.[221] As of July 2001, more than twenty-five customers had called the Connecticut Department of Consumer Protection to complain about the speeding fines.[222]

As the GPS example illustrates, the way in which a data-collection system is designed can affect the risk of secondary uses. Increasingly popular automated highway toll collection systems allow drivers to pass through toll booths without stopping to pay an attendant or drop change in a bin.[223] Each vehicle carries a transponder that signals the toll collection system when it passes through the tollbooth. These systems *could* be designed so that they simply deducted the necessary toll from the account holder's toll balance card. Passing through a toll lane would not involve the exchange of any data identifying the owner.[224] Instead, these systems have generally been designed so that the transponders emit unique codes that identify the owner. The first type of system would protect drivers' privacy, but would require an alternative way to charge drivers whose toll-balance cards have insufficient funds.[225] One alternative would be to photograph the license plate of any car that registers insufficient funds as it goes through the tollbooth. This would be less intrusive than the system that identifies the vehicle at each toll, which creates a vast database of vehicles' movements.[226]

By choosing a system that can track where and when specific vehicles pass through specific toll booths, the government creates a potential gold mine of secondary use data for anyone who might someday like to learn where you have been. Law enforcement is already exploiting this new source of information. New York law enforcement agencies have already used New York's E-Zpass records in dozens of criminal prosecutions.[227] Massachusetts authorities recently obtained a court order—over the turnpike authority's objections—requiring the Turnpike Authority to

---

219. *See* Stephanie Stoughton, *Watching You Watching Them*, BOSTON GLOBE, July 9, 2001, at C1, *available at* 2001 WL 3941635.

220. AirIQ, Inc., *About AirIQ*, *available at* http://www.airiq.com/airiqnewweb/content.cfm?ChapterID=11&PageID=67=58&SegmentID=99 (last visited Nov. 6, 2001).

221. Stoughton, *supra* note 219, at C1.

222. *See id.*

223. *See* Froomkin, *Death of Privacy?*, *supra* note 1, at 1529–30.

224. *Id* at 1530.

225. *Id*.

226. *Id*.

227. Ross Kerber, *MTA Gives Court Toll-Use Data*, BOSTON GLOBE, Aug. 13, 2001 at C4, *available at* 2001 WL 3946550.

disclose a motorist's Fast Lane records for use in a grand jury proceeding.[228] The judge also refused the Turnpike Authority's request to notify the motorist of the disclosure.[229] The Turnpike Authority's Fast Lane program terms explain that it "shall hold all customer account information confidential."[230] Other parties interested in automated toll collection system data may include such diverse groups as social service agents tracking where parents take their children, auto insurers estimating how far insured vehicles travel, and divorce lawyers trying to expose cheating spouses.

Grocery store loyalty cards present another example of secondary uses. These cards offer shoppers "rewards" in the form of slightly lower prices on certain items when they present their cards at the checkout counter. By presenting the card, however, the shoppers allow the grocery store to record every item that they purchase.[231] The card not only helps the store enhance its inventory and advertising efforts, but also to sell its customers' data to third parties. Law enforcement may also take an interest in such data, as occurred when the Utah Drug Enforcement Agency subpoenaed customers' purchase records to see whether suspected drug dealers were buying unusual amounts of sandwich bags.[232] And health or life insurers may be interested in whether a prospective insured buys yogurt or yodels, or whether a diabetic buys sugary snacks.

Similarly, the vast online profiles compiled and shared by Internet marketers could find their way into law enforcement's hands. Law enforcement agents can easily consult any company that kept a Web surfing profile on a particular user, and gather all of the clickstream data recorded in that profile. They need only find out a suspect's IP address—which can be done in any number of ways, including sending an e-mail with an embedded Web bug[233]—to give them a starting point to search for all of that suspect's clickstream data that profilers have compiled.[234]

---

228. *Id.*
229. *Id.*
230. *Id.*
231. *See* Matt Beer, *Club Cards, Bargains and Privacy in Peril*, S.F. EXAMINER, Oct. 11, 1999, at D1.
232. Carl M. Cannon, *Ambushed: A Laundry List of Hot Digital Issues Awaits George W. Bush*, FORBES ASAP, Feb. 19, 2001, at 47, 49.
233. Privacy Foundation, *Privacy Watch: New Proposal: Make Web Bugs Visible*, *available at* http://www.privacyfoundation.org/privacywatch/report.asp?id=40&action=0 (last visited Apr. 18, 2002).
234. *See All Things Considered, Analysis: Internet Privacy in Regards to*

2. Inadequate Security of Personal Information

A second form of unintended consequences flows from the failure to protect data adequately. Hackers pose perhaps the most highly publicized security threat to personal information in government and business databases. In early 2001, an organized ring of hackers stole over a million credit card numbers from commercial Web sites.[235] Operating mostly from Russia and the Ukraine, the hackers exploited a well-known vulnerability in Microsoft's Windows NT operating system.[236] The hackers tried to blackmail businesses by threatening public embarrassment if the companies did not pay them or hire them as security consultants.[237] When companies ignored their demands, the hackers posted tens of thousands of credit card numbers online.[238] Microsoft has made free "patches" available online to fix the vulnerability.[239] However, even when software makers identify vulnerabilities, the companies using such software often devote insufficient attention to ongoing security issues. According to a former Defense Department security officer, "many of the people who hastily constructed Web sites during the past few years assumed that putting commercially available electronic firewalls around their systems would protect them."[240]

Hackers have also exploited security weaknesses at major credit reporting agencies such as Equifax and Experian, stealing consumers' credit report data.[241] And the government is not immune from hackers. The federal government reported that 155 computers in thirty-two federal agencies were temporarily taken over by hackers in 2000, up from 110 computers in 1999.[242] Officials warned that only about one in five hacking incidents are even detected.[243] The General Accounting Office reported in March 2001 that it had successfully hacked into Internal Revenue Service computers which store sensitive data, including electronically filed tax returns.[244] The GAO report "demonstrated that

---

Information Collected by Web Sites Without the Knowledge of the User, (National Public Radio, Apr. 5, 2000) (interview with Richard Smith, President, Privacy Foundation), *available at* 2000 WL 21470303 [hereinafter, *All Things Considered: Internet Privacy*].

235. Ariana Eunjung Cha, *Hackers Feast on Complacency: Security Holes Well Known*, WASH. POST, Mar. 9, 2001, at E1.

236. *Id.*

237. *Id*.

238. *Id*.

239. *Id.*

240. *Id*.

241. Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847, 851 (1998).

242. D. Ian Hopper, *US Government Computers Seen as Prey to Foreign Hacking*, BOSTON GLOBE, Apr. 6, 2001, at A35.

243. *Id*.

244. Declan McCullagh, *Xenu Do, But Not on Slashdot*, WIRED NEWS, Mar. 17,

unauthorized individuals, both internal and external to IRS, could have viewed and modified electronically filed taxpayer data on IRS computers."[245]

Hacking is not the only way for outsiders to exploit weaknesses in the security of personal information. Companies often make personal information available to more employees than necessary, because tighter restrictions would increase their costs. Health care providers, for example, allow many employees to access patients' medical records, most of whom have no medical need to do so.[246] Though this may allow the providers to work more efficiently, it also puts patient privacy at risk. One woman who checked into a hospital was promised confidentiality regarding her AIDS-related illness.[247] Although she shared her condition only with her doctors and close family, an acquaintance of the woman worked as a secretary at the hospital, and was able to read the woman's medical records on her computer.[248] The secretary shocked the woman by stopping by to express her concerns about her condition, and told a neighbor of the woman's condition as well.[249]

Privacy is also at risk from accidental disclosures by government and businesses, even of the most sensitive information. In an ironic and embarrassing gaffe, Justice Department workers trying to assuage privacy concerns over Carnivore accidentally disclosed information about the supposedly secret team of researchers hired to conduct a Carnivore independent review.[250] In September 2000, the Justice Department posted online a PDF file containing a report by the independent review team.[251] The document contained thick black bars to

2001, *at* http://www.wired.com/news/print/0,1294,42486,00.html (last visited Apr. 23, 2002).

245. *Id.*

246. *See* CHARLES J. SYKES, THE END OF PRIVACY 102 (1999) (describing widespread but routine sharing of patients' medical information among players in health care bureaucracy, including HMOs, insurance companies, hospital workers, pharmacists, pharmaceutical companies, and employers); AMITAI ETZIONI, THE LIMITS OF PRIVACY 164–74 (1999) (proposing a variety of ways to restrict unnecessary access to patients' health care information).

247. SYKES, *supra* note 246, at 107.

248. *Id*.

249. *Id.* Ironically, some hospital employees are prone to snooping into each other's medical records, as demonstrated when one hospital administrator became a patient in her own hospital, and two hospital employees were caught reviewing her records. *Id.* at 106.

250. Declan McCullagh, *Carnivore Review Team Exposed!*, WIRED NEWS, Sept. 27, 2000, *at* http://www.wired.com/news/print/0,1294,39102,00.html (last visited Apr. 23, 2002).

251. *Id.*

conceal the names, telephone numbers, and government security clearances of the review team.[252] However, "anyone with Adobe-supplied software—or a text editor and a little bit of time—can view the unaltered document."[253] That same day, an unaltered version of the document appeared on the Web site of Cryptome.org.[254] The unmasked information revealed that members of the review team enjoyed a close relationship with the Clinton administration and held active top secret security clearances.[255]

Accidental disclosures of financial and medical information have become alarmingly frequent. In 1997, Experian abandoned an online credit report feature after it accidentally misdirected 2000 reports.[256] Drug manufacturers Eli Lilly & Co. and Kaiser Permanente inadvertently divulged confidential medical information in misdirected e-mails.[257] In one of the most egregious examples, someone at the University of Montana, apparently by accident, posted detailed psychological records of over sixty children and teenagers on its Web site.[258] The records described information that patients revealed during therapy, as well as the therapists' diagnoses. University officials said a student or technical employee may have accidentally posted these files on the Web site,

---

252. *Id.*

253. *Id*.

254. *Id*. The unaltered document is posted on the Cryptome.org Web site, *at* http://cryptome.org/carnivore-mask.htm (last visited July 22, 2002). The Cryptome.org site contained an anonymous poster's explanation of how the poster noticed the Justice Department's mistake: "Have you seen the DoJ announcement of the Carnivore review team? The winning proposal . . . has most of the names blacked out—but during the display, I noticed that the overwritten stuff is at the PDF level; I could briefly see some of the names during the screen-painting." Posting of Anonymous, to JYA@pipeline.com (Sept. 26, 2000), *at* http://cryptome.org/carnivore-mask.htm. Cryptome.org explained the flaw in more detail:

> Cryptome has confirmed that digital overwrites in the Carnivore review proposal can be unmasked by copying and pasting the PDF text or by using an Adobe plug-in, such as Pitstop, to remove overwriting. This cloaking is weaker than a similar technique used by the New York Times for cropping text of the secret CIA report on Iranian Premier Mossadeq's 1953 overthrow: http://cryptome.org/cia-iran.htm.
>
> In addition, the participants' resume names are pseudonyms of "He" or "She," some of which can be replaced with possible true names by comparison with other information in the proposal and online sources.

Cryptome.org Web site, *at* http://cryptome.org/carnivore-mask.htm. The altered document, black bars and all, may be found in IIT RESEARCH INSTITUTE, TECHNICAL PROPOSAL: INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE ELECTRONIC COMMUNICATION COLLECTION SYSTEM, *available at* http://www.usdoj.gov/jmd/pss/iitritechnicalproposal.pdf (Sept. 20, 2000).

255. McCullagh, *supra* note 250.

256. Budnitz, *supra* note 241, at 854.

257. Charles Piller, *Web Mishap: Kids' Psychological Files Posted*, L.A. TIMES, Nov. 7, 2001, at A1.

258. *Id.*

where they remained for eight days, until a local newspaper reported the story.[259] The University's attorney said that accidental online disclosures of private medical information are not unusual and are quickly corrected.[260]

Identity theft is a lucrative business for thieves in part because credit card companies have not devised an effective way to verify the identity of mail-in or telephone applicants.[261] Credit card companies could minimize the number of innocent victims of identity theft simply by restricting the issuance of new cards to verified applicants.[262] They simply choose not to, because that would hinder their ability to generate new customers.[263]

Finally, privacy is always threatened by dishonest or corrupt individuals with access to personal information held by governments or businesses. Access to the government's vast information resources can be sorely tempting. Politicians and bureaucrats have used, and will continue to use, our personal information for their personal or political gain. Stories of J. Edgar Hoover's elaborate files are legendary.[264] In 1963, President Kennedy authorized the IRS to send citizens' tax returns to the House Committee on Un-American Activities upon the committee's request.[265] In 1970, a former military intelligence agent revealed that he had "helped compile a card file on 5000 to 8000 residents of the St. Paul, Minnesota, area who had opposed the Vietnam War."[266] The Senate Judiciary Subcommittee on Civil Rights later discovered that the St. Paul file was "just one part of a sprawling government surveillance project, in which dossiers on hundreds of thousands of U.S. citizens were compiled by the Military Intelligence

259. *Id.*
260. *Id.*
261. GARFINKEL, *supra* note 73, at 31.
262. *See id.*; *see also* Miguel Bustillo, *Victim Tells Senate Panel of Identity Theft*, L.A. TIMES, May 3, 2000, at A3 (discussing California bill that would prevent companies from sending preapproved credit cards to consumers).
263. *See* GARFINKEL, *supra* note 73, at 32 ("Ultimately, identity theft is flourishing because credit-issuing companies are not being forced to cover the costs of their lax security procedures. The eagerness with which credit companies send out preapproved credit card applications creates the risk of fraud.").
264. *See, e.g.*, Orr Kelly, et al., *The Secret Files of J. Edgar Hoover*, U.S. NEWS & WORLD REP., Dec. 19, 1983, at 45 (stating that Hoover's files corroborated ex-Hoover aides' reports that Hoover "drew on the wealth of defamatory information at his fingertips to curry favor with Presidents and other officials and used the bureau's resources to intimidate persons who criticized him or the FBI.").
265. *Nothing Sacred*, *supra* note 80, at 2.
266. *Id.* at 12.

Command headquarters at Fort Holabird, Maryland."[267] The Wall Street Journal Board of Editors quotes President Richard Nixon in 1971 as saying he intended to select an IRS commissioner who "is a ruthless son of a bitch, that he will do what he's told, that every income tax return I want to see I see, that he will go after our enemies and not go after our friends."[268] According to some reports, President Clinton "apparently sanctioned the illegal transfer of nine hundred or more FBI files to the White House," possibly for political reasons.[269]

Congress and the White House have no monopoly on such abuses of power. The Internal Revenue Service has been plagued with employees browsing through the confidential tax records of friends, relatives, and celebrities. An IRS internal audit documented browsing in 1515 cases during fiscal years 1994 and 1995.[270] One IRS employee was acquitted on charges for browsing through tax records of Elizabeth Taylor, Lucille Ball, Tom Cruise, Elvis Presley, and other celebrities.[271] In another case, a Ku Klux Klan member working for the IRS browsed through the records of "suspected white supremacists, a family adversary, and a political opponent."[272]

Such abuses are not limited to government employees. A Columbia University professor estimates that some emergency room employees make more money forwarding patient information to unscrupulous lawyers seeking clients than they do from their paychecks.[273] And when singer Tammy Wynette checked into a hospital in 1995, a hospital employee provided details of her medical condition to the *National Enquirer*, which ran a story about her hospitalization.[274] By its nature, by its desire to be free,[275] centralized information is vulnerable to abuse by anyone who can access it.

IV. FAILURE OF MARKETS AND THE POLITICAL PROCESS

Part IV examines why the encroachment on privacy often faces little meaningful opposition. If individual consumers, employees, and citizens could unite to oppose the encroachment, they might preserve

267. *Id.*
268. *Review & Outlook, Politics and the IRS*, WALL ST. J., Jan. 9, 1997, at A12 (quoting then-President Richard M. Nixon; *see also* Twight, *Watching*, *supra* note 190, at 196).
269. Twight, *supra* note 190, at 196.
270. *See* Stephen Barr, *IRS Audit Reveals More Tax Browsing: 23 Fired, Hundreds Disciplined by Agency*, WASH. POST, Apr. 9, 1997, at A1.
271. *Id*.
272. *Id*.
273. SYKES, *supra* note 246, at 106.
274. *Id*. at 107.
275. *See generally* Barlow, *supra* note 179.

their expectation of privacy. Numerous factors, however, conspire against such solidarity.

A. Market Failures

The ideal of the free market allocating goods efficiently rests on assumptions that often prove false in practice. Markets may function inefficiently because of informational asymmetries, unevenly distributed bargaining costs, and disparities in bargaining power.[276] Moreover, market failure is exacerbated by collective action problems that prevent customers from uniting to oppose the encroachment.[277]

Paul Schwartz characterized the ideal privacy market as one that requires companies to engage in "privacy price discrimination."[278] In traditional economic terms, price discrimination entails the seller selling goods at different prices to different purchasers, depending on the elasticity of their demands for her product.[279] Privacy price discrimination, then, would require companies to differentiate in the way they collect and use data about different individuals in accordance with those individuals' preferences about the use of their data.[280] The current state of affairs does not approach this ideal model. Instead, due to pervasive market failures, companies can buy privacy valuers' and non-privacy-valuers' data for the same price, so they do not pay the true cost of personal data.[281] The reality, then, is that consumers in the current privacy market cannot adequately claim the privacy they desire, and therefore cannot mount meaningful opposition to the encroachment on privacy.

---

276. *See* COOTER & ULEN, *supra* note 186, at 38–43; PINDYCK & RUBINFELD, *supra* note 186, at 591–93, 595–602; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1395 (2000).

277. Schwartz, *supra* note 132, at 31 (citing CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 153–55 (1997)).

278. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 832 (2000).

279. RICHARD A. POSNER, 305 (5th ed. 1998), (cited in Schwartz, *supra* note 278, at 832).

280. Schwartz, *supra* note 278, at 832–33.

281. *Id*. at 833. For an "analysis of the flaws of combining strong market power and price discrimination," Schwartz directs the reader to Wendy J. Gordon, *Intellectual Property as Price Discrimination: Implications for Contract*, 73 CHI.-KENT L. REV. 1367, 1384 (1998). Schwartz, *supra* note 278 at 833 n.80.

1. Informational Asymmetry

When buyers know more about certain products or transactions than sellers, or vice versa, information is distributed asymmetrically in the market.[282] Severe asymmetries "can disrupt markets so much that a social optimum cannot be achieved by voluntary exchange."[283] For example, house buyers are often at a severe informational disadvantage compared to house sellers, who are more likely to know of latent defects in the house.[284] This informational asymmetry leads to market inefficiency, because buyers may pay more than homes are worth, or may inefficiently refrain from buying out of fear of latent defects.[285] Both types of inefficiency—overpayment and underparticipation—are prevalent in today's privacy marketplace. Many consumers participate in transactions without any knowledge that merchants are gaining a valuable commodity—their personal information or transactional data—for free.[286] Other consumers refuse to buy any goods or services online because of privacy fears. A Forrester Research survey found that in the year 2000, privacy fears prevented consumers from spending $12.4 billion on e-commerce.[287]

a. Lack of Knowledge About Information Collection Practices

The most basic information deficiency is individuals' ignorance of data collection and surveillance practices. The free market theory presupposes that consumers make informed choices when they decide with whom to share certain information.[288] The reality, however, does not approach this ideal assumption. Consumers are generally unaware of the variety of ways that businesses collect information about them.

The world of online profiling offers several examples. Broadly speaking, online profiling can mean collecting information anonymously to create targeted advertising, or it can mean merging clickstream data with

---

282. COOTER & ULEN, *supra* note 186 at 43.
283. *Id*.
284. *Id*.
285. *Id*. States have responded by requiring house sellers to disclose knowledge of any latent defects to prospective buyers. *Id.*
286. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1072–73 & n.202 (1999).
287. Anthony Shadid, *Crackdown Seen on Customer Databases*, BOSTON GLOBE, Jan. 8, 2001, at C1.
288. *See* COOTER & ULEN, *supra*, note 186, at 38–43; PINDYCK & RUBINFELD, *supra* note 186, at 591–96; Eli M. Noam, Ph.D., *Privacy in Telecommunications: Markets, Rights, and Regulations Part III: Markets in Privacy*, *reprinted in* NEW TELECOM QUARTERLY, Fourth Quarter 1995, at 53, *available at* http://www.tfi.com/pubs/ntq/articles/view/95Q4_A9.pdf (last visited Apr. 29, 2001).

personally identifiable information.[289] When you visit a Web site, that site can surreptitiously collect data such as your computer's IP address, the type and version of browser you use, your computer type, your activities during your last visit to the Web site, and your activities on other Web sites.[290] The Web site can also track the pages and images you download at the site, the time of those downloads, the data you enter, the cookies on your computer, and the referring Web page—the page where you clicked on the link that sent you to the current Web page.[291] This clickstream data "is a potentially rich source of information about your habits of association, speech, and commerce."[292] Someone who reviews your clickstream data can approximate the experience of watching over your shoulder while you surf the Web, with the added benefit of being able to sort through all your data and select only the data interesting to them.

Web sites gather personal data in a wide variety of ways, many of which are unknown to most Internet users. The most publicized method involves cookies—small text files that Web sites write directly to your hard drive without your notice or consent.[293] Cookies can contain a variety of information, such as login or registration information, online "shopping cart" information, and your preferences and interests.[294] Cookies are widely used to "facilitate the tracking of specific individuals' activities in order to customize content and advertisement."[295]

Even more difficult to detect than cookies are Web bugs, which are part of a Web site's source code.[296] Unlike cookies, which must be

289. *See* CDT's Guide to Online Privacy, *Getting Started: Online Tracking FAQ*, *at* http://www.cdt.org/privacy/guide/start/track.html (last visited Jan. 24, 2001).

290. *Id.* Privacy.net has established a demonstration of the information that Web sites can collect about you. When visited from the author's home computer, simply by clicking on the link to privacy.net/analyze, the site learned the following about the author's computer: IP address; browser type and operating system; the number of Web pages visited in the current session and window; the date and time registered; the names and versions of various plug-ins installed, such as ShockWave Flash, Real Player, Media Player, and Adobe Acrobat; the precise route of "hops" from one IP address to another by which the author's computer found the Web site; the name of the author's Internet service provider; and much more. *See* Privacy.net, *Privacy Analysis of Your Internet Connection*, *at* http://www.privacy.net/analyze (visited March 19, 2001).

291. CDT's Guide to Online Privacy, *supra* note 289.

292. *Id*.

293. *Id*.

294. *Id*.

295. *Id*.

296. Todd R. Weiss, *Privacy Group Warns of 'Web Bugs'*, PCWORLD.COM, Sept. 15, 2000, *at* www.pcworld.com/resource/printable/article/0,aid,18474,00.asp (last visited

physically written to a user's hard drive, Web bugs hide within the HTML code of a Web page.[297] They usually exist on the Web page as a graphic element about the size of a period, and are therefore invisible to users.[298] Users are essentially defenseless against these bugs, because Internet browsers do not contain any features to disable Web bugs.[299] Despite their small size, these bugs can convey a wealth of information. When you surf to a Web page containing a bug, the bug can send the following information "home" to the company that planted it: the IP address of your computer; the URL of the Web page you are visiting; the URL of the Web bug image itself; the time you triggered the Web bug; the type of browser you use; and any of the information in the cookies already on your hard drive.[300] Web bugs can also be planted in e-mail messages.[301] Such bugs can tell the planter whether and when a message was read.[302] If a recipient tries to remain anonymous, the Web bug can relay the IP address of the recipient's computer.[303] Users cannot stop Web bugs from collecting and relaying information about them or their computers.[304] Their best defense against Web bugs is to use their browsers, or other more complicated measures, to block the placement of cookies on their computers.[305] This at least denies Web bugs access to some information about users' surfing habits.[306] In keeping with the covert nature of Web bugs, Web site privacy policies rarely disclose the use of Web bugs.[307]

March 12, 2001).

297. *Id.*

298. *Id*.

299. *Id*. Internet Explorer and Netscape Navigator both incorporate options to reject some or all cookies, but activating these mechanisms can make Web surfing less efficient. Some Web sites either refuse access to users who do not accept cookies, or make several attempts to place each cookie—with each attempt causing an intrusive dialog box to pop up and ask the user to accept the cookie.

300. Richard M. Smith, *FAQ: Web Bugs, Privacy Foundation*, *available at* www.privacyfoundation.org/education/webbug.html (last visited March 12, 2001).

301. *Id*.

302. *Id*.

303. *Id*.

304. *Id*. That may soon change. The Privacy Foundation has created a Web bug detector that it calls Bugnosis. *See* The Privacy Foundation, *Bugnosis*, *at* http://www.bugnosis.org/ (last visited July 23, 2002). Bugnosis, which currently works only with Internet Explorer, analyzes every Web page that a user visits and alerts the user when the program discovers a Web bug. *See* Bugnosis, Web Bug FAQ, *at* http://bugnosis.org/faq.html#bugnosis%20basics (last visited July 23, 2002). Though the current version of Bugnosis is merely a detector, the arms race in privacy-related technology may well spawn a Web bug "exterminator."

305. *See* Smith, *supra* note 300.

306. *See id*.

307. *See id*. For a demonstration of how a Web bug monitors who accesses a particular Web page, visit *Webbug 2000s Profile*, *at* http://profiles.yahoo.com/webbug2000. Richard Smith of the Privacy Foundation planted a Web bug on this page, but made the

Data profilers also use surreptitious programs referred to beneficently as "phone home programs" and more critically as "spyware." When online game player Robert Ellsworth noticed persistent delays while he played the game "Everquest: The Scars of Velious," he suspected that personal data was being surreptitiously copied from his computer. Using a "sniffer" to monitor all data leaving his computer, he learned that the game's host, a division of Sony Online Entertainment, was using a spyware program to collect information about the other applications running on his computer.[308] These programs are small applications often found embedded in software. They can serve beneficial purposes, like automatically verifying that the user has the latest software patches and versions. But they can also "extract information about users, their Internet browsing habits or their PC's configuration, and transmit the information to a Web site when the user is online."[309] Companies using these programs can gather personal information from you while you surf the Web, and sell that information to advertisers.[310] Users are usually unaware of the covert data collection, though their existence may be noted somewhere in the fine print of the "clickwrap" software licenses which users almost uniformly ignore.[311] Moreover, privacy expert Richard Smith observes that it would be difficult for most users to understand exactly what these programs do based on a description in a program's contractual terms or privacy policy.[312] Software vendors are increasingly turning to these types of programs. The list of past and present spyware users includes prominent players such as Microsoft, Netscape, RealNetworks, and Intuit.[313]

---

bug visible for purposes of illustration. The Web bug will show the host name and IP address of your computer. Additionally, the page will plant a cookie on your computer, albeit a nonidentifying one that cannot be used for tracking purposes because it assigns every visitor the same value. The visible Web bug displays the following message: "*** GOTCHA! *** I know you are at [Host name and IP address], and I just set a non-identifying cookie in your browser." *See* Smith, *supra* note 300.

308. Howard Millman, *How to Keep Vendors from Quietly Violating Your Privacy*, N.Y. TIMES, Jan. 18, 2001, at G9.

309. *Id.*

310. *See All Things Considered: Internet Privacy*, *supra* note 234.

311. Millman, *supra* note 308.

312. *See All Things Considered: Internet Privacy*, *supra* note 234.

313. Millman, *supra* note 308. According to a computer security expert quoted in the article, "In the hands of a skilled marketer, personal information gathered by a phone home applet is a virtual treasure trove. Stealth data collection is like having a telemarketer listen in on the speakerphone while you eat dinner with your family." *Id.*

b. Lack of Knowledge About Information Uses

Even if individuals were aware of all the data that companies collect about them, they would still have little idea of how those data are used, or by whom. For example, many Web sites collect names and addresses through a variety of techniques, including registration processes and sweepstakes offers.[314] Such sites do not usually highlight the consequences of registering or participating in the sweepstakes.[315] Individuals have extreme difficulty learning about the secondary and tertiary uses of their personal data.[316] Yet without specific knowledge about the identity of those other companies, and the purposes for which they may use the data, individuals cannot intelligently decide what data they should share with or withhold from the primary collector.[317]

It should not surprise anyone that data collectors are reluctant to disclose all the potential uses for the information they collect. Consumer data can be used for many purposes to which consumers probably would not agree.[318] These uses include, to name just a few: employment and health insurance decisions that "exclude or disadvantage genetic or medical 'have-nots'; employment or housing decisions based on perceived personality risks; [and] employment or housing decisions based on religious preferences."[319] "Data processors have no . . . interest in disclosing these uses, . . . because individuals are likely to find them so objectionable."[320]

2. Valuation Difficulty

Individuals are ill equipped to conduct the types of valuation decisions that market theory presumes. Michael Froomkin coined the term "privacy myopia" in reference to the valuation difficulty that consistently

---

314. *See* Murphy, *supra* note 46, at 2414 ("Many software companies allow a user the option of on-line registration of their purchase. Registration, on-line or otherwise, is marketed to the consumer as beneficial for access to support services and product updates. Incidentally, it provides the software merchant with valuable information about the consumer."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1625 (1999).

315. Schwartz, *supra* note 314, at 1625.

316. Cohen, *supra* note 276, at 1397; *see* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 54 (1993) ("[I]ndividuals are never aware of the variety of interests that will have access to personal information, nor can they imagine all the analytical and strategic uses to which this personal information may be put.").

317. Cohen, *supra* note 276, at 1397.

318. *Id*. at 1398–99.

319. *Id.* at 1399.

320. *Id*.

leads consumers to undervalue their personal information.[321] The main feature of privacy myopia is that, for marketers, aggregating large amounts of personal data produces a profile whose value exceeds the sum of each individual datum's value.[322] Consumers, however, are unaware of the increased value of aggregation.[323] So, in each exchange, the consumer will value the datum at its marginal value in terms of lost privacy, while the merchant will also include the value the datum when aggregated with other data in a profile.[324] Accordingly, the consumer will always assign data a lower value than a merchant, and the consumer will always be willing to sell data at a price a merchant will be willing to pay.[325]

Furthermore, if a consumer assigns a very small marginal value to a particular datum, the value of not disclosing that datum will usually be lower than the cost of negotiating a confidentiality clause or foregoing the entire transaction.[326] For this reason, privacy clauses usually will not appear unless the data are unusually revealing.[327] For a consumer buying an appliance, the cost of her address will probably seem trivial compared to the cost of not buying the appliance. Consumers generally make their datasharing decisions within the framework of each incremental transaction in which they participate, while merchants base their practices on the realities and economies of scale of the data profiling business.

Froomkin's privacy myopia analysis accepts, for the sake of argument, the idealized assumption that individuals can assign specific monetary values to losses of privacy. Individuals, however, cannot effectively reduce an intangible like privacy to a fixed monetary value.[328] Like other dignitary goods, privacy has "inherently nonmonetizable dimensions. These dimensions may be lost or distorted beyond recognition in the translation to dollars."[329] Merchants, however, have no trouble converting

321. Froomkin, *Death of Privacy?*, *supra* note 1, at 1502–04.
322. *Id*. at 1503.
323. *Id*. at 1503–04.
324. *Id*. at 1503.
325. *Id.*; *see also* Cohen, *supra* note 276, at 1398 (The "trivial and incremental character" of each exchange of data in the consumer context "tends to minimize its ultimate effect. A comprehensive collection of data is vastly more than the sum of its parts.").
326. *See* Froomkin, *Death of Privacy?*, *supra* note 1, at 1503–04.
327. *Id*.
328. Cohen, *supra* note 276, at 1398.
329. *Id*. at 1398 ("[M]onetary measures of value do not capture the very real

the value of personal data to dollars, because they need not consider the dignitary implications. The merchant values personal data based either on the amount for which it can sell that data to a third party, or on the benefit it can gain from using that data in its own business. Thus, in many respects the consumer and merchant are speaking different languages, yet the structure of the market forces consumers to deal entirely in the merchant's language. For consumers, something significant is lost in the translation, and that loss predisposes them to undervalue their privacy interest.

Finally, even if individuals were equipped with perfect information about the uses of their personal data, and could place an accurate monetary value on those uses, they still could not assign those data a meaningful value. People are demonstrably bad at estimating future value and discounting for present value.[330] Yet those are precisely the types of calculations required in an ideal market for privacy. Consider a hypothetical proposed transaction whose terms include the sharing of the consumer's name, telephone number, and income level. Assume that the customer has perfect knowledge of (1) the uses the merchant will make of that data, (2) the companies to whom the merchant may later sell that data, and (3) the possible uses those future buyers might make of that data. Even under these ideal conditions, the consumer cannot attach a value to her data without first estimating, based on the probability of each use and the number of uses, the value of the uses to which that data might someday be put.[331] She must next discount that value to its present value.[332] These types of calculations may be commonplace in the corporate world of risk versus benefit analysis, but they are entirely foreign to consumers registering their new stereo or registering for a Web site.

3. Imbalance of Bargaining Power and Bounded Rationality

In 1971, Arthur Miller observed that an imbalance of bargaining power would prevent individuals from successfully claiming their privacy.[333] Companies, as well as government organizations, generally have sufficient leverage to extract the data they want from people.[334] Credit bureaus, for example, can simply deny uncooperative individuals

---

incommensurabilities that the choice [whether to waive one's privacy] presents.").

330. *Id*. at 1397–98.

331. *Id*.

332. *Id*.

333. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 214 (1971).

334. *Id.*

access to the credit economy.[335] Individuals are in no position to demand promises of confidentiality with regard to their transactional data.[336] Consumers understand that they cannot persuade a company to alter its standard terms.[337] Even if some consumers were inclined to compare the standard terms for a variety of companies—on the assumption that the terms will vary among companies—the careful reading and comparison necessary to make an intelligent choice would be an arduous task, and its cost might outweigh the benefit of the transaction at issue.[338] The task is even more difficult where consumers must deal not with concrete form contracts, but with nebulous privacy policies that can be difficult even to find, let alone decipher. A recent study of sixty financial companies' privacy notices showed that, on average, the notices were written at a third- to fourth-year college reading level.[339] Literacy experts recommend that materials written for the general public be at a junior high school reading level.[340]

Behavioral economics offers another reason why individuals do not resist standard terms or practices, even when resistance might be the rational choice. Rational choice theory, which underlies traditional law and economics theory, is generally understood as either a relatively weak "presumption that individuals act to maximize their expected utility," or a relatively strong "presumption that individuals act to maximize their self-interest."[341] The burgeoning law and behavioral

335. *Id*. at 213–14.
336. *Id*.
337. Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1225 (1983).
338. *Id*. at 1226.

> When contracts of adhesion become commonplace, even the individual who reads and understands is, and may well perceive himself to be, essentially helpless. The consumer's experience of modern commercial life is one not of freedom in the full sense posited by traditional contract law, but rather one of submission to organizational domination, leavened by the ability to choose the organization by which he will be dominated.

Id. at 1229 (footnote omitted).
339. MARK HOCHHAUSER, LOST IN THE FINE PRINT: READABILITY OF FINANCIAL PRIVACY NOTICES (2001), *available at* http://www.privacyrights.org/ar/GLB-Reading.htm (last visited Apr. 10, 2002). Hochhauser evaluated the notices by using several software packages, including Prose, WStyle 1.6, Grammatik 6, Reader 1.2 and Correct Grammar 2.0. Those programs all calculated readability based on the Flesch Reading Ease Score. *Id.*
340. *Id*.
341. Russell B. Korobkin & Thomas S. Ulen, *Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics*, 88 CAL. L. REV. 1051, 1055 (2000).

science movement is exploring the ways rational choice theory fails to predict behavior.[342] "Bounded rationality" is a broad term sometimes used to encompass the variety of patterns in which individuals depart from the rational choice model.[343] Exploring the status quo bias, one aspect of bounded rationality,[344] Russell Korobkin found that individuals negotiating contracts will prefer standard form terms or legal default terms over terms they must create themselves.[345] This preference, which Korobkin also refers to as the inertia theory of contract negotiation,[346] substantially limits individuals' choices when dealing with standard terms or practices that encroach on privacy.[347]

Finally, privacy-intrusive industries can do far more than simply agree on standard terms and practices. They can develop technological standards for such products as Web browsers or wireless phones that preserve the status quo of maximum information disclosure, and even leave individuals without effective recourse to other practices or standards.[348] Individual consumers are powerless in the face of such a unified front. Perhaps they could exercise a meaningful choice if they acted collectively. But as the next Section shows, consumers face substantial collective action problems.

4. Collective Action Problems

Individuals attempting to preserve their privacy face collective action problems.[349] Mancur Olson explained that in a large group, each member can make only a small contribution to the whole, so there is a strong incentive for each to free ride on the efforts of the others.[350] In the context of consumer privacy, an individual could refuse to deal with companies that condition their goods or services on the exchange of personal information. The cost to that individual would be substantial, however, and the benefit to the whole group would be quite small. As a

342. *Id*. at 1057–58.
343. *Id*. at 1075–76.
344. *Id*. at 1111–12; Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583, 1587–88 (1998).
345. Korobkin, *supra* note 344, at 1627.
346. *Id*.
347. Schwartz, *supra* note 278, at 822–23 (citing Korobkin, *supra* note 344, at 1587–92).
348. *Id.* at 823 ("Once online industry is able to 'lock-in' a poor level of privacy on the Web as the dominant practice, individuals may not have effective recourse to other practices.").
349. *Id*. at 822; Schwartz, *supra* note 132, at 50.
350. MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 16 (2d prtg. 1971).

result, that individual and most similarly situated individuals are likely to continue sharing their personal information. They will wait for others to take that strong stand, and hope to free ride on the benefits that flow from their action. The problem, of course, is the few individuals who do take a stand and refuse to deal on unfavorable privacy terms cannot significantly impact the market.

Several additional factors inhibit consumers from undertaking collective action against standardized terms and practices. First, with regard to online privacy, the fragmented nature of Internet commerce makes collective action quite difficult. Even if a small group of sophisticated consumers were knowledgeable about a particular privacy-invasive practice, the vast number and relative isolation of Internet users would make it difficult to share that information with other interested consumers.[351] Second, even if all consumers were fully aware of the standard privacy practices, they would usually have to either accept or reject those terms, rather than negotiate changes.[352] The costs of exit can be quite high, even in the supposed new frontier of cyberspace, when consumers have invested time and resources learning to use a particular service, or when exit would require substantial administrative effort, as with changing e-mail addresses or Internet banks.[353] Third, individual consumers are disadvantaged in comparison to merchants because individuals do not enjoy the repeat player and other efficiency benefits that standard terms provide for merchants.[354] For these reasons, rule shopping and drafting are more costly for consumers than merchants.[355] Finally, even if a small group of sophisticated consumers united, merchants would have little incentive to alter their terms for all consumers, and at most would simply discriminate by providing more favorable terms to the small group of sophisticated consumers.[356]

Two proposed solutions to the collective action problem merit attention. The first involves privacy certification programs, or privacy seals, such as TRUSTe, BBB*OnLine* and WebTrust.[357] These programs

351. Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 437–38 (2000).
352. *Id*. at 437; Rakoff, *supra* note 337, at 1224–29.
353. Netanel, *supra* note 351, at 439–40.
354. *Id*. at 438.
355. *Id*.
356. *Id*. at 438–39.
357. Schwartz, *supra* note 14, at 1693–94; Froomkin, *Death of Privacy?*, *supra* note 1, at 1525–28.

involve theoretically independent entities that grant their seals of approval only to companies whose privacy polices meet certain baseline standards, like notice of what information they collect and how they use it, and opportunity to correct errors in the information they collect.[358] Ideally, consumers would then do business only with approved merchants. Different certification programs could even evolve to have different levels of privacy protection. These privacy certification programs, however, have several shortcomings. First, they are entirely voluntary. So far, very few merchants have chosen to participate, and there appears to be no pressure to do so.[359] The privacy seal organizations have also been accused of not cracking down on approved companies that violate the certification standards.[360] As of December 2000, none of the privacy seal programs had ever revoked or suspended a seal, and privacy violations by sealholders often come to light through the media or advocacy groups, rather than the seal programs.[361]

Another proposed solution to the collective action problem involves what Lawrence Lessig colorfully referred to as an "electronic butler," a privacy agent to whom you delegate the process of negotiating privacy terms.[362] The most prominent of these privacy agents is the Platform for Privacy Preferences Project, known as P3P™. The P3P standard would allow users and Web sites to express their privacy practices in a standard vocabulary. Each user's agent could then negotiate with Web sites, blocking (or at least warning the user about) sites whose privacy practices do not conform with the user's preferences.[363] Ideally, the privacy agent saves users the trouble of reading every character of every

358. Sovern, *supra* note 286, at 1095–96 & 1096 n.296; TRUSTe, *Privacy Seal Programs*, *at* http://www.truste.com/programs/pub_how.html (last visited Apr. 10, 2002) (stating that TRUSTe awards its trustmark "only to sites that adhere to our established privacy principles of disclosure, choice, access, and security. Furthermore, Web sites that display the TRUSTe privacy seal agree to comply with ongoing TRUSTe oversight and our alternative dispute resolution process."); Council of Better Business Bureau, Inc., *BBBOnline Privacy Seal*, *at* http://www.bbbonline. com/Privacy/ (last visited Apr. 10, 2002) (A BBBOnLine privacy seal signifies that the online merchant has met BBBOnLine Privacy Program requirements in regards to notice, choice, access and security regarding personally identifiable information collected online).

359. Edmund Sanders, *Web Privacy Programs Are Scrutinized: Government May Intervene As Self-Regulation Falters*, L.A. TIMES, Dec. 11, 2000, at C1; *see also* Froomkin, *Death of Privacy?*, *supra* note 1, at 1527 (stating that the minuscule percentage of firms participating in privacy seal programs "suggests that market pressure to participate is weak to nonexistent").

360. Sanders, *supra* note 359.

361. *Id*.

362. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 160 (1999).

363. *Id*.; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 521 (1999); World Wide Web Consortium, *P3P and Privacy on the Web FAQ, #1: What Is P3P?*, *at* http://www.w3.org/p3p/p3pfaq.html (last modified Jan. 29, 2002).

privacy policy for every site they visit. P3P automates that process by requiring Web sites to rate their own privacy practices and display them in a vocabulary the privacy agents can understand.

The primary weakness of the privacy agent solution to consumers' collective action problem, however, is that it requires merchants to act collectively against their own interests. The proposed privacy agents depend on merchants rating their own privacy practices, and doing so accurately. Merchants have a strong incentive *not* to provide consumers with the means to act collectively to express their privacy preferences.[364] A March 2002 survey by the Progress and Freedom Foundation found that four percent of 302 randomly sampled Web sites, and twenty-two percent of the eighty-five most popular Web sites, used P3P.[365] According to the World Wide Web Consortium, which developed P3P, only 445 Web Sites were using some version of P3P as of July 8, 2002.[366]

P3P has other shortcomings as well. Without some enforcement mechanism, P3P does not guarantee that Web sites will comply with their stated privacy practices.[367] P3P could even facilitate industry-wide lock-in of privacy-invasive practices.[368] The P3P vocabulary may also be too complicated for many individuals to use.[369] Finally, because the vocabulary itself will be chosen by P3P designers, not the individual users, the P3P protocol risks shifting the power to dictate privacy preferences away from individuals.[370]

---

364. Schwartz, *supra* note 132, at 50–51; Letter from Jason Catlett, Junkbusters Corp., to Lorrie Faith Cranor, AT&T Labs (Sept. 13, 1999), *reprinted in* Junkbusters Corp., *Technical Standards of Privacy: P3P (Platform for Privacy Preferences)*, *at* http://www.junkbusters.com/standards.html (last visited Apr. 26, 2002).

> As a product to protect the privacy of the average American shopper, P3P is doomed to fail, because such an outcome is not in the commercial interests of the organizations who decide whether and how it will be deployed. P3P has become a mirage in the desert of Internet privacy.

Id.

365. WILLIAM F. ADKINSON, ET AL., PRIVACY ONLINE: A REPORT ON THE INFORMATION PRACTICES AND POLICIES OF COMMERCIAL WEBSITES 81 (2002), *available at* http://www.pff.org/publications/privacyonlinefinalael.pdf (last visited July 10, 2002).

366. W3C® Platform for Privacy Preferences Initiatives, *Web Sites using P3P*, *at* www.w3.org/P3P/compliant_sites (last visited July 10, 2002).

367. Lessig, *supra* note 363, at 521 n.65.

368. *Id.*

369. Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 754–55.

370. *Id.* at 755.

B. Failures in the Political Market

Charlotte Twight coined the phrase "political transaction-cost manipulation," which she defined as "government officials' deliberate alteration of people's costs of undertaking collective political action in matters that affect the scope of government authority."[371] Twight described a useful parallel between the spheres of economics and politics. In the political market, the analog to market exchange is "collective political action that alters the role and scope of government."[372] In the economic market, transaction costs include the costs of obtaining information, negotiating contracts, and enforcing contracts.[373] In the political market, transaction costs for individuals and legislators include the "*costs of perceiving, and of acting upon their assessment of*, the net costs of particular governmental actions and authority."[374]

Twight divided the manipulation of political transaction costs into two categories: (1) manipulation of agreement and enforcement costs, that is, the cost to individuals of reaching and enforcing collective agreements on where to draw the line between the governmental and non-governmental spheres of action; and (2) manipulation of information costs relevant to people's decisions regarding where to draw that line.[375] Both types of manipulation involve what Twight called "contrived" political transaction costs.[376] I have slightly refined these categories to reflect parallels between failures in the political and economic markets. The manipulation of political transaction costs can usefully be subdivided into three categories: informational asymmetry; leveraging superior bargaining power; and incrementalism.

1. Informational Asymmetry

Information asymmetry arises in the political market when laws are drafted or promoted in a way that obscures or misrepresents their true effects. The resulting incomplete and inaccurate information deters citizens from opposing privacy-invasive laws.[377]

---

371. Twight, *supra* note 187, at 15 & 21 n.1. *See generally* Charlotte Twight, *Political Transaction-Cost Manipulation: An Integrating Theory*, 6 J. THEORETICAL POLITICS 189 (1994) [hereinafter, Twight, *Manipulation*].
372. Twight, *supra* note 187, at 15 & 21 n.1.
373. *Id*.
374. Twight, *Manipulation*, *supra* note 371, at 190–91.
375. *Id.* at 202, 207; Twight, *supra* note 187, at 20.
376. Twight, *supra* note 187, at 20.
377. *Id*. at 15.

Government can cause information asymmetry by concealing privacy-invasive provisions in legislation that has nothing to do with privacy. We find one recent example in Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[378] Buried under the heading "Administrative Simplification" lay the requirement that the Secretary of Health and Human Services "adopt standards providing for a standard unique health identifier" for all participants in the health care system.[379]

The unique health identifier provision was slipped into HIPAA in a last minute amendment filed by Ohio Representative David Hobson. Hobson had been pushing "unique personal identifier" legislation since 1993 at the behest of health and data processing companies and associations.[380] In fact, Hobson did not write the legislation himself. It was drafted by:

> a coalition of private interests with billions of dollars at stake, including the American Health Information Management Association, the American Hospital Association, the American Medical Association, the Association for Electronic Health Care Transactions, Blue Cross and Blue Shield Association, Electronic Data Systems, International Business Machines Corporation [IBM], and the Working Group for Electronic Data Exchange.[381]

Hobson's 1996 reelection campaign received $28,000 from "health, insurance, and information interests that favored the legislation."[382] The largest contribution came from the American Hospital Association, which helped write the legislation.[383] While the HIPPA bill was pending, two members of co-sponsor Sen. Kassebaum's staff were negotiating for jobs with pharmaceutical and health insurance interests.[384] Kassebaum's health policy counsel Dean Rosen was negotiating to become director of government affairs in Washington for Glaxo Wellcome, the international pharmaceutical company.[385]

---

378. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C., 42 U.S.C., 18 U.S.C., 26 U.S.C.).

379. *Id*. at § 1173(b)(1) (codified at 42 U.S.C. § 1320d-2(b)(1) (2000)).

380. *Nothing Sacred*, *supra* note 80, at 34–35. From 1987 to 1998, Hobson received more than $65,000 from the anti-privacy lobby. Tiffany Danitz, *Deceit, Denial and the Fate of Privacy*, INSIGHT ON THE NEWS, Aug. 24, 1998, at 14, *available at* 1998 WL 9105751.

381. *Nothing Sacred*, *supra* note 80, at 34.

382. *Id*. at 35.

383. *Id*.

384. *Id.*

385. *Id*. Another Kassebaum aide joined the staff of the Health Insurance Association of American soon after the bill passed. *Id*.

Despite its stealthy inclusion, the unique health identifier requirement ultimately became public and fell under fierce criticism, prompted in part by a 1998 Department of Health and Human Services White Paper titled "Unique Health Identifier for Individuals."[386] HHS considered six alternatives as "candidate identifiers," including the SSN and biometric identifiers, such as fingerprints and voiceprints, retina and iris scans, and DNA.[387] The White Paper suggested that the SSN could be improved by "begin[ning] with a newborn patient in the birth hospital" where "at once the proper authorities would assign a birth certificate number, assign an SSN, and assign the health identifier."[388] After the White Paper's release, the *New York Times* ran a front-page article publicizing the unique health identifier plans.[389] The health identifier requirement "horrified liberals and conservatives alike, with fears that privacy ultimately would be breached no matter what precautions were installed."[390] In response to the public outcry, Vice President Gore announced in 1998 that the Administration would not promulgate a unique health identifier regulation until comprehensive medical privacy protections were in place.[391] Congress subsequently prohibited the Department of Health and Human Services (HHS) from promulgating such an identifier, and HHS has no plans to promulgate a unique health identifier.[392] Clearly the prospect of a universal health identifier faces substantial public opposition. By burying the identifier provision in the midst of HIPAA, Congress circumvented that opposition, albeit only temporarily. However, not all such misdirection ultimately comes to light.

Government also creates information asymmetry by mislabeling privacy invasive legislation as privacy protective legislation. A classic example is the so-called Bank Secrecy Act of 1970.[393] Unwitting citizens would never have expected this secrecy act to require banks to make permanent copies of their bank records so the government could

386. U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 190.
387. *Id.* §§ III.B & III.C.2.
388. *Id.* § III.A.3.
389. Sheryl Gay Stolberg, *Health Identifier for All Americans Runs into Hurdles*, N.Y. TIMES, July 20, 1998, at A1.
390. James P. Lucier, *Antiprivacy Plot Is Well-Kept Secret*, INSIGHT, Aug. 24, 1998, at 16, *available at* 1998 WL 9105765. The unique health identifier was originally a key part of the Clinton administration's failed healthcare plan. *Id*.
391. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82566 (Dec. 28, 2000).
392. *Id*.
393. Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified at 12 U.S.C. §§ 1730d, 1829b, 1951–1959 (2000); 18 U.S.C. § 6002 (2000); 31 U.S.C. § 321, 5311–5314, 5316–5322 (2000)).

use them in "criminal, tax, or regulatory investigations or proceedings."[394]

2. Leveraging Superior Bargaining Power

Government also leverages its vastly superior bargaining power by tying anti-privacy legislation to government benefits. In 1935, when Congress sought to create a SSN for all Americans' retirement accounts, it secured passage by tying the SSN plan to popular programs such as "needs-based old-age assistance, unemployment compensation, and maternal and child health services."[395] In the throes of the depression, people were unlikely to oppose crucial social welfare programs to prevent the creation of a national database identifying every American. By linking these programs together, proponents of the SSN plan vastly increased the political transaction costs of opposing the plan.

Congress subsequently leveraged its bargaining power to ensure the SSN's widespread use as a de facto national identifier.[396] In theory, no one need obtain a SSN until they begin working and paying into the Social Security fund. In practice, however, Congress has effectively removed any element of choice, by conditioning income tax deductions for children upon parents registering their children for SSNs.[397]

3. Incrementalism

Finally, government proceeds with many privacy-invasive programs incrementally, eroding peoples' expectation of privacy gradually. Incrementalism has been most effective and pervasive in the exponential growth of the SSN. In 1935, officials assured Americans that the SSN would be used exclusively to identify their Social Security accounts.[398]

---

394. 12 U.S.C. § 1951(b) (2000) (stating purpose of recordkeeping requirement).

395. Twight, supra note 187, at 18.

396. *See* Twight, *supra* note 190, at 169. For a discussion of the SSN's proliferation, see *infra* § III.B.3.

397. *See* I.R.C. § 151(e) (2000) (prohibiting dependent deductions unless return includes dependent's identifying number); I.R.C. § 6109(d) (stating that individual's social security account number shall be used as identifying number for purposes of Internal Revenue Code). Congress originally required parents to provide SSNs for children by age five in order to obtain the deduction. Pub. L. No. 99-514, § 1524, 100 Stat. 2085 (1986). Congress lowered the age to two years in 1988, one year in 1990, and required SSNs for all dependent deductions, regardless of age, in 1994. Pub. L. No. 100-485, § 704(a), 102 Stat. 2343 (1988); Pub. L. No. 101-508, § 11112, 104 Stat. 1388 (1990); Pub. L. No. 103-465, § 742(b), 108 Stat. 4809 (1994).

398. H.R. REP. NO. 106-996, pt. 1, at 23 (2000).

In many gradual steps, however, the federal government has ensured the widespread use of the SSN as a personal identifier by federal agencies, state government, and the businesses sector.

In 1943, President Roosevelt issued an executive order requiring federal agencies to use the SSN to identify personnel, rather than have each agency develop its own identification system.[399] The 1960s saw three federal agencies adopt the SSN as an identifier: the Civil Service Commission in 1961; the Internal Revenue Service in 1962; and the Department of Defense in 1967.[400] The 1970s saw the SSN extended to a variety of government benefits programs. In 1972, the federal government began issuing SSNs to legally admitted aliens and to anyone receiving or applying for federal benefits.[401] Aid for Families with Dependent Children and the food stamp program began using the SSN for eligibility purposes in 1975 and 1977, respectively.[402] In 1976, state governments began using the SSN for tax purposes, public assistance identification, and driver's licenses.[403] Use of the SSN expanded even more dramatically in the 1980s and 1990s. In the 1980s it spread to the school lunch program, interest-bearing bank accounts, commercial motor vehicle operator's licenses, blood donor identification, and the National Student Loan Data System.[404] In the early- to mid-1990s its use extended to Department of Veterans Affairs payments, jury selection, worker's compensation claims, professional licenses, commercial driver's licenses, occupational licenses, marriage licenses, and death certificates.[405]

As suggested by public outcry over the National Data Center plan[406] and the universal health identifier,[407] the government could not have taken these steps in one fell swoop. Instead, by proceeding incrementally, the government has enabled itself to create SSN-based dossiers that track people from cradle to grave, through SSN-identified federal databases describing their educational experiences, medical histories, employment,

---

> The SSN was created in 1935 for the sole purpose of tracking workers' earnings so that Social Security benefits could be calculated upon retirement or disability. . . .
>
> Because a unique SSN is assigned to each individual, the number is commonly used as a personal identifier, although it was never intended for this purpose.

Id.; *accord* Twight, *supra* note 187, at 19–20.

399. GARFINKEL, *supra* note 73, at 20.
400. *Id.* at 33.
401. *Id*.
402. *Id*.
403. *Id*.
404. *Id.*
405. *Id*. at 33–34
406. *See supra* Part I.C.3.
407. *See supra* Part III.B.1.

financial transactions, public benefit receipts, social security benefits, and death certificate.[408] The federal government has thus achieved cradle to grave tracking via a de facto national identifier.

V. CONCLUSION

The foregoing observations provide strong arguments for implementing broad structural measures empowering individuals to claim their own privacy. Others have proposed many such structural measures, so I do not treat them in great detail here. I shall point out, however, how these observations about the expectation-driven conception of privacy bolster the arguments for structural reform.

The most sweeping structural measure would be establishing a Privacy Commission as part of the federal government.[409] A Privacy Commission, even without enforcement powers, would go far toward eliminating the informational, bargaining power, and collective action obstacles to individuals' claiming their privacy.[410] The Commission's primary power over industry and government would derive from investigating and publicizing privacy-invasive practices, and recommending legislative or regulatory solutions where appropriate. This would help alleviate the informational asymmetry that puts individuals at a disadvantage, and the Commission could employ its substantial bargaining power to persuade industries to revise privacy-invasive form contracts and technological standards. The Commission would also give individuals a powerful voice to help them overcome their collective action problems. Finally, the Commission could help deconstruct the internalization of privacy-invasive practices by publishing studies showing how conceptions of privacy have changed over time, and perhaps how they might change in the future. Adding enforcement powers would enable the Commission to deter specific violations and encourage pro-privacy practices. Even

408. *See generally* Twight, *supra* note 190.

409. *See* Schwartz, *supra* note 132, at 65–68 (proposing a United States Data Protection Commission).

410. *See id.*

> A United States Data Protection Commission would assist numerous social groups and draw the attention of the legislature and the public to the weaknesses of current laws. By fulfilling these tasks, the data protection agency would keep the legislature, citizens, and the business community aware and active as information technology continues to utilize different kinds of personal information in new ways.

Id. at 66.

without enforcement powers, the Commission could wield influence by referring illegal practices to the appropriate enforcement authorities.

In the realm of consumer privacy, privacy advocates have long called for legislative or regulatory requirements that industry adopt opt-in rather than opt-out approaches to collecting and using personal information. A meaningful opt-in requirement would combat information asymmetry by mandating plain language notice of what information merchants collect and how they will use it. That would give consumers far greater knowledge of the consequences of sharing their data. An example mentioned above shows that the opt-in approach is dramatically more effective than opt-out. The Driver's Privacy Protection Act of 1994 (DPPA) prohibited states from releasing drivers' personal information for certain purposes without the drivers' consent, but allowed states to presume such consent unless the drivers opted out.[411] A 1999 amendment changed the DPPA's protection scheme to opt-in; states could not release the information without the drivers' express consent.[412] In the month after Ohio implemented its opt-in law, only a handful of drivers opted in.[413] In the consumer context, the opt-in approach would shift the informational burden to merchants, who would have to inform consumers about the possible uses of their personal information, and to justify their requests with specific articulations of why they want consumers to opt in. Merchants are far better suited to shoulder the informational burden, since they already have mechanisms in place to exchange information with every one of the customers. The alternative—requiring every consumer to research each merchant's policies and practices—wastes consumers' limited resources.

Consumer privacy legislation should further combat information asymmetry by requiring every business to obtain the consumer's express consent each time it wishes to share personal data about that consumer with a third party.[414] Businesses could send notice via e-mail or post card, giving consumers the option to grant or deny permission via e-mail, Web site, or toll-free telephone number. The notices would have to disclose the identity of the third party. Although some consumers are dimly aware that their data is shared, most have no conception of how pervasive the data web is. Merely receiving notice of each instance of

411. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, § 300002(a), 108 Stat. 1796, 2099 (1994).

412. Department of Transportation and Related Agencies Appropriation Act of 2000, Pub. L. No. 106-69, § 350(c)-(e), 113 Stat. 986, 1025 (1999).

413. Welsh-Huggins, *supra* note 197, at C10.

414. *See* Schwartz, *supra* note 314, at 1673–74 (proposing legislation prohibiting sharing personal information for purposes not "compatible with the original collection" without the individual's formal consent).

data sharing would raise awareness among consumers, and the opportunity to deny permission would add to the process an aspect of meaningful consent that is notably absent today.

Building on the foregoing proposals, a more dramatic step would be to prohibit companies from discriminating in their terms or conditions against consumers unwilling to share personal information. The DPPA provides a legislative model for this approach.[415] A 2000 amendment prohibits states from "condition[ing] or burden[ing] in any way" the issuance of a driver's license, title, or registration to obtain express consent to disclose information.[416] Some will protest that this step would deprive willing individuals of the right to sell their privacy. But it may be the only effective way to remedy the problem of incrementalism, in which consumers perceive the benefits of each individual transaction as outweighing the cost of surrendering one bit of personal information.

Preventing merchants from discriminating against consumers who deny consent would also test the industry claim that most people actually enjoy the benefits that flow from consumers' sharing personal information, such as targeted advertising and improved service. If the claim is true, then many individuals will still share their data voluntarily, while those more sensitive about their privacy will find it far easier to protect. On the other hand, if the claim is false, then very few people will share their data voluntarily, and the legislation will have helped people choose long-term privacy over other short-term benefits.

Merchants, especially Internet merchants, will complain that such legislation would drastically increase their costs, which they would have to pass on to consumers. That argument assumes that the sharing of personal data is an integral part of their business. However, the current trade in personal data may be more properly understood as an attempt to generate an income stream to supplement the merchant's primary business. And if restricting the trade in personal data would be fatal to some data profilers and Internet companies supported almost entirely by data-sharing revenues, that would demonstrate that we have been subsidizing inefficient business models by allowing a trade in personal data.

---

415. *See* Froomkin, *Death of Privacy?*, *supra* note 1, at 1535 (explaining that to prevent opt-in consent from becoming part of a standard form or terms, law would have to prevent repercussions for failure to convey consent).

416. *See* Pub. L. No. 106-346, § 309(e), 114 Stat. 1356 (2000) (codified at 18 U.S.C. § 2721(e) (2000)).

Workplace privacy presents an even greater need for structural reform. Employers wield far more bargaining power over employees than do merchants over consumers. As discussed above, employers have taken full advantage of the expectation-driven nature of privacy by preemptively defeating employees' expectation of privacy. Lawmakers could alleviate the imbalance of power by depriving employers of the tools they use to lower expectations. For example, new laws could restrict the circumstances in which employers could monitor employee e-mail or Internet usage, and could also prohibit employment policies or contracts from stating that the employer will monitor such usage. A privacy commission could play a useful role in this context, perhaps by requiring employers to issue employee privacy notices similar to workplace safety notices required by the Occupational Safety and Health Administration.

More important than specific solutions, however, may be the recognition that privacy is a matter of expectations. The privacy battle is to be won or lost not by theoretical argument about the nature of privacy, but by concrete action and advocacy designed to affect society's expectations. Today, some of the most important work is done by watchdog and advocacy groups working to expose and deter encroachment. We may best serve the cause of privacy not though abstract arguments about what *ought* to be private, but through careful examination of not only our current expectations of privacy, but also how and why those expectations have changed. For under the expectation-driven conception of privacy, what we expect to be private today will determine what the law will protect as private tomorrow.

Finally, the shocking September 11 terrorist attacks threaten to skew the already tenuous balance between privacy and security in favor of the latter. Now, more than ever, the immediacy of the danger may blind decisionmakers to the widespread and potentially irrevocable effects of each seemingly limited encroachment on privacy. The new USA PATRIOT Act[417] has already expanded substantially the government's ability to conduct surveillance on its citizens. To take one example, the USA PATRIOT Act has expanded the types of Internet usage information that any "governmental entity"—not merely a law enforcement agency[418]—may review without obtaining a warrant or court order.[419] They need only serve an administrative subpoena,[420]

417. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of 8 U.S.C., 15 U.S.C., 18 U.S.C., 22 U.S.C., 31 U.S.C., 42 U.S.C., 49 U.S.C., 50 U.S.C.).

418. *Id.* The Electronic Communications Privacy Act does not define the term "governmental entity" as used in 18 U.S.C. § 2703(c)(2) (2000).

419. 18 U.S.C. § 2703(c)(2), *amended by* Pub. L. No. 107-56 § 210, 115 Stat. 283 (2001).

grand jury subpoena, or trial subpoena upon an electronic communication service provider.[421] The newly authorized information includes the time and duration of any user's Internet sessions, the user's Internet Protocol address, and any credit card or bank account number that pays for the user's Internet service.[422] Indeed, even without new legislative or executive measures, many businesses disregarded their own privacy policies to disclose information to law enforcement in the days following the attacks.[423] Congress justified the USA PATRIOT Act as necessary to "deter and punish terrorist acts in the United States and around the world, [and] to enhance law enforcement investigatory tools."[424] But its effect on privacy expectations will reach beyond terrorists and other legitimate subjects of law enforcement investigations. Indeed, anyone who uses the Internet must expect the possibility that a government agency may learn their credit card or bank account numbers, their IP address, and dates and times of their Internet sessions.[425]

Those who make law and policy must include long-term privacy consequences in their decision-making equation. Measures that could diminish privacy are often justified by reference to superficially more concrete goals such as efficiency, crime deterrence, and security. To the extent that policymakers balance privacy against those goals at all, they may consider only the most immediate privacy implications. For example, adopting a national identification card to promote security at airports and borders[426] might appear to have only minimal privacy

420. The general standard for review of an administrative subpoena is extremely lenient. Courts must enforce an administrative subpoena if the inquiry is "within the authority of the agency, the demand is not too indefinite, and the information sought is reasonably relevant." United States v. Morton Salt, 338 U.S. 632, 652 (1950). The *Morton Salt* court explained that an agency's investigative authority is analogous to a grand jury's authority, and that the agency "can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not." *Id*. at 642–43.

421. 18 U.S.C. §2703(c), *as amended by* USA PATRIOT Act § 210.

422. *Id.*

423. Stephanie Stoughton, *Poll: Firms Relaxed Privacy Rules*, BOSTON GLOBE, Oct. 8, 2001, at C4, *available at* 2001 WL 3956333 (reporting that fifty-nine percent of airlines, hotel chains, travel agencies, rental car companies, and other travel-related firms surveyed said they relaxed their own privacy policies to aid law enforcement officials in the wake of the terrorist attacks).

424. USA PATRIOT Act, pmbl.

425. 18 U.S.C. § 2703(c), *amended by* Pub. L. No. 107-56 § 210, 115 Stat. 283 (2001).

426. *See, e.g.*, Alan M. Dershowitz, *Why Fear National ID Cards?*, N.Y. TIMES, Oct. 13, 2001, at A23. *See generally* Ross Kerber, *ID, Please: Idea of National Identity Card System Gains Momentum in Wake of Attacks*, BOSTON GLOBE, Sept. 24, 2001, at C1.

implications, because airlines routinely ask passengers for identification,[427] and people must present a passport or other identification at most border checkpoints.

Such a narrow view, however, ignores the widespread unintended consequences of a national identification card. Secondary uses of such a card would multiply exponentially, as have uses of the social security number.[428] A national identification system would require a national database and a single identifier—a number or a biometric, like a fingerprint or facial image—for each cardholder. Such a centralized infrastructure would present irresistible secondary uses, both in and out of government. Welfare agencies could include relevant information in the database to prevent people from fraudulently obtaining benefits. Law enforcement could merge criminal records into the database. The database could hold confidential medical data, and serve as the universal health identifier proposed in the Health Insurance Portability and Accountability Act of 1996.[429] In the business sector, financial institutions and merchants could insist upon presentation of a valid national ID card as a condition to extending credit or conducting transactions with individuals.

Such a centralized database of personal information is ripe for abuse, regardless of the government's attempts to keep the information confidential. To list just one egregious example, during World War II, the government used supposedly confidential Census Bureau information to identify Japanese-Americans for incarceration in internment camps.[430] Moreover, as discussed above, governmental officials are not above using confidential information for personal or political gain,[431] and even confidential IRS information is vulnerable to abuse from within and hacking from without.[432]

Each incremental expansion of the national identification card's use would erode individuals' expectation of privacy.[433] The requirement to

427. *See Airlines Demanding ID, But Not for Security*, 22 PRIVACY J., Nov. 1995, at 1, 1.

428. *See* discussion *supra* notes 187–192 and accompanying text.

429. *See* discussion *supra* notes 378–392 and accompanying text.

430. John J. Miller & Stephen Moore, *A National ID System: Big Brother's Solution to Illegal Immigration*, at n.14 (Cato Policy Analysis No. 237, 1995), *available at* http://www.cato.org/pubs/pas/pa237es.html (last visited Apr. 21, 2002).

431. *See* discussion *supra* notes 264–269 and accompanying text.

432. *See* discussion *supra* notes 270–272 and accompanying text.

433. Although some sections of the USA PATRIOT Act will sunset at the end of 2005, the sunset provision does nothing to forestall this erosion. It is true that Congress will have to renew those few provisions that expire in 2005. USA PATRIOT Act § 224 (2001). But in the intervening four years, people's expectations of privacy may diminish in response to more aggressive law enforcement practices. Expectations will not spontaneously bounce back simply because the technical authority for the intrusions

present our virtual dossier would almost inevitably expand—from airports, to welfare offices, to banks and merchants. So would the types of data that those dossiers routinely exposed to scrutiny—from our physical characteristics to our addresses to our confidential medical and financial information. With each step in this process, we would become increasingly used to the idea that our personal information is free for inspection by others. Exposure of personal information would shift toward the norm rather than the exception.

As the national ID card example demonstrates, government must recognize that its actions and initiatives have far reaching effects on expectations of privacy. If government succumbs to short-term fears and ignores the long-term privacy consequences of its actions, the inevitable secondary uses and unintended consequences of sweeping anti-terrorism initiatives will make privacy a collateral casualty of the war on terrorism.

expires. Instead, the diminished expectations of privacy will present Congress with only minimal resistance to renewing these intrusive provisions.