MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 27 | Issue 3 Article 16

2001

The Privacy Paradox

Eric Jorstad

THE PRIVACY PARADOX

Eric Jorstad†

I. INTRODUCTION

Americans are ambivalent about privacy.

On the one hand, we believe in self-creation, and cherish the private space required to plot, plant and nurture our dreams. We recoil at intrusions into that space, whether by government, business, the media or our neighbors. On the other hand, we believe in enlightened progress through competition, science, technology, the market and ideas. No hypothesis goes untested, a process powered by mind probing beneath every surface, behind every truism, past every "Keep Out" sign, driven by the quest for progressive, pragmatic, ever-changing truths.

The law reflects this ambivalence. A property law regime protects the personal identity paradigm inherent in the *garden* metaphor for self-creation. The space we own is ours and may not be entered without consent. At the same time, a free market and free

† Eric Jorstad is a partner in the law firm of Faegre & Benson LLP. He coordinates the firm's Data Privacy practice. He wishes to thank John Borger, Kate Boschee, Michael Carlson, Tom Schroeder, Nan Remus, Ann Kraemer, Jonathan Asner, Kristin Eads and Paul Civello for reviewing earlier drafts of this article; for better or worse, however, he is responsible for what is written here.

speech regime protects the dynamic personal capacities paradigm inherent in the *progressive* metaphor for competitive transformation. The powers of inquiry should not be thwarted by out-moded barriers and no question, no comment, no product, is out of bounds.

The Internet brings this conflict to a head.

The current debates about privacy should be understood in the context of our underlying ambivalence, what I call the privacy paradox. We have fashioned, to date, a legal and cultural system which permits both paradigms to flourish (usually). At the dawn of the Cyber Age, however, there are proposals to lop off one side or the other of our core values. The secret of our success has been the ability to maintain both sides of the paradox simultaneously. The challenge now is to refashion legal norms to restructure our vibrant ambivalence, our gloriously conflicted self-understanding, for the New Age.

In this article, I will explore the privacy paradox as businesses, government and American culture grapple with the appropriate scope and limit for the regulation of data privacy in the Cyber Age. In Part II, the core fear underlying the privacy debates is described as loss of autonomy. Intrusions on (data) privacy by business, government and individuals are feared with respect to "big brother" Internet, harassment, children, medical records, credit history, and loss of face. The core fear is placed alongside the other core value in the privacy debates, the free flow of information in the political and economic spheres. In Part III, the developing regulatory regime governing data privacy is described, looking at the process of regulatory development through an analogy to the development of the product safety regulatory regime. "Data" are, in one sense, simply another type of product in the stream of commerce.[1] Finally, in Part IV, I propose a model for organizations (business, nonprofit and governmental) to move beyond privacy "compliance" to the flexible integration of the privacy paradox into fundamental organizational mission. Ultimately, it is the unresolvable nature of the privacy paradox which gives the issue of privacy its dynamic power to catalyze organizational processes. As the philosopher Friederich Nietzsche wrote, "One is fruitful only at the cost of being rich in contradictions."[2] In short: embrace the privacy

1. Reno v. Condon, 528 U.S. 141 (2000) (stating that personal information may be a "thin[g] in interstate commerce") (alteration in original).

2. FRIEDERICH NIETZSCHE, *Twilight Of The Idols Or How To Philosophize With A*

paradox.

II. PRIVACY FEARS

Although the definition of the word, "privacy," is primarily negative or exclusive, the concept of "privacy" includes both a positive and a negative dimension. According to Merriam-Webster's Collegiate Dictionary, privacy is defined as: "(1)(a) the quality or state of being apart from company or observation: seclusion; (b) freedom from unauthorized intrusion <one's right to privacy>; (2) ... a place of seclusion; (3)(a) secrecy; (b) a private matter: secrecy."[3] This definition emphasizes the negative notion of privacy, that it is a state of *not* being visible to others, where one is *not* intruded upon. As the poet Robert Browning wrote,

I give the fight up: let there be an end,
A privacy, an obscure nook for me.
I want to be forgotten even by God.[4]

Privacy is the state of being safe behind a wall which excludes others.

But there is a positive dimension implicit in this definition. Privacy includes the power to build and maintain that wall of safety. Privacy includes the power to set a boundary protecting the self–and whatever or whomever else the self chooses to include–from all others. Thus, a core value inherent in the concept of privacy is *autonomy* or, to use a political term, *freedom.* Privacy is the freedom to define and express one's self as one chooses. Whom do you welcome in your kitchen? In your bedroom? In the "c:\" drive of your computer? The power to welcome as one chooses, and to exclude as one chooses, is the positive dimension of privacy.

In this light, we can see what motivates the current debates over privacy, and understand why these debates are so highly charged. With the growth of cyberspace and increased awareness of the mobility of personally identifiable data ("PID"), the core fear is *loss of autonomy.* In the "hierarchy of needs" identified by psychologist Abraham Maslow, the most basic need is to not die, with fear of death, then, being the primal fear. The next most basic

---

Hammer, in TWILIGHT OF THE IDOLS/THE ANTI-CHRIST 54 (R.J. Hollingdale trans., Penguin Books 1968) (emphasis omitted).

3. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 927 (10th ed. 1993), *at* http://www.m-w.com (last visited Nov. 24, 2000).

4. ROBERT BROWNING, *Paracelsus, in* THE POETICAL WORKS OF ROBERT BROWNING 40, 44 (G. Robert Strange ed., Houghton Mifflin Co. 1974) (1895).

need, closely related, is for safety, the need to not be harmed. In Maslow's approach, the higher order needs–for love, productivity, meaning, art and spirituality–cannot be met unless the primal needs are first secured.[5] Privacy is an element of the nearly-most primal need for safety,[6] and may even involve fundamental life-and-death fears.[7]

This hits home for me with a simple metaphor. I have two daughters, currently ages eleven and fifteen. I often feel that sitting them down, alone, at a personal computer connected to the Internet is the cyberspace equivalent of setting them down by themselves in the middle of Times Square in New York City. What can they see? Who can see them? How can they evaluate the motives of everyone who might approach them? How will they find the fun, *safe* places that make Times Square a delight? Or will they unwittingly fall prey to ... what? Do I even know what I should really be afraid of, on their behalf?

Privacy fears take many forms in cyberspace.

One privacy fear is the power of "big brother" Internet. For example, in 1998 GeoCities settled a suit brought by the FTC alleging that GeoCities was collecting extensive PID from Web site visitors without the visitors' knowledge.[8] GeoCities was collecting such information as e-mail and postal addresses, gender, interest areas, marital status, income, occupation and education. It collected this from children as well as adults. The privacy fear is that Web sites can function like "big brother" in Orwell's work of "fiction," *1984*, seeing all, hearing all, knowing all, and then making decisions affecting the quality of your life without your knowledge or consent,

5. *See generally* ABRAHAM MASLOW, MOTIVATION AND PERSONALITY (3d ed. 1987).

6. According to neuroscientists, the need for safety arises from the most primitive "reptilian" brain inside our skulls, the limbic system at the base of the brain where it meets the spinal cord. This primitive brain asks only six questions of any particular person encountered: whether this is someone to "1) nurture, 2) be nurtured by, 3) have sex with, 4) run away from, 5) submit to, or 6) attack." H. HENDRIX, GETTING THE LOVE YOU WANT 11 (1998) (citing P. McLean, *Man and His Animal Brains*, MOD. MED., Feb. 1964). The higher brain, like the higher order needs described by Maslow, rests atop this primitive foundation.

7. The issue of abortion is often cast as a matter of privacy or autonomy. *See generally* Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833 (1992). The intensity of feeling and fears related to abortion, on all sides of the public debate, illustrates the kind of response often connected to "privacy" issues.

8. *In re* GeoCities, FTC File No. 982 3015 (Aug. 13, 1998). Copies of the complaint and the proposed consent order can be found at http://www.ftc.gov/os/1998/9808.

let alone participation. Web users may not make the distinction critical to Orwell's vision, between the omniscient totalitarian "eye" of the government and of businesses. It is simply "another" who is watching me, invading my privacy. The core fear is loss of autonomy.

Another privacy fear is personal harassment. Stories of Internet "stalking" are common, or at least felt to be common. One report illustrates the concern. A direct marketing company contracted with the Texas prison system for inmates to enter survey data into computers. One inmate, a sex offender, used information from the data entry to write a twelve-page threatening letter to a woman who had responded to the company's survey. Because of this case, the Texas legislature barred sex offenders from record-entry work. "We lost some damn good programmers-pedophiles," said the director of state prison industries. "Some of our best computer operatives were sex offenders."[9]

A related privacy fear is identity theft. Trans Union, one of the Big Three credit reporting agencies, noted that its credit bureau received more than 45,000 calls a month from people complaining that their credit accounts had been taken over.[10] This fear is not limited to cyberspace. My own credit card was stolen and used to purchase more than $1200 in clothing and electronics in one evening.[11] More people are now buying paper shredders for their personal mail, shredding the voluminous credit card offers received by mail which often contain PID. In the cyberworld, we are less confident of our ability to "shred" revealing electronic information about us.

Medical information may be particularly sensitive. Last year, University of Michigan medical records were posted on the Internet for at least two months before the error was discovered.[12]

---

9. Nina Bernstein, *Lives on File: Privacy Devalued in Information Economy*, N.Y. TIMES, June 12, 1997, at A1.

10. *Id.*

11. My experience showed the value of legal protections for credit card holders. I was not aware that the card was even missing (I had left it behind at a supermarket), until the credit card company called the next morning because of "suspicious" purchases which it wanted to verify were authorized. Local police actively investigated and apprehended the thief based on a store video camera which captured a purchase at the exact time and location noted on the credit card records. The credit card company even waived my payment of the standard $50 deductible for theft protection, so I ended up losing nothing in the end (except some peace of mind).

12. Jodi Upton, *U-M Medical Records End Up on Web*, DETROIT NEWS, Feb. 12,

Targeted direct mailing raises the question for consumers: how much do "they" really know about me? I recently received a direct mail political advertisement from a candidate promising to keep our private information private ... addressed to me, personally, at my home address. How did he know I lived there? How much personal information is for sale? Who will target us, for what?

A skeptic might ask, reasonably, how much of our privacy fear reflected in these anecdotes is grounded in fact. There is a striking paucity of reliable information.[13] The FBI's Uniform Crime Reporting Program includes subcategories for counterfeiting, forgery, credit card fraud, bad checks and hate crimes but no Internet-specific reports.[14] The FTC will take consumer complaints about Internet fraud, spam, identity theft, and anything else about which one wishes to complain, but its enforcement activities are limited and its publication of Internet privacy resources slim.[15] Creating good public policy about privacy under these circumstances is like drafting anti-crime legislation based on what you read while waiting in the supermarket checkout line.

There is more to the story. The privacy fears based on non-consensual intrusion into personal (data) space represent only one side of the privacy paradox. The other side of the paradox does not grab headline attention in the same way, but it is equally critical to understanding data privacy.

A free society requires the free flow of information. This is true in both the political and economic spheres. The First Amendment protects the rights of expression, underlying the proc-

---

1999, at A1, *available at* 1999 WL 3915521.

13. A compendium of shockingly unreliable information either about, or transmitted by, the Internet can be found at http://www.urbanmyths.com.

14. *See* FEDERAL BUREAU OF INVESTIGATION, *Uniform Crime Reporting Program, at* http://www.fbi.gov/ucr.htm (last visited Nov. 24, 2000).

15. The FTC's Web site contains a complaint form, which also contains links to the FTC's identity theft report form and unsolicited commercial e-mail (spam) report form. FEDERAL TRADE COMMISSION, *Bureau of Consumer Protection Complaint Form, at* http://www.ftc.gov/ftc/complaint.htm (last updated Oct. 27, 2000). The FTC's Web site also describes its enforcement activities and publications related to privacy. FEDERAL TRADE COMMISSION, *Privacy Initiatives, at* http://www.ftc.gov/privacy/index.html (last updated Oct. 10, 2000). A leading critic of the FTC privacy initiatives is the Electronic Privacy Information Center, or EPIC. *E.g.*, Electronic Privacy Center, *Network Advertising Initiative: Principles Not Privacy*, (July 2000), *at* http://www.epic.org/privacy/Internet/NAI_analysis.html (last visited Nov. 13, 2000); http://www.epic.org/privacy/Internet/EPIC_testimony_799.pdf (last visited Nov. 13, 2000).

ess of democratic self-governance.[16] This applies to political expression, to be sure;[17] but it also applies to protect the capacity of businesses to create target audiences for particular commercial solicitations.[18] The Freedom of Information Act and numerous state-law "government in the sunshine" acts create public access to government information and give citizens the information they need to scrutinize the operations of government.[19] In the political sphere, information flows freely both directions, from the governed to the government and from the government to the governed, at least in principle.

In the economic sphere, the free flow of information is critical to the flexibility and power of the market. Consider just one example. A consumer may feel queasy about the full range of information available to a credit reporting agency, which may document every loan, bank account, criminal conviction, and asset one has (and could even include reports of interviews with neighbors and coworkers).[20] But in a mobile, diverse and *large* community of potential borrowers, who wants to rely on the personal knowledge of a banker the next time one applies for a home loan, car loan, or credit card? Credit makes the (economic) world go around, and in this big world it could not function without credit reports.

Furthermore, the commercial capacity for profiling target market audiences is the flip side of the credit evaluation process.[21] In a free economy – where customers can choose what to purchase, from whom, and where businesses can choose what to sell, to whom

16. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 269 (1964). *See also* Burt Neuborne, *Free Expression and the Rehnquist Court*, 538 PLI/PAT 1273, 1275-81 (1998); Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757, 1760 (1995); Alexander Meiklejohn, *Testimony On The Meaning of the First Amendment*, FIRST AMENDMENT CYBER-TRIB., *at* http://w3.trib.com/FACT/1st.meikle.html (last updated Oct. 21, 1997).

17. Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 194 (1999).

18. U.S. West, Inc. v. Fed. Communications Comm'n, 182 F.3d 1224, 1232 (10th Cir. 1999), *cert. den. sub nom.*; Competition Policy Inst. v. U.S. West, Inc., 120 S. Ct. 2215, 2217 (2000).

19. Freedom of Information Act, 5 U.S.C. § 552 (1994 & Supp. 1998); Minnesota Government Data Practices Act, MINN. STAT. §13.01 (1997) *amended by* 2000 Minn. Sess. Law Serv. 468 (H.F. 3501) (West).

20. Fair Credit Reporting Act, 15 U.S.C. § 1681a(e) (1994).

21. For the FTC's report about Web site profiling of customers, *see* FEDERAL TRADE COMMISSION, *Online Profiling Report* (June 2000), *at* http://www.ftc.gov/os/2000/06/index.htm#13; Federal Trade Commission, *Online Profiling: A Report to Congress (Part 2): Recommendations* (July 2000), *at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

–the exchange of information is critical to finding a mutual "fit" between customer and business so that a sale can be made. When it comes to a small-town hardware store, you feel good getting a call from the owner at home telling you about a new shipment of innovative products helpful to your farm, home, or business.[22] But "telemarketing" by impersonal behemoths or computer-generated voices is hardly a feel-good enterprise.[23] Customer profiling is the mass market's attempt to simulate the personal attention of a business that is known, liked, and trusted.

The commercial privacy fear, corresponding to the individual privacy fears discussed above, is loss of trust. To succeed, a business needs to be seen as reliable and responsive. At a minimum, a business does not want to get "caught" breaching the rules of privacy expected by customers. At the other end of the spectrum, a business wants to be known as a place customers can count on, a place that cares about what customers think and handles their concerns with respect. In some lines of business involving particularly sensitive information—financial, medical, insurance, credit, etc.—the trust relationship is critical to the business's existence and growth.[24]

This is the dilemma for business: how to obtain and use the most helpful information about customers and potential customers, and at the same time show respect for the walls customers have constructed to keep business (among others) out. The simple, small-town answer is to be invited inside for conversation. In the mass markets defining most business today, however, this kind of access is not available.

---

22. My grandfather ran the local hardware store in Kenyon, Minnesota (population of 1150) for many years. The description above is not a hypothetical.

23. There are exceptions, based in part on the detail of information available to telemarketers. One evening this year, just as I was talking with my older daughter about the exhibit I had seen a few days earlier at the Minneapolis Art Institute, the phone rang and it was a telemarketing solicitation from the Art Institute! Was it ESP, surveillance, luck, or good-targeted marketing information? I recalled entering a contest during my visit to win a design consultation at the Art Institute, which was the likely source of my (unlisted) phone number. Needless to say, I am now a proud member of the Minneapolis Art Institute.

24. Another dimension of the commercial regulatory fear is the high cost of litigation in the area, due in part to the legal uncertainties. *See infra* Part III. Because data privacy is so prominent on the current public radar screen, and because of the inherent sensitivities involved in "privacy," the high *cost* of litigation also includes the loss of goodwill and trust. Commercial privacy fears are directly connected to the business bottom line of earnings, as well as the social psychological factors discussed above.

III. PRIVACY REGULATIONS

If autonomy and access—freedom as the power to set a wall and freedom as the power to cross every wall—are the competing core values at stake in the concept of privacy, what legal regime should be developed to advance these values? Looking at the bigger picture in historical context, privacy regulation today is (with a few important exceptions) about where consumer product safety regulation was in about 1965. Indeed, the experience with the development of consumer product safety regulations is helpful for understanding the current climate for the regulation of privacy.[25]

The mass market for tangible consumer products "took off" in the 1950s. Although the Industrial Revolution and rise of automated production had been growing for decades, the transformation from a *custom-made* to a *mass-produced* economy was not complete until after the second world war. At the dawn of the consumer product economy, the governing legal regime could be summarized in the Latin motto, *caveat emptor*, "let the buyer beware." But a regime appropriate to the custom-production economy, characterized by face-to-face interactions between maker and buyer, proved inadequate to the anonymous fungible mass-market "modern" system which came to reign.

In California (naturally), in a case involving power tools (of course), the state supreme court espoused a new view of liability for harm to consumers from modern products.[26] The older view, *negligence*, required some showing of fault on the part of the manufacturer before a consumer could recover. The California court replaced the fault system with *strict liability* in tort. An injured consumer could recover if the product was defective, without regard to the fault, or lack of fault, on the part of the manufacturer who made it. Thereafter, in federal and state legislatures, consumer product safety regulations came to prescribe standards for product manufacture, and agencies arose to monitor complaints and enforce compliance with the new standards. Industry groups

25. The impetus for this analogy was a line from Marc Rotenberg, Director of the Electronic Privacy Information Center, while testifying at the FTC hearings on electronic consumer privacy in 1996. He stated, "[p]rivacy will be to the information economy what consumer protection and product safety were to the industrial age." Bernstein, *supra* note 9, at A1. The development and critique of this analogy in this article is, however, my own creation.

26. Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 899 (Cal. 1963) (embracing the concept of strict liability in a tort case involving a power tool).

and trade associations often developed safety standards in conjunction with governmental efforts.

The *laissez-faire* regime of product safety was replaced by the regulated market we take for granted today. One advantage of the commonplace nature of these regulations is that a business may procure insurance for its liability risks. The transaction costs for the regulated market are enormous (insurance premiums, legal departments, compliance officers, training, tax-funded agencies, etc.), but the costs are for the most part predictable. Consumer product safety is just one of the costs of doing business, like labor, equipment and advertising.

The world of data privacy regulation today is much like the world of consumer product safety regulation in the mid-1960s. Just as the universalization of automation replaced a custom-made consumer product world with a mass-produced world, the universalization of electronic data storage and communication is replacing the custom-made consumer information databases with mass-produced and mass-distributed information. The market for information "took off" in the 1990s. It is epitomized by the commercialization of cyberspace. At the dawn of the cyber-economy, the governing legal regime can be described by a variant on the old Latin phrase: *caveat orator*, "let the communicator beware." In other words, communicate about yourself at your own risk. The communicator bears the risk that the information communicated will be misused somewhere in cyberspace—that one's survey results will be entered in a computer by a convicted sex offender in Texas, that one's purchasing patterns will be sold to telemarketers, that one's credit identity will be misappropriated by someone else's wild spending spree, that one's children will be stalked by Internet pedophiles, and so on.

This "wild west" mentality of free-wheeling Internet data exchange is being faced with a stagecoach full of sheriffs eager to clean up (or at least be seen cleaning up) the town. Data privacy regulations are proliferating. The patchwork nature of the law is breathtaking. Businesses struggling to meet even minimum goals of compliance with data privacy laws are faced with complex internal data practices audits and development of new compliance strategies—but to comply with ... what? What was/is/will be the data privacy law? What will be the contours of the regulated data privacy market which will, ineluctably, replace the *caveat orator* world of the late 1990s?

Before turning to a brief outline of current data privacy laws, I would like to make three overall comments.

First, the First Amendment changes the parameters of the regulation of data privacy, in contrast to the now well-settled regulation of consumer product safety. The collection, organization, maintenance and dissemination of "information" is, after all, a form of communication, and the First Amendment places distinct and unique limits on the ability of the government to regulate communication.[27]

Second, the cyberworld of information distribution differs significantly from the geoworld of consumer product distribution. Consumer products "exist" in a world of atoms and molecules and manufacturing plants (in a definable place) and sellers (in a definable place) and buyers. Cyber-information "exists" in a different manner. To be sure, it does exist. But its regulation poses problems of jurisdiction, choice of law, regulatory authority and international cooperation that are different from the regulation of tangible consumer products.[28]

Third, the dynamic power of the privacy paradox makes the regulation of privacy particularly problematic. I will discuss this in more detail in Part IV below. Indeed, I will ask whether it is possible—and desirable—to develop a regulatory scheme for data privacy along the model of consumer product safety regulation, in light of the critical issues posed by the First Amendment, cyber jurisdiction, and the privacy paradox.

With these historical and philosophical principles in mind, we can sketch the current law of data privacy with broad brush strokes. There are five areas in which data privacy is regulated: federal statutes and regulations, state statutes and regulations, state common

27. *E.g.*, Am. Civil Liberties Union v. Reno, 217 F.3d 162, 173 (3d Cir. 2000).

28. *E.g.*, Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1329 (E.D. Mo. 1996) (involving personal jurisdiction over the California operator of an Internet site that provided information on a forthcoming service); State by Humphrey v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998) (involving personal jurisdiction over Nevada operator of forthcoming online gambling service advertised to Minnesota residents); *see also* Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 165 (D. Conn. 1996) (holding that Massachusetts corporation purposefully availed itself of privilege of doing business in Connecticut by advertising its activities and its toll-free number on Internet on a continuing basis); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (concluding "likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet").

law, the European Union, and self-regulation.

A. *Federal Statutes And Regulations*

The main federal statutes governing data privacy have been developed to address specific sub-areas of privacy, according to the kind of data at issue. The Fair Credit Reporting Act ("FCRA") governs credit reporting agencies and certain employment-related data.[29] The new Financial Services Modernization Act, or Gramm-Leach-Bliley Act, governs data practices of "financial institutions," broadly defined.[30] The Health Insurance Portability and Accountability Act governs data use by health care institutions.[31]

In addition to these broad laws governing certain categories of data, other federal statutes regulate data based on the age of the data subject, type of data recipient, or means of data collection. The Children's Online Privacy Protection Act governs Web site col-

29. 15 U.S.C. §§ 1681, 1681a-u (1994 & Supp. 1998). The FTC has published formal commentary on the FCRA. *See* Federal Trade Commission, *Fair Credit Reporting Act*, *at* http://www.ftc.gov/os/statutes/fcrajump.htm (last updated Oct. 17, 2000), as well as extensive letter opinions concerning specific FCRA issues, *at* http://www.ftc.gov/os/statutes/fcra/index.htm (last updated Aug. 22, 2000) and guidelines for compliance, *at* http://www.ftc.gov/os/statutes/2-fedreg.htm.

30. Financial Services Modernization Act of 1999 ("FSMA"), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 U.S.C. & 15 U.S.C.). The FTC published its final rule implementing the FSMA on May 24, 2000, with full compliance required by July 1, 2001. Privacy of Consumer Financial Information, 65 Fed. Reg. 33, 677 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313). *See also* Electronic Fund Transfer Act, 15 U.S.C. §§ 1693, 1693a-r (1994 & Supp. 1998) (establishing rights, liabilities, and responsibilities of participants in electronic fund transfer systems for the provision of individual consumer rights); Fair Credit Billing Act, 15 U.S.C. §§ 1666, 1666a-j (1994 & Supp. 1998) (establishing a consumer's rights and a creditor's duties in resolving alleged errors in an open-end credit (e.g. credit card) account and applying generally to disputes about goods or services that are not accepted or delivered as agreed, but not covering disputes relating to quality of goods or services a consumer accepts); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3420, 3422 (1994 & Supp. 1998) (specifying what a bank must receive before it can release customer information to a federal agency; this applies to disclosure of financial records and response to customer authorization, administrative summons, subpoenas, search warrants, formal written requests or judicial subpoenas. Contrary to the Act's title, it does not establish a general right of financial privacy); Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (1994 & Supp. 1998) (criminalizing hacking if hackers gain unauthorized access to computer systems, whether they intend to damage the system or not).

31. 42 U.S.C. § 1320a-7e (Supp. 1998). For the complete Act, see Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

lection and use of data from children age thirteen and under.[32] The Electronic Communications Privacy Act governs the means of turning over information from electronic databases to law enforcement agencies.[33] Federal anti-eavesdropping and wiretapping laws prohibit the third-party interception of electronic communications, except under very limited circumstances.[34]

The statutes creating and defining certain federal agencies have been interpreted by those agencies to create jurisdiction over data privacy regulation. The Federal Trade Commission has been particularly active with respect to domestic data privacy matters, and the Department of Commerce has been active with respect to international data privacy matters.[35]

Previous federal efforts to regulate the content of Internet communications, particularly with respect to indecent or offensive speech, have been invalidated under the First Amendment.[36]

B. State Statutes And Regulations

It is beyond the scope of this article to delineate the full panoply of state statutes and regulations governing data privacy.[37] Relevant state statutes may include a deceptive trade practices act,[38] electronic eavesdropping act,[39] anti-harassment and/or anti-stalking act, and industry-specific statutes covering data practices in

32. 15 U.S.C. §§ 6501-6506 (Supp. 1998).

33. 18 U.S.C. §§ 2510-2513, 2515-2522 (1994 & Supp. 1998).

34. *Id.*

35. *See* Federal Trade Commission Act, 15 U.S.C. §§ 41-57, 57a-c, 58 (1994 & Supp. 1998).

36. Am. Civil Liberties Union v. Reno, 217 F.3d 162, 163 (3d Cir. 2000). Restrictions on *obscene* speech have been upheld under criminal jurisdiction. *See, e.g.*, United States v. Hilton, 167 F.3d 61, 67 (1st Cir. 1999); United States v. Thomas, 74 F.3d 701, 701 (6th Cir. 1996).

37. I asked an associate in our firm to go through just the Minnesota statutes to determine every law which addresses data privacy. She dropped on my desk two large binders of laws, all *in addition* to the data privacy laws catalogued by the Revisor of Statutes at MINN. STAT. § 13.99 (1998). Unlike the law of product liability, such as *Products Liability* by Louis R. Frumer and Melvin I. Friedman, there is no single reporter or looseleaf service yet compiling and organizing the law of data privacy for the fifty states, or even at the federal level. LOUIS R. FRUMER & MELVIN I. FRIEDMAN, PRODUCTS LIABILITY (Supp. 2000).

38. National Conference of Commissioners on Uniform State Laws, Uniform Deceptive Trade Practices Act (1966), enacted in Minnesota at MINN. STAT. §§ 325D.43-325D.48 (1998).

39. *See* Reporters Committee for Freedom of the Press, *Can We Tape?: A Practical Guide to Taping Phone Calls and In-Person Conversations in the 50 States and D.C., at* http://www.rcfp.org/taping/index.html.

insurance, health care, banking, human relations departments, and elsewhere.[40]

States also attempt to regulate the content of Internet communications, but similarly run afoul of the First Amendment[41] or the dormant Commerce Clause.[42]

C. *State Common Law*

Most of the fifty states recognize some part of the common law of privacy.[43] The high court of the most recent state to recognize invasion of privacy torts, Minnesota, described the privacy interest protected by the common law:

> Today we join the majority of jurisdictions and recognize the tort of invasion of privacy. The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.
>
> Here [plaintiffs] Lake and Weber allege in their complaint that a photograph of their nude bodies has been publicized. One's naked body is a very private part of one's person and generally known to others only by choice. This is a type of privacy interest worthy of protection. Therefore, without consideration of the merits of Lake and Weber's claims, we recognize the torts of intrusion upon seclusion, appropriation, and publication of private facts.[44]

It is an oversimplification to describe "invasion of privacy" as one tort. In actuality, "invasion of privacy" has been employed as the general rubric to subsume four separate privacy torts: (a) intrusion upon seclusion; (b) misappropriation; (c) publication of private facts; and (d) false light publicity.[45] The first and third of these

40. Lawyers, of all people, should be sensitive to data privacy issues, in that lawyers routinely work with confidential client information, under strict ethical and evidentiary rules limiting (or requiring) disclosure. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (1983) (amended 1998).

41. State v. Weidner, 611 N.W.2d 684, 694 (Wis. 2000).

42. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 167 (S.D.N.Y. 1997).

43. Eric Jorstad & John Borger, *Invasion of Privacy: Minnesota's New Torts*, 55 MINN. BENCH & B. 38, 38-41 (Oct. 1998); BRUCE W. SANFORD, LIBEL AND PRIVACY § 11.2.1, at 525 & n.4 (2d ed. 1991 & Supp. 1994).

44. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998).

45. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 652 (B)-(E) (1976).

torts are particularly apt to be applied to data privacy, as it has been discussed in this article. Although tortious intrusion upon seclusion developed in the geo-world context of physical intrusion upon physical seclusion, it may be applied to intrusion upon *data* seclusion in the cyberworld where one has a reasonable expectation of privacy in the data and the other essential elements of the tort are met.[46] Similarly, tortious publication of private facts may be especially appropriate in the context of the Internet, where everyone with a computer and a modem may be a "publisher" of erstwhile private data to the entire cyberworld.[47]

Where the information published in cyberspace is false (not true, as presupposed for the above variants of tortious invasion of privacy), there may also be a remedy in the state common law of defamation.[48]

D. European Union

In the late 1990s, the European Union took the initiative to regulate the creation, maintenance and transborder transmission of data involving European data subjects with the adoption of the Data Privacy Directive.[49] The Directive regulates the free movement of data containing personal information. After considerable diplomatic and commercial consternation about differences between the Directive and data privacy practices in the United States –and the impact of those differences on trans-national businesses– the U.S. Department of Commerce and the European Union agreed to "Safe Harbor" provisions which now effectively govern the European data practices of U.S. enterprises.[50]

There are seven basic principles to the European Union Data Privacy Directive, as implemented for U.S. businesses through the Safe Harbor provisions:

- *notice* to data subjects of data practices;
- *choice* by data subjects to opt-out of those practices;
- *onward transfer* of data consistent with described practices;

46. *See* Eric Jorstad, *Invasion of Privacy in Minnesota* (Jan. 1999), *at* http://www.faegre.com/articles/article_208.asp.htm.

47. Am. Civil Liberties Union v. Reno, 217 F.3d 162, 169 (2000); *cf.* David Phelps, *Judge Limits Salary Data in Web Case,* STAR TRIB., Mar. 29, 2000, at 1D, *available at* 2000 WL 6966479 (posting certain sensitive information permitted).

48. Eric Jorstad, *Online Business Defamation: How to Respond to "Cybersmearing"* (July 2000), *at* http://www.faegre.com/articles/article_414.asp.

49. Data Privacy Directive, 95/46 EC, 1995 O.J. (L 281).

50. Dep't of Commerce, *SafeHarbor, at* http://www.export.gov/safeharbor.

- *security* of data protected by prescribed protocols;
- *integrity* of data use consistent with the purposes for which data were collected;
- *access* to personally-identifiable data, with the opportunity to correct it; and
- *enforcement* through national administrative agencies.[51]

These principles may come to guide general data privacy practices in the United States, although there is hot debate concerning the nature of access, the kind of choice, whether notice should be mandatory, the adequacy of various security measures, and federal agency versus state agency versus judicial enforcement of alleged privacy violations.[52]

E. Self-Regulation

Pre-existent industry and trade associations have taken a keen interest in data privacy regulation, and various ad hoc groups have formed to create voluntary guidelines and certifications. The National Association of Insurance Commissioners, for example, has published model statutes concerning privacy of insurance, health, financial and other personal information.[53] The Online Privacy Alliance is an organization of cyber-companies determined to develop voluntary privacy compliance principles and to stave off governmental privacy regulation.[54] The Individual Reference Service Group ("IRSG") is an association of data research companies which provide information–for a fee–investigating individual or business assets, location, criminal history, judgments, UCC filings, and so on. The IRSG has developed an extensive and detailed set of voluntary privacy principles for its members' compliance, together with a system of independent third-party certification (like an audit) of compliance.[55] The Better Business Bureau has developed an online version of its consumer-friendly voluntary reporting system;[56]

51. *Id.*

52. Federal Trade Commission, *Privacy Initiatives, Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security* (May 15, 2000), *at* http://www.ftc.gov/acoas/papers/finalreport.htm.

53. *See* Health Information Privacy Model Act (1998), Privacy of Consumer Financial and Health Information Regulation (2000), and Insurance Information and Privacy Protection Model Act (1980), *at* http://www.naic.org/1papers.

54. http://www.privacyalliance.org.

55. Individual Reference Service Group, *Industry Principles* (Dec. 1997), *at* http://www.irsg.org/html/industry_principles_principles.htm.

56. http://www.bbbonline.org/privacy/index.asp.

and the "TrustE" certification logo has appeared on many Web sites indicating participation in that organization's voluntary data privacy program.

IV. PRESERVING THE PRIVACY PARADOX IN PRACTICE

Watching the sheriffs come swaggering into cybertown, it is tempting to adopt the view of Henry David Thoreau who once wrote, "If I knew for a certainty that a man was coming to my house with the conscious design of doing me good, I should run for my life."[57] Thoreau's worldview is also tempting in his attempt to create "Walden Pond," a utopian community set apart from commercial culture. That is an extreme answer to privacy fears, however, in the age of *caveat orator.* There is always one solution to the fear of misuse of one's personal information: stop communicating with others. Create your own "Walden Pond" retreat.

At the other extreme, cyber dreamers envision a united, wired world of free and universal communication, an electronic utopia that welcomes everyone in a new Republic of Silicon. Our language encourages this vision, expressed most powerfully in the metaphor driving the Cyber Age: "World Wide Web." We are unified in the emerging multicultural, transnational, democratic, interconnected, synergistic web metaphysic. Reasonable skeptics (and unreasonable conspiracy theorists) may note that the heart of the metaphor, "web," necessarily includes a spider who does the weaving and whose goals are neither aesthetic nor altruistic. We are united in a single reality by the web: we are *prey.*

Most of us inhabit the space on the continuum between the utopian/paranoid retreatists and the utopian/paranoid ecumenicists. The extremes illustrate the conflicting tendencies facing businesses and policy makers trying to address privacy concerns responsibly. How can we develop reasonable privacy policies which provide both safety and free communication?

Trying to craft privacy policy in these transformative times is like trying to write a jazz mass in Latin. It can be done. But there is something fundamentally grating, some basic, clashing cultural and linguistic forms that don't (yet) feel like they belong together. For lawyers, this clash is particularly awkward, because legal norms develop and mature at a slower pace than business and cultural

57. HENRY DAVID THOREAU, *Walden, in* WALDEN AND OTHER WRITINGS 70 (B. Atkinson ed., 1937).

norms. Some courts are starting to "get" the Internet, and what it means for jurisdiction, the First Amendment, and the like. But judges still wear robes, after all. Most courts still don't even allow cameras in the courtroom. Having resisted the video age, and presiding amidst the trappings of eighteenth century England, courts are not at the leading edge of the regulation of the *caveat orator* cyber world. Lawyers habituated to the judicial culture are also ill-equipped to structure privacy policy in the new Age.

But there is something important lawyers can preserve and, ideally, adapt for the cyber world. Good lawyers have good judgment, with flexibility to apply basic norms in changing contexts and to predict what courts will, eventually, do. It is precisely that kind of leadership which is needed to create workable privacy policies.

It is impossible to prescribe one "privacy program" to guide privacy policy development in every situation. Nevertheless, certain factors and dynamics may be helpful to identify. My audience is particular entities, be they business or nonprofit, with some side glances toward governmental legislators and regulators. I propose a three-part privacy policy paradigm to structure the privacy process: integrity, participation and challenge.[58] This is an ongoing process that builds in the dynamic tension of the privacy paradox.

A. *Integrity*

As recent lawsuits attest, perhaps the most important part of any organization's privacy policy is to "practice what you preach."[59] State Attorney Generals and federal regulators scrutinize the privacy practices of organizations under consumer, charitable, and other fraud standards, to ensure that the practices comport with the stated privacy policies.

The issue for organizations, however, goes deeper than avoiding embarrassing lawsuits and bad press. The prerequisite to integrity is to *know who you are* and to *know what you are doing.* It may be quite a challenge to meet these prerequisites, especially for large or multi-faceted organizations. To understand the potential enormity, ask this preliminary question: Where is data maintained within the organization that might be subject to privacy concerns?

58. Or, if I modify the third part to read, "overhaul" instead of "challenge," we have a privacy policy acronym tailor-made for the dot-com world: IPO.

59. *See, e.g.*, State of Minnesota v. Minn. Pub. Radio, No. C5-99-11388 (arising out of the Minnesota Public Radio's donor list-sharing practices; settled August 4, 2000) (complaint on file with author); *In re* GeoCities, *supra* note 8.

The thorough way to meet these prerequisites is to conduct a data privacy inventory ("DPI"). The organization should know every situation and place where any person or system in the organization collects, maintains, discloses or transmits PID. There should be a map or flowchart showing the dynamics of collection, maintenance and transmission of PID. This inventory should include:

- type of data;
- source of data;
- purpose(s) for which data were collected;
- software format of database;
- physical location of database;
- security of data (firewalls, passwords, etc.);
- who has the ability/authority to enter data, access data, transmit data in bulk, and/or transmit data as to one data subject– and for what purposes;
- who provides and oversees that authority to enter, access and/or transmit data; and
- how collection, maintenance, and disclosure of data are documented.

In addition, the inventory should identify what vendors or service providers have access to PID maintained by the organization; then review all contracts with vendors and service providers for levels of compliance currently required. Do these contracts include non-disclosure provisions at least as strict as the organization's own commitments to privacy? The inventory should identify all internal, affiliated, and non-affiliated third parties with which PID are shared.

This is just the prerequisite to integrity. You cannot operate with integrity unless you know, first, how you are in fact operating. The next step is to understand how privacy is integrated with your fundamental organizational mission. This depends on who you are as an organization. Assuming the organization has a "mission statement" or some equivalent, the goal is to analyze mission in terms of privacy issues. A medical device manufacturer, for example, may see its basic mission, in part, in terms of patient and physician *trust* in both the scientific prowess and complete candor of the company. It may want to take an extremely proactive approach to privacy to be (and be seen as) a leader in privacy protection. A retail company, on the other hand, which relies on mass marketing tailored by every available piece of consumer data, may see its basic mission, in part, in terms of expanding customer interest in its

many products. It may want to work chiefly through trade associations to limit or influence governmental regulation of cross-marketing and its use and acquisition of PID for targeted marketing, and be seen as valuing customer choice through complying with industry-standard privacy policies. The analysis will be different for every organization.

Once an organization knows what data it has, and knows how its data privacy policies fit with its basic mission, the organization can take the final step toward integrity: implement data use practices to ensure consistent compliance with privacy goals (and laws).

Implementation should be reviewed with the following matters in mind, in addition to the simple question, are we doing what we say we are doing?

- Know who is in charge of privacy policy.
- Formalize implementation controls and testing.
- Document all compliance procedures developed including the rationale for the procedures.
- Assess whether training in privacy compliance is far-sighted, practical and adequate for the future.
- Anticipate short and long term data, technology, product, channel and geography plans of the organization, including future acquisitions.
- Build into the privacy policies a "responsible flexibility" to be able to adapt and change and respond as the market, technology, laws, attitudes, etc., change. The goal is to maximum business flexibility consistent with compliance.
- Integrate privacy policy into future organizational plans. How does the privacy policy help to meet long-term organizational goals? Brainstorm future markets and channels and relationships.
- Develop procedures to monitor law and media for needed adjustments.
- Consider an annual third-party independent certification (as in a financial audit) that organizational practices comply with organizational procedures and all relevant law.

John Kennedy, as president-elect, spoke to the Massachusetts legislature about the characteristics of leadership. He spoke of the historical qualities of public service, but his comments are appropriate to any organization and apropos to decisions about privacy:

> When at some future date the high court of history sits in judgment on each one of us–recording whether in our brief span of service we fulfilled our responsibilities to the

> state–our success or failure, in whatever office we may hold, will be measured by the answers to four questions– Were we truly men of courage? Were we truly men of judgment? Were we truly men of integrity? Were we truly men of dedication?[60]

Inspiring words. But of course integrity is not the only goal. As the "Mayflower Madam" told the *Boston Globe*: "I ran the wrong kind of business, but I did it with integrity."[61]

B. Participation

The second part of the privacy policy paradigm for particular entities relates not to the goal, integrity, but to the process of working toward that goal. Because "privacy" has become a current "hot button" issue, it is tempting simply to slap together a nice-sounding privacy program, announce it to the world, hope one doesn't get sued, and then move on to the next issue. But, as I have tried to show in Part II of this article, the underlying issues run deeper than today's hot topics. Integrity in privacy policies should go hand-in-hand with *integration* of privacy concerns into the organization's various processes and structures. The development and implementation of privacy policies should involve the participation of all affected.

"Participation" requires an understanding of who should be involved. During the course of conducting a data privacy inventory, *data subjects* and *data holders* should be identified. In addition, there are other possible constituents of the organization who may have a stake in privacy policies. Certain processes should be considered in privacy policy development:

- understand the organizational culture with respect to privacy issues;
- research and understand customer privacy concerns, and be able to show how the organization has responded appropriately;
- involve all organizational stakeholders, including investors, prospective investors (or donors and prospective donors), communities, etc.;
- integrate legal and business considerations with respect to privacy;

60. SIMPSON'S QUOTATIONS, *at* http://www.bartleby.com/63/59/159.html (citing N.Y. TIMES, Jan. 10, 1961).

61. SIMPSON'S QUOTATIONS, *at* http://www.bartleby.com/63/76/1876.html (citing BOSTON GLOBE, Sept. 10, 1986).

•develop a detailed public relations plan for privacy;

•consider whether to develop an advocacy plan on privacy issues before legislatures, state and federal regulators, and courts, perhaps through a trade association; and

•know what competitors or counterparts are doing.

Organizational structure may be affected by this participatory process. Someone "high up" in the organization should take the lead in organizing and running the process, but the person or group in charge at the beginning should be flexible to adapt as issues develop. In some cases, a "Chief Privacy Officer" on the level of a Chief Financial Officer or Chief Operating Officer may be appointed. In other cases, an ad hoc committee or task force may be the best approach. In all cases, assertive leadership is needed along with an openness to the genuine participation and concerns of all affected by privacy issues.

C. Challenge

Because the privacy paradox is inherently unresolvable, no privacy policy will ever be adequate. It is impossible to provide complete safety for individual autonomy and complete openness in the exchange of information at the same time. The best an organization can accomplish is to reach a *balance* appropriate for a given organizational structure, mission, data inventory, and political context ... and then be ready to change.

In the Cyber Information Age ("CIA"), the value of data to an organization will only increase over time. The possibilities for data mining, data applications and data value enhancement are still only emerging,[62] as are information technologies. The global nature of the nascent CIA not only increases the quantity of available data and the number of potential markets, but also increases the *volatility* of data acquisition and use because there are so many different actors involved with so many different agendas and bases of power in so many jurisdictions. If an organization's privacy policy is not already obsolete by the time it is implemented, then the organization is out of touch with the CIA. *Every* privacy policy is temporary.

This complexity and volatility is compounded, in the United States and other countries committed to free expression, by the

62. For example, in journalism there is an organization dedicated to the discovery and use of cyberdata in reporting. *See* National Institute for Computer Assisted Reporting, *at* http://www.nicad.org.htm.

protections for communication like those provided by the First Amendment. Governmental restrictions on data use are problematic. In this light, as well as in light of the global flow of information technology and data, the kind of predictability achieved in the regulated consumer product economy may elude the CIA. To be sure, high-tech and database insurance products are already on the market, and more can be expected. The Safe Harbor reached between the E.U. and U.S. shows the potential for global development of some (possibly) effective data privacy regulatory principles.

But the privacy paradox cannot be avoided.

There will be calls to scale back First Amendment protections in the name of protecting the safety of data subjects. There will be calls to sacrifice the values of free communication for a safety "fix." There will also be calls to get used to the surveillance society of lots of big brothers and big sisters. There will be calls to sacrifice the values of personal autonomy at stake in the ability to restrict access to unwanted intrusions. And there will be calls to limit state or even national jurisdiction over data use in order to develop effective international regulatory bodies or tribunals. The cyber sheriffs are pretty good at what they do.

I would not pretend to predict the long-term effect of current trends in the CIA or its erstwhile regulation. I can only note the critical importance of both sides of the privacy paradox, the dynamism of its inherent tension, and suggest possible effects of proposals to lop off one side or the other.

This is why I call the third part of the privacy policy paradigm *challenge*. As one newspaper editor said to a conference of colleagues: "Let there be a fresh breeze of new honesty, new idealism, new integrity. You have typewriters, presses and a huge audience. How about raising hell?"[63] Computers have replaced typewriters, and the number of "presses" has multiplied with the speed of the expansion of the Internet. But the advice is the same. A fresh breeze is needed. In the CIA, the irony of privacy policy development is that every policy and every regulation will always miscarry. The only way that organizational integrity and participation can be effective is to continually challenge organizational integrity and participation. Ultimately, it is the unresolvable nature of the priv-

63. SIMPSON'S QUOTATIONS, *at* http://www.bartleby.com/63/32/8032.html (citing Jenkin Lloyd Jones, Editor, Tulsa Tribune, speaking to Inland Daily Press Association, as reported in U.S. NEWS & WORLD REP., May 28, 1962).

acy paradox which gives the issue its dynamic power to catalyze organizational processes.