



# Stanford Technology Law Review

## Where Everybody Knows Your Name:

### A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange

KENT WALKER\*

[HTTP://STLR.STANFORD.EDU/STLR/ARTICLES/00\\_STLR\\_2](http://STLR.STANFORD.EDU/STLR/ARTICLES/00_STLR_2)

#### I. INTRODUCTION

¶1 Privacy is good and privacy is grand. It is arguably “the most comprehensive of rights and the right most valued by civilized men,”<sup>1</sup> “a shield that protects the sword of liberty,”<sup>2</sup> and an “aspect of individual liberty” that implicates “self-possession, autonomy, and integrity.”<sup>3</sup> It is perhaps essential to “the capacity for creativity and eccentricity, for the development of self and soul, for understanding, friendship, and even love.”<sup>4</sup> And it may well be that “the struggle over privacy is the preeminent issue of the Information Age.”<sup>5</sup>

¶2 And yet. And yet . . .

¶3 Privacy, construed as the withholding of personal information from others,<sup>6</sup> keeps you from enjoying all that society and the market have to offer. Perhaps more troubling, withholding such information sometimes reduces these benefits for everyone else as well. My goal in writing this article is to stress the ever-increasing individual and community benefits of information exchange and to raise a few cautionary flags about the potential costs of regulating how we exchange information about ourselves. My argument is obviously not against privacy, but rather in favor of a sound balance of privacy and other virtues.

#### A. *Defining Privacy*

¶4 Let’s start by defining terms. “Privacy” comes from the Latin word meaning “to separate or deprive,” referring to the distinction between what belongs to the

\* Kent Walker is General Counsel of Liberate Technologies. He was formerly Associate General Counsel of Netscape Communications and America Online, and previously served with the U.S. Department of Justice. The opinions in this article are his own, and do not necessarily reflect those of his present or former employers.

<sup>1</sup> *Olmstead v. United States*, 277 U.S. 438, 478-79 (1928) (Brandeis, J., concurring).

<sup>2</sup> CHARLES JENNINGS & LORI FENA, *THE HUNDRETH WINDOW: PROTECTING YOUR PRIVACY AND SECURITY IN THE AGE OF THE INTERNET* 190 (2000).

<sup>3</sup> SIMSON GARFINKEL, *DATABASE NATION* 3-4 (2000).

<sup>4</sup> JEFFREY ROSEN, *THE UNWANTED GAZE* 223 (2000).

<sup>5</sup> CHARLES J. SYKES, *THE END OF PRIVACY* 221 (1999).

<sup>6</sup> See note 11, *infra*.

individual rather than the state. Thus, our concept of privacy is bound up with our sense of the proper bounds of community (the polis) and commerce (the agora). Other understandings of privacy that focus on the distinctions between the personal and the public, the market and the state, or private interests and overarching public interests.<sup>7</sup> And many other definitions are certainly possible,<sup>8</sup> but the variety of such definitions leads to confusion. As one example, many people think of privacy as a proxy for security, preventing others from having access to their financial records. In fact, security and privacy are quite different, and the sharing of information is often an essential part of the authentication that is an integral part of security. As another example, some conflate support for the Supreme Court's contemporary cases dealing with a "right to privacy," which actually concern reproductive choice and family autonomy, with support for information privacy

¶5 In practical terms, information privacy is not the "right to be let alone," which carries all sorts of libertarian overtones.<sup>9</sup> Nor is it "the right to an inviolate personality,"<sup>10</sup> which presumably no one opposes. Rather, it is the ability to prevent other people or companies from using, storing, or sharing information about you. It means that you'll get less junk mail (and fewer offers of possible interest to you), that Amazon.com won't track which books you prefer (or be able to suggest new ones of interest to you), that Safeway won't track your buying patterns (or give you discounts in exchange), that cameras won't observe you walking down the street (or catch red-light-runners), or that other people won't know about your interests (or be able to engage you in e-mail chats about them).

¶6 For purposes of framing the contemporary debate about whether and how to regulate the exchange of personal information, the best definition of privacy arguably comes from the seminal modern work *Privacy and Freedom* by Alan Westin, the godfather of the contemporary privacy movement. Westin summarizes informational privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."<sup>11</sup>

### B. *Rational Review of the Benefits & Costs of Information Exchange*

¶7 Using Westin's definition as a touchstone, how should a society collectively decide which claims for control over information warrant legal protection? The fundamental organizing principle of this article is that before leaping to establish new information rights we should carefully review not just the benefits of information privacy, but also the benefits of information exchange and the costs of regulating that exchange. This cost-benefit assessment should not be limited to financial or economic considerations. While such considerations may prove

<sup>7</sup> See PUBLIC AND PRIVATE IN THOUGHT AND PRACTICE (Jeff Weintraub & Krishan Kumar eds., 1997).

<sup>8</sup> E.g., FRED CATE, PRIVACY IN THE INFORMATION AGE 19-23 (1997) (summarizing various perspectives on privacy).

<sup>9</sup> *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

<sup>10</sup> Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

<sup>11</sup> ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). This definition has been widely adopted in the regulatory context. See, e.g., Privacy Working Group, Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, at [http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niprivprin\\_final.html](http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niprivprin_final.html) (last modified June 6, 1995) (using the similar definition of "an individual's claim to control the terms under which personal information— information identifiable to an individual— is acquired, disclosed, and used").

substantial, they should be balanced with the broader interests of individuals and the community as a whole.

¶8 Importantly, this approach avoids assuming the conclusion of many privacy advocates: that “privacy” is a nonnegotiable “right.” In a recent article regarding access to information, a staff member at the Center for Democracy and Technology was quoted as saying, “I liken this to a due process kind of right. Just the very notion that if other people are using data about you, you should get to see it, too.”<sup>12</sup> Yet presumably she did not mean to suggest that she has, or should have, an enforceable legal right to be present when her local baker tells an assistant of her liking for cinnamon rolls, nor would she plausibly claim an enforceable legal “right” to read the list of good customers kept by her local florist. Others have asserted that there should be a property right in personally identifiable information, as though they could collect money from someone every time that person spoke their name.<sup>13</sup> Such examples of course stretch the intent of the speakers, but they demonstrate that these sweeping claims quickly run afoul of common sense notions of how we exchange and use information.

¶9 More generally, leaping to assertions of nonnegotiable rights unfortunately tends to preempt reasoned discussion of the costs and benefits of regulatory action.<sup>14</sup> In the context of privacy, there’s no widespread agreement on the existence or scope of such an absolute right. In fact, public opinion arguably runs to the contrary. The best long-term assessment of public attitudes toward privacy is provided by Columbia’s Alan Westin, who has conducted a series of polls over the last thirty years on this issue. On average, he finds that one quarter of the American public cares deeply about keeping personal information secret, one quarter doesn’t care much at all, and roughly half are in the middle, wanting to know more about the benefits, safeguards, and risks before providing information.<sup>15</sup> Customer behavior in the marketplace— where many people freely provide personal information in exchange for various offers and benefits— seems to bear out this conclusion.<sup>16</sup>

¶10 Thus, rights advocates to one side, a “rational review” of the costs and benefits of privacy and information regulation would seem uncontroversial. And yet the contemporary American debate over information privacy is notable chiefly for the absence of exactly this sort of balanced assessment. For example, the Federal Trade Commission, the American agency that has taken a leading role in proposing privacy legislation, omitted such a review before reaching its conclusions. According to Commissioner Orson Swindle, who dissented from the FTC’s May, 2000 Privacy Report,

[T]he Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. Shockingly, there is

<sup>12</sup> Peter S. Goodman, *Digital Whirl Blurs Policies*, WASH. POST, Sept. 20, 2000, at G3.

<sup>13</sup> See Electronic Privacy Information Center, *Court Ruling Hurts Consumers*, at [http://www.epic.org/privacy/junk\\_mail/decision\\_pr2.txt](http://www.epic.org/privacy/junk_mail/decision_pr2.txt) (June 14, 1996).

<sup>14</sup> AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 183-200 (1999); Declan McCullagh, *Expert: Go Easy on Privacy Regs*, WIRED NEWS, at [www.wired.com/news/politics/0,1283,38893,00.html](http://www.wired.com/news/politics/0,1283,38893,00.html) (Sept. 19, 2000) (citing Professor Richard Epstein).

<sup>15</sup> U.S. DEPT OF COMMERCE & FED. TRADE COMM’N, PUBLIC WORKSHOP ON ONLINE PROFILING, 98-100 (Nov. 8, 1999), available at <http://www.ftc.gov/bcp/profiling/online.pdf>; see also Katie Hafner, *Do You Know Who’s Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1.

<sup>16</sup> Edward C. Baig et al., *Privacy*, BUS. WK., Apr. 5, 1999, at 87-88.

absolutely no consideration of the costs and benefits of regulation; nor the effects on competition and consumer choice; nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced.<sup>17</sup>

¶11 A second report, focusing on online profiling, devoted a total of two pages of a lengthy two-part report to the benefits of collecting this data.<sup>18</sup> The governmental entities that have moved to regulate information flow, including the European Union, the Canadian Parliament, and International Trade Administration of the Department of Commerce (which led the “Safe Harbor” negotiations with the European Union), have similarly failed to conduct a review of such factors.

### C. *Factors Interfering with Rational Review*

¶12 How could this be? Undoubtedly, the current environment is not amenable to conducting a sensible review of the exchange of personal information. As one observer recently noted, the current political setting is a “perfect privacy storm,”<sup>19</sup> a remarkable coming together of various forces pushing for extreme solutions to vaguely identified problems at unknown costs.

¶13 By their nature, privacy concerns lend themselves to individual dramatizations—the touching vignettes loved by reporters and movie writers. It’s certainly easier to paint a sympathetic portrait of Sandra Bullock caught in “The Web” of identity theft than to assess the widely dispersed benefits of a thousand people who received products more cheaply and easily. The problems make for simple stories; the benefits are less obvious. Furthermore, it’s a tempting media story, mixing substance (the hot New Economy) with the sizzle of potential wrongdoing and the human-interest angle of “how do I protect myself.” Unfortunately, our human weakness for vivid imagery often makes for bad public policy, discounting the low-key interests of many in favor of the dramatic troubles of a few. It’s harder to play defense in this context; we tend to take the advantages for granted and the debate often pits the slow but steady evolution of the marketplace against bold but untested proposals for an imagined and cost-free alternative.

¶14 Moreover, privacy is a romantic virtue of heroic individualism and uplifting oratory. Such virtues appeal to journalists, novelists, and screenwriters because they make for better stories. But the bourgeois values of convenience, order, community, and affordability are virtues too, and arguably at least as essential to a functioning society.<sup>20</sup> Such virtues are typically ignored by privacy advocates, or at best dismissed in scornful or condescending asides— but they make people happy in small but tangible and important ways.

<sup>17</sup> U.S. FED. TRADE COMM’N, *PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE 16* (May, 2000), available at <http://www.ftc.gov/os/2000/05/privacyswindle.htm> [hereinafter *PRIVACY ONLINE REPORT— SWINDLE DISSENT*].

<sup>18</sup> U.S. FED. TRADE COMM’N, *ONLINE PROFILING 8-10* (June, 2000), available at <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> [hereinafter *ONLINE PROFILING REPORT*].

<sup>19</sup> Dave Steer of TrustE, quoted in Stefanie Olsen, *Accounting Companies Tackle Online Privacy Concerns*, CNET News.com (Sept. 18, 2000), available at <http://news.cnet.com/news/0-1007-200-2804964.html?tag=st.cn.sr.ne.1>.

<sup>20</sup> See DAVID BROOKS, *BOBOS IN PARADISE* (2000); ETZIONI, *supra* note 14.

¶15 Given these imbalances, it's understandable that those concerned about overbroad regulation have lost the rhetorical battle. The issue is now "privacy"—a virtue that no one opposes per se, but that weights the scales in favor of limiting information exchange—rather than the more sinister "secrecy" or even the more neutral "information sharing" or "information exchange." In contemporary sound-bite politics, such a formulation irreversibly loads the dice. Just as no one is "pro-abortion" or "anti-life," no one can be "anti-privacy," yet that's the only label left by the rhetoric. As Lenin and the Bolsheviks established by claiming the name "Bolsheviks," or "majority party," even though they were in a minority, labels matter.

¶16 In the context of online privacy, privacy advocates have also been able to tap into reservoirs of technophobia, fueled by the rapid advance and proliferation of the Internet and other new technologies. Americans' distrust, both of government and business, has grown over time, amplified by the Vietnam War, Watergate, and more recently by a culture that promotes shows like "The X-Files" and conspiracy-theory cinema. In such an environment, there's an instinctive desire to "control" the increasingly complex world around you, which appeals to the reflexive idea that you should be able to "control" what others say about you. Unfortunately, as discussed below, the regulatory mechanisms for exerting such control carry significant problems of their own.

¶17 Privacy concerns have spawned an entire alarmist genre. Within the last several years an explosion of books argue that your privacy is at risk and offer self-help tips on how to shield your information.<sup>21</sup> Consider the following example of alarmist rhetoric:

Remember, they are always watching you. Use cash when you can. Do not give your phone number, social-security number or address, unless you absolutely have to. Do not fill in questionnaires or respond to telemarketers. Demand that credit and data-marketing firms produce all information they have on you, correct errors and remove you from marketing lists. Check your medical records often. If you suspect a government agency has a file on you, demand to see it. Block Caller ID on your phone, and keep your number unlisted. Never use electronic tollbooths on roads. Never leave your mobile phone on— your movements can be traced. Do not use store credit or discount cards. If you must use the Internet, encrypt your e-mail, reject all "cookies" and never give your real name when registering at websites. Better still, use somebody else's computer. At work, assume that calls, voice mail, e-mail and computer use are all monitored . . . .

According to *The Economist*, this sounds like the paranoid ravings of the Unabomber. In fact, it is advice being offered by the more zealous of today's privacy campaigners.<sup>22</sup>

<sup>21</sup> See, e.g., ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD (1997); JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY (1997); GARFINKEL, *supra* note 3; JENNINGS & FENA, *supra* note 2; MIZELL LOUIS, JR., INVASION OF PRIVACY (1998); ROSEN, *supra* note 4; LARRY SONTAG, IT'S NONE OF YOUR BUSINESS— A COMPLETE GUIDE TO PROTECTING YOUR PRIVACY, IDENTITY, AND ASSETS (2000); ROBERT ELLIS SMITH, BEN FRANKLIN'S WEBSITE (2000); SYKES, *supra* note 5; TECHNOLOGY & PRIVACY (Philip Agre & Marc Rotenberg eds., 1997). For more moderate reviews of the issue, see, e.g., CATE, *supra* note 8; PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

<sup>22</sup> See, e.g., *The End of Privacy*, *ECONOMIST*, May 1, 1999, at 15.

¶18 Book after book on this topic has resorted to (and often led with) dystopian “day-in-the-life” scenarios that appear to be taken from the pages of Kafka or Orwell, or rely on science-fiction-like imaginings of technological abuse presented as tomorrow’s reality.

¶19 The language is often spooky, nightmarish, and replete with florid metaphorical references to “data rape” and totalitarian societies. Of course, some of these books are well-written and thought-provoking. But many are hysterically overwrought, and certainly make for bad guides to public policy. As described below, the dystopian scenarios are typically highly remote, while existing legal limitations or public opinion itself (and the financial damage resulting from “privacy scandals”) often provide significant safeguards against their ever coming to pass.<sup>23</sup>

¶20 As a result of each of these factors, individual companies— who would otherwise have the incentive to defend new uses of information because they, like dispersed consumers, benefit from them— cannot practically oppose regulations for fear of reflexive public opposition. Few if any major corporations have been willing to testify publicly on these issues, opting instead to speak, if at all, via trade associations lest they be branded “anti-privacy.” In making public policy, it’s sometimes wise to be wary of unanimity, which may cloak the stifling of reasoned dissent or lack the rigor that results from the strenuous testing of ideas.

¶21 The result of this constellation of factors— in addition, of course, to the unquestionable expansion of databases in online and offline commerce— has been a dramatic increase in public attention to the issue of privacy. Polls show that the commercial sharing of individual information, a phenomenon as old as business and widespread since the advent of the database, is high on the nation’s list of most pressing concerns,<sup>24</sup> fueled by regular press “scandals” over inadvertently or improperly gathered information and the breathless hysteria of science-fiction.

¶22 Following the polls, Congress and state legislators have seen hundreds of privacy-oriented bills.<sup>25</sup> Those most concerned about privacy have often been politicians distrustful of large organizations— typically liberal Democrats and libertarian conservatives. This confluence has contributed to the frequent description of privacy matters as a bipartisan concern, when in fact they often pit the pragmatic moderates of each party against their brethren on the wings.

#### D. *The Benefits of Privacy*

¶23 In setting out to catalog the litany of advantages associated with the contemporary free flow of personal information, it’s only fair to acknowledge the serious and real benefits of personal privacy. A clear-eyed recognition of those benefits helps focus the assessment of whether it may be appropriate for the government to regulate the flow of information, and, if necessary, how best to do so.

¶24 Certainly, limiting information flow may foster autonomy and intimacy, self-definition and self-evaluation, free association and communication, independent

<sup>23</sup> JOHN HART ELY, *DEMOCRACY AND DISTRUST* (1981). Ely argues persuasively that democratic opinion itself (and not judicial overreaching, as via “substantive due process” review) provides the best check against grossly wrong-headed public policies. A similar analysis arguably applies to a fully informed marketplace.

<sup>24</sup> JENNINGS & FENA, *supra* note 2, at 38; SMITH, *supra* note 21, at 336.

<sup>25</sup> JENNINGS & FENA, *supra* note 2, at 13.

decision-making, and the freedom and creativity that comes from a release from public roles.<sup>26</sup> Complete information about everyone all the time is pretty clearly a bad thing, evoking images of Bentham's PanOpticon, a prison designed to let the guards watch all the prisoners all the time.<sup>27</sup> Social coercion toward good behavior is likely incompatible with the independent judgment and deliberation essential to democracy. In Milan Kundera's phrase, anyone "who was the same in both public and intimate life would be a monster. He would be without spontaneity in his private life and without responsibility in his public life."<sup>28</sup> And the ability to deliberate, discuss, and associate in private are essential to most conceptions of citizenship in a democracy. That said, I do not purport to give a review of the advantages of privacy. The plethora of recent books and articles noted above have examined these virtues at far greater length and with far more eloquence than I can muster here.

¶25 My goal, rather, is to fill out the other sets of factors appropriately considered in setting public policy for the exchange of personal information. The two-fold purpose of this article is to set forth my perception of the benefits of the exchange of information, and to detail the potential costs of improper regulation of that exchange.

## II. THE BENEFITS — MATERIAL AND CULTURAL, INDIVIDUAL AND COLLECTIVE — OF SHARED INFORMATION

¶26 The desire to exercise complete control over your information is understandable as a way of seeking to reduce the chances of financial or reputational injury, or simply blocking undesired access to such information. But what would we— both as individuals and as a society— lose from such a policy? And to what degree should we incorporate such preferences into our systems and our regulations?

¶27 Certainly not all information exchange benefits the individual. Some of it results in annoying efforts to contact you, such as spam or junk mail. But such annoyances— like being pitched by merchants in a bazaar or hectored walking by Speaker's Corner— are often a necessary part of our capitalist economy and open society. And in many cases, there's an awful lot of wheat amidst the chaff. So let's review the benefits of information exchange: Cost, Access, Convenience, Collaboration, Community, Security, Responsibility, and Trust.

### A. Cost

¶28 At a basic level, withholding your contact information typically means that you won't see the discounts and offers that are most likely to interest you— whether those are free videos, discounts on kids' toys, a deal on a new computer when you're in the market to buy one, or a cut-rate airfare to your home town. That kind of tailored discount has real value in reducing the cost of living for millions of Americans. The virtually costless communications of the Internet let consumers and businesses buy and sell less expensively by cutting out the middle-man and the brick-and-mortar overhead. And they facilitate advertising the availability of

<sup>26</sup> CATE, *supra* note 8, at 23-28.

<sup>27</sup> Jeremy Bentham, *Panopticon Papers*, in A BENTHAM READER 194-208 (Mary Peter Mack ed., 1969).

<sup>28</sup> Quoted in SYKES, *supra* note 5, at 213 & n.15.

perishable goods that were never before considered perishable— things like airline tickets, hotel rooms, empty cargo-truck space, and long-distance time.

¶29 More generally, targeted offers reduce marketing and distribution costs for both businesses and consumers, and thus ultimately reduce the prices of all goods and services. Auctions, reverse auctions, and other pricing innovations that let buyers and sellers exchange contact, interest, and bid information reduce prices and create competitive pressures that keep off-line goods less expensive and make people's lives better in very tangible ways.

¶30 Some of this targeting and tracking is automatic, like the discount coupons increasingly printed on the backs of supermarket receipts (e.g., buy peanut butter, get a coupon for jelly.) But much of it requires depositing information in a database for later retrieval, which provides other convenience-oriented benefits and also raises other privacy issues.

¶31 Several emerging business models are mixing individual and collective benefits by using the power of networks to reduce the costs of goods. Mercata and MobShop let consumers join together to enroll for bargains— the more people interested in something, the lower the price. Recent disputes between eBay, Fair Market, and AuctionWatch demonstrate the value of building large auction networks— the more participants, the more variety for buyers and the more sellers get for their goods. Similarly, much of the success of e-commerce sites like Ariba and CommerceOne is based on their creation of networks of interested buyers and sellers communicating information about their offerings and preferences.

¶32 Some savings are controversial, like the recent situation in which Amazon.com charged different shoppers different prices for the same books. The press has been critical of such price discrimination:

Companies on the Web that know consumers' shopping habits and history can engage in sophisticated kinds of discrimination. If a business finds out that you, for example, are not a big spender, it may leave you dangling on help lines, refuse to notify you of juicy deals and discounts, or cut you off as a customer. And you won't even know you've been a victim.<sup>29</sup>

¶33 After receiving unfavorable press coverage, Amazon dropped the practice. But the criticism is largely negative spin on the idea of doing special things for good customers. Through Green Stamps, loyalty programs, and premier frequent-flyer clubs, companies have traditionally offered different promotions and levels of service to different customers. And classical economics holds that such price discrimination is efficient, resulting in the socially optimal production of the goods or services in question.<sup>30</sup> As one economist noted, price discrimination “would obviously be good for Amazon. But it would also be good for the overall book business. Publishers would be willing to publish more titles, book buyers who would otherwise have delayed their purchase until the thing came out in paper would be spared the wait.”<sup>31</sup> And the distributional effects are unclear, since it's

<sup>29</sup> Edward C. Baig et al., *supra* note 16, at 84.

<sup>30</sup> HAL R. VARIAN & CARL SHAPIRO, INFORMATION RULES 40-43 (1999).

<sup>31</sup> Paul Krugman, *What Price Fairness?*, N.Y. TIMES, Oct. 4, 2000, at A31. For a provocative argument about the even more controversial issue of genetic discrimination, see Andrew Sullivan, *Promotion of the Fittest*, N.Y. TIMES MAG., July 23, 2000, at 16-17 (arguing that genetic discrimination is both rational and inevitable— “The irrational cruelty of bias will be replaced by the rational cruelty of fate”— and suggesting the need for new social and insurance structures to cope with that reality).

typically the more affluent who would be less price sensitive, and thus likely to be charged more.

#### B. Access

¶34 A number of new businesses have sprung up in recent years premised on providing new goods and services to consumers in exchange for, or in reliance on, information about them. For example:

Free-PC, Inc. [started] on the premise that people would part with detailed personal information and put up with a constant barrage of ads in exchange for a \$500 computer. Privacy advocates mocked the proposition as a loser. But within days of announcing registration, the company fielded more than 1.2 million applications.<sup>32</sup>

¶35 Like television and radio, many of these new businesses are supported by advertising revenues.<sup>33</sup> Advertising revenues pay for the wide and increasing variety of content and services. Ad revenues are as high as they are for two reasons. First, unlike traditional media in which advertising and selling were distinct, the Internet permits both brand identification and actual purchasing in a single transaction. Second, and more importantly, technology permits precisely focused demographics, which increases the probability that any given viewer will be interested in buying a given product or service. Taking away the ability to focus advertisements would slash advertising revenues, and thus reduce new content and services.

¶36 More traditional goods and services also become available— or are able to enter markets as new competitors— as a result of targeted marketing geared to information about potential customers. Discover, AT&T, and GM credit cards became successful because they were able to use information about consumers and then send them offers in the mail.<sup>34</sup>

¶37 Thus, even the annoying junk mail serves a purpose in expanding the offerings available to consumers. The Direct Marketing Association estimates that more than 132 million adults— two-thirds of the U.S. population— regularly purchase products through direct marketing.<sup>35</sup> In an increasingly advertising-based society, the likely alternative to direct marketing is more mass marketing— more advertisements in other media: television, radio, newspapers, billboards and Web sites. Such mail makes it easier to get a credit card (rather than having to go to the bank for an application), gives you a variety of offers, and makes it easier to compare those offers. The same is true of other products and services— you get more choices as more businesses (including those in other states that otherwise couldn't have reached you) compete for your business. It's thus not surprising that despite recent publicity around privacy and "opting-out," fewer than 2% of Americans have opted

<sup>32</sup> Edward C. Baig et al., *supra* note 16, at 88. The business model eventually proved unsustainable, but Free PC's initial success still illustrates that people will share their personal information when they are aware of direct benefits from doing so.

<sup>33</sup> Hal Varian describes the difficulty of figuring out how to support production of something that must be given away, noting that a leading early idea for the support of radio included a tax on vacuum tubes. Among the other possibilities avoided by the advent of advertising included subscription, "ransom" (a la Steven King's approach with his latest novel), and other incentives not to free ride. Hal Varian, *Economic Scene*, N.Y. TIMES, July 27, 2000, at C2.

<sup>34</sup> Oscar Marquis, *Privacy and Opting Out of Options*, N.Y. TIMES, Sept. 19, 2000, at A28.

<sup>35</sup> *Id.*

out of direct mail solicitations or telemarketing contacts via the Direct Marketing Association's Marketing Preferences Lists.<sup>36</sup>

¶38 Finally, companies like LifeMinders, or those promoting avatars or intelligent agents, are springing up, promising to help people organize and use the increasingly vast amounts of available information. Such services not only rely on advertising, but necessarily require a large amount of information about their customers' preferences in order to make their systems work well.

¶39 Decreased revenue to business may sound unimportant. But consider the effects of burdening this revenue flow:

[G]overnment-created standards for all consumer-oriented, commercial Web sites may cause some online companies, particularly smaller ones, to limit their online services or exit the marketplace altogether. What are the likely effects of the majority's proposed legislation on consumers and competition? Will the advantages of the bigger players be enhanced, while small entrepreneurs face artificial and costly barriers to entry? How will that affect the innovation and provision of services that consumer want? What costs will it impose on consumers who do not care about privacy or are willing to make some tradeoffs?<sup>37</sup>

Such effects are likely especially chilling for small companies not wealthy or politically savvy enough to pay lobbyists to participate in the bill-drafting or lawyers to advocate for them in the implementation.

### C. Convenience

¶40 Having some information about yourself out there in the world offers real convenience that goes beyond dollars and cents. Many people benefit from warehousing information— billing and shipping addresses, credit card numbers, individual preferences, and the like— with trustworthy third parties. Such storage of information can dramatically simplify the purchasing experience, ensure that you get a nonsmoking room, or automate the task of ordering a kiddie meal every time your child boards a plane. Likewise, most people prefer to use a credit card rather than a debit card, trading confidentiality of purchases for the convenience of deferred payment.

¶41 Moreover, giving others information about yourself— your name and preferences— helps others make you feel at home. Like your local restaurant, they know your name, know your “usual,” know that you like a table by the window. Most callers to L.L. Bean like the fact that the customer service representative can greet them by name and access their ordering and shipping information. Shoppers on Webvan appreciate the ability to store their weekly shopping list, avoiding repetitive and time-consuming searches through the virtual aisles. Lands End surfers like the personalized model that lets them “try on” clothes online. Bookbuyers on Amazon.com like the “one-click buy” that retains their credit card information. Shopping online for shoes, music, furniture? Just leave a list of your tentative selections in your online shopping cart and return later if you want to buy them. Giving others information about your purchases has benefits that range from notices of recalls to facilitating technical support to discounts on related products. In the near future, it will likely facilitate intelligent agents that conduct your

<sup>36</sup> Interview with Pat Faley, Direct Marketing Association (Oct. 6, 2000).

<sup>37</sup> PRIVACY ONLINE REPORT— SWINDLE DISSENT, *supra* note 17, at 24 (emphasis omitted).

shopping and store valuable information resources (like music, video, writings, and software applications) on a free-floating network, accessible from anywhere.

¶42 Because these types of information and service come secondhand, via computer rather than direct observation, they can seem spooky or artificial. But the process is the same, and the result is the creation of a “virtual small town” where people know more about each other. In fact, it’s been argued that the rise of “urban anonymity” is a passing phase between the closeness of small town agrarian life and the individualized information society made possible by computer technologies.<sup>38</sup> It’s notable that the “New Economy” was originally called “The Information Revolution,” as rising information density creates an exponentially increasing number of critical mass and network externality effects.<sup>39</sup>

¶43 New technologies accentuate these trends. Personalization (with preferences derived from a user’s conduct), customization (with preferences derived from a user’s expressed desires), and interactivity (a user’s interaction with a website to obtain tailored content) add tremendous value. According to *Business Week*: “At Excite Inc., for example, customers who exchange tidbits about themselves in return for a personalized experience— in the form of selected news, movie listings, local weather, etc.— return to the site roughly 20 times more often than those who don’t.”<sup>40</sup> New products and services are being built around these principles:

Some big computer out there knows all about Joan Schram. Its massive memory has stored the birth dates of family members and friends, the fact that she drives a Ford Explorer, and the names and birth dates of her American shorthair cat and rare Brazilian fila dog.

And she’s thrilled about it.

Schram gave out the info herself, to LifeMinders, Inc., a firm that gives people reminders of important dates, tips on when it’s time to treat the cat for ticks, and news and ads targeted to their interests. ‘You give us information about yourself and we give you a great product in return,’ says LifeMinders’ CEO.<sup>41</sup>

Thus in many cases the terms of exchange of personal information are mutually beneficial, and regulations burdening them should be approached carefully.

#### D. *Collective Benefits*

¶44 Critically, these benefits of information sharing can be collective as well as purely personal. In a very real sense, privacy creates a Tragedy of the Commons effect,<sup>42</sup> in which not sharing information imposes costs on others.

<sup>38</sup> *The End of Privacy*, *supra* note 22, at 16 (citing George Gilder).

<sup>39</sup> VARIAN & SHAPIRO, *supra* note 30.

<sup>40</sup> Edward C. Baig et al., *supra* note 16, at 86 (citing Joe Kraus, Excite’s co-founder and senior vice-president).

<sup>41</sup> John Schwartz, ‘Opting In’: A Privacy Paradox, WASH. POST, Sept. 1, 2000, at H1.

<sup>42</sup> See Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243-48 (1968). Hardin’s classic article reviewed how individual farmers grazed more and more of their cattle on shared lands, leading to overgrazing and ultimately to the Enclosure movement, in which individual farmers took ownership of part of the common. Notably, no individual farmer intended to impoverish the collective, but that result inevitably followed.

¶45 The most ready example is the unlisted phone number. Unlisting a phone number has the same effect as not having your street address visible from the street: it makes it more difficult for others to find you. You may not care about some of those “others”— say, direct marketers who call during dinner— but some “others” are friends, relatives, or business associates who have mislaid your number or with whom you would have gladly shared your number but just never did. A cartoon from several years back had one person telling another of a terrible invention: “It tracks your name, your number, your address, the identities of the people who live with you, and how many phones you have. And they charge you every month if you want to stay out of it! They call it the phone book.” The joke comes at the expense, not just of technophobia, but of the assumption that anything that compromises privacy is bad. But a world without phone directories would have lost an important and useful tool for facilitating communication. Even a world in which participation in phone directories was “opt-in” would result in far smaller, less useful directories (akin to current non-Yellow Pages directories).

¶46 While there’s often little individual incentive to participate in the aggregation of information about people, a great collective good results from the default participation of most people. The aggregation of information often requires a critical mass to be worth doing, or for the results to be worth using. (A phone book with only one out of ten numbers would hardly be worth using, let alone printing.) Opt-out policies for information exchange— leaving someone’s information available for compilation unless they object— can provide exactly the right set of incentives for the best social outcome: People with strong privacy preferences don’t participate, while those with milder preferences do participate, resulting in the inclusion of a critical mass of information that offers value to everyone. In economic terms, the effort required to opt-out effectively internalizes what would otherwise be an uncaptured externality.

¶47 In contrast, the difficulty of tracking down someone’s email (the high-tech equivalent of a phone number) is chiefly due to the reluctance of corporations to allow broad access to their databases of employee e-mail addresses. Afraid that headhunters will poach their prized employees, they complicate the lives of anyone outside the corporate walls hoping to reach those inside. The lack of a means to capture the benefits of widely available information results in outside callers being disadvantaged.

¶48 Another example is Caller ID, which pits different privacy claims against one another. Many people like the notion of an electronic peephole, letting them know who’s at the electronic door before they decide whether to pick up the phone. Yet many people block transmission of their own numbers, valuing protection of their privacy. Neither choice is necessarily right, but it’s worth recognizing that the assertion of the privacy claim affects the contending desires of others. The classic Tragedy of the Commons aspects are clear. From my selfish perspective, I want access to information about everyone else— the identity of who’s calling me, their listed phone number, etc. I want to be able to intrude on others without their knowing who I am (which I can accomplish by blocking Caller ID), and don’t want others to be able to intrude on me unbidden (which I can accomplish by unlisting my phone number). The gain in privacy makes it harder to find the people you want to reach, and harder to know who’s calling you.

¶49 Many of the new systems for processing information depend on universal (or at least strong majority) acceptance to be workable. Think of the phone directory example discussed earlier— the fewer listed numbers, the less value the directory

has. As another example, Intelligent Transportation Systems seek to ease traffic congestion by using peak pricing, charging higher prices at rush hour. To accomplish this without inefficient back-ups at tollgates, cars would have to carry devices to automate the payment of tolls or to allow roadway sensors to track the number of miles traveled or roads used. The more drivers who participate, the better the results for everyone. The individual decisionmaking process fails to capture these collective values.

¶50 This analysis applies to any new technology whose value increases with the number of people who use it or permit their information to be shared. For example, new cellular phone technology permits tracking the speeds of cellular phone users, allowing instant and precise identification of problem areas, and minimizing traffic jams without additional costs. Again, the more people who participate, the more effective the technology. Consider collaborative filtering, which powers Amazon's amazingly useful book recommendations, with accuracy increasing according to the number of participants. If companies had to get the consent of each user, participation rates would fall (because of the free-rider problems described above) and the quality and value of collaborative filtering would decline for everyone.

#### E. *Community*

¶51 It's unfortunate, but perhaps not surprising, that debates over privacy have devolved into traditional business-versus-consumer or government-versus-citizen confrontations. Yet the polarization of the debate as "big guy versus little guy" risks missing the fundamental organizational dynamic of the increasingly multilateral exchange of information. Certainly the exchanges are often sponsored or facilitated by companies, but the participants and chief beneficiaries are often individuals.

¶52 As Robert Bellah and Robert Putnam have persuasively written, the sense of community is in increasingly short supply in contemporary society.<sup>43</sup> In a traditional urban neighborhood, the high density, lack of garages, and presence of stores within walking distance means that you often see your neighbors unloading groceries, walking to the park, or playing with kids on the sidewalk. One or two people stop to chat, and others gather, occasionally creating groups of a dozen parents and kids hanging out on the front stoop. The right kind of urban environment creates the bars and coffee shops that serve as gathering points— ad hoc forms of community reflected in the national popularity of the TV show "Cheers" and the closing line of its theme song: "You want to go/Where everybody knows your name." Too often the alternative is not just the right to be left alone, but being alone.

¶53 How does information exchange facilitate community? While the wider availability of contact information (whether telephone numbers, physical addresses, or e-mail addresses) promotes both offline and online interaction (like getting back in touch with someone you knew in high school or college), the most novel examples are found in the flourishing new online communities. Perhaps the largest example is America Online's Member Directory, in which upwards of 20 million people post personal information about themselves to encourage other people to

<sup>43</sup> ROBERT N. BELLAH ET AL., *HABITS OF THE HEART: INDIVIDUALISM AND COMMITMENT IN AMERICAN LIFE* (1985); ROBERT D. PUTNAM, *BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY* (2000).

contact them about topics of mutual interest, and to give context about themselves when they communicate with others.<sup>44</sup> (Certainly many participants remain pseudonymous even though they establish long-term online personas. While there is the widely publicized error by an AOL staff member that led to the disclosure of Timothy McVeigh's identity to a Navy investigator reviewing his sexual orientation, this exceedingly rare exception among the tens of millions of satisfied users simply proves the rule.) A raft of community-oriented web sites has emerged, building on older chat rooms, Multi-User Domains, and Usenet groups. Sites like epinions.com provide opinions of everything from movies to music to computer software, and then rank those opinions based on your evaluation of the reviewer's prior opinions. TheGlobe.com, egroups.com, Critical Path's InScribe, NBCi.com, Tripod.com, and TalkCity.com offer the modern equivalent of back-fence gossip, with wide-ranging, opinionated discussions of everything from your cheating spouse to Scientology. Yahoo's Geocities provides "homesteaders" with individualized homepages, while AOL's Digital Cities provides discussion focused on your geographic community. Stock chat rooms like those offered through The Motley Fool attract millions of day traders. You can go to Edmunds.com to debate the merits of different cars, or to Women.com to discuss gender issues, or to Charity.com to learn about volunteer opportunities in your area. Voter.com and Grassroots.com are devoted to mobilizing political communities. Meanwhile, browser "tag-along" applications allow all current viewers of any given website to share their thoughts about the contents with other viewers.

¶54 But the advantages aren't limited to explicitly community-oriented sites and technologies. When you click on to Amazon, the site recommends additional books you might like, based on the purchasing patterns of others who have bought the same books in the past. By and large, the recommendations are pretty good. If you live in Manhattan, surrounded by like-minded friends, it's relatively easy to get good movie recommendations or ideas for a book or a restaurant. But if you live in Montana, five miles from your nearest neighbor, it's harder to establish any connection, let alone connections with people who have similar interests. Collaborative filtering and chat rooms allow a virtual community of admirers—whether of Akira Kurosawa films, *The Economist*, or the Toledo Mudhens—to establish links and share ideas, whether they live in the East Village or Bozeman. And every time you sign up for a list, an e-mail alias of friends, or a discussion group of colleagues, you are sharing information about your interests. Other, noncommercial projects like the "SETI@home" initiative (using the power of unoccupied computers to help in the search for extra-terrestrial life) or the Human Genome Project's effort to map the intricacies of human chromosomes, entail the sharing of certain personal information in order to pool the resources of huge numbers of people in pursuit of a common goal.

¶55 Without having information about ourselves out in public, we appear to the outside world as anonymous and interchangeable. Providing such information gives texture to our public persona, permits tailoring of information, and provides traction to others who seek to engage us. Admittedly, there's always a risk of junk mail, prank phone calls, spam, or flame wars. But the difficulties pale in comparison with the benefits. And, as discussed below, fashioning a remedy that appropriately distinguishes between desirable and undesirable communications is challenging at best.

<sup>44</sup> For AOL's claim to 25 million members, see e.g. [http://corp.aol.com/press/press\\_datapoints.html](http://corp.aol.com/press/press_datapoints.html) (talking points for AOL public relations employees). The Member Directory is available to AOL members.

¶56 Some scoff at the forms of "community" created online, especially those sponsored by commercial entities, as weak-tea versions of the rich and multilayered community interactions that we have traditionally enjoyed. There's much to that critique. Ferdinand Tonnies wrote of capitalism as a sea of *Gesellschaft* (market-based society) enveloping the island of *Gemeinschaft* (community) represented by family and, by extension, the local community.<sup>45</sup> Joseph Schumpeter wrote of capitalism as a "gale of creative destruction," sweeping before it older social orders and community ties.<sup>46</sup> On the other hand, many real-world communities are fading away. As more and more people get online, their very numbers and their growing comfort with the medium enrich the online community. Plus, as noted, electronic communications often facilitate and reinforce the creation of offline communities.

¶57 More generally, the market's invisible hand can have many positive social consequences. The role of the phone company in profiting from your use of the line doesn't reduce the value of your conversation with your kids; in fact, it depends on it. The local hardware store's sponsorship of a Little League team, while a form of marketing, is an essential part of the community institution. Communities need the chance for regular interaction to build lasting personal and social bonds. Those interactions, as often as not, stem from the necessity of regular commercial exchange, motivated (at least in the first instance) by self-interest. In contemporary society, merchants increasingly focus on shopping as a social activity— witness the proliferation of bookstores-cum-coffee-bars in every major American city, or the flowering of upscale "farmers' markets." Likewise, online retailers are increasingly adding "community" components to their offerings, providing chances to chat, letting shoppers compare products, and building loyalty to the site.<sup>47</sup>

¶58 But will the market foster only a narrow form of "consumer community?" People have a way of making the naked cash nexus of the market evolve into a broader community. Farmers' markets are civic events, notwithstanding the commercial transactions at their core. As de Tocqueville noted, citizens can often move from advocacy of self-interest into a broader realization of 'self-interest rightly understood' that takes into account community interests.<sup>48</sup> The self-interest of the agora often becomes the civic virtue of the polis.

¶59 The notion that technology can build community dates back at least to Marshall McLuhan's global village, created by broadcast media of all types, distributing shared experiences and building common tastes. To date, the promised global village of broadcast television and movies has proven more broad than deep. While promoting a uniformity of tastes, it lacks nuance or the prospect of interaction. It necessarily panders to the lowest common denominator. As George Gilder has argued:

Television is not vulgar because people are vulgar— it is vulgar because people are similar in their prurient interests and sharply different in their civilized concerns.' Sex, shopping and violence, in other words, are what

<sup>45</sup> FERDINAND TONNIES, COMMUNITY AND SOCIETY (GEMEINSCHAFT UND GESELLSCHAFT) 223-231 (Charles P. Loomis ed. and tr., 1957).

<sup>46</sup> JOSEPH SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY 82-85 (Harper & Row 1975) (1942).

<sup>47</sup> Ellen Neuborne, *Why E-tail Will Click*, BUS. WK. ONLINE, July 24, 2000, at <http://bwarehouse.businessweek.com/cgi-bin/display.cgi?id=39dd19c722b50Mpqaweb1P11005&doc=results.html>.

<sup>48</sup> ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 519-530 (George Lawrence tr., Doubleday 1969).

people have in common. What differentiates them is their enthusiasm for folk music, tropical fish or Viennese waltzes.<sup>49</sup>

In contrast, interactive Internet communities can flourish not just around shopping, but around folk music as well. The advent of interactive and communicative technologies creates a much richer and more varied interchange, and facilitates offline interchange as well.

¶60 Finally, the argument for taking community into account in balancing privacy interests does not suggest that community is an unalloyed good, whether in cyberspace or elsewhere, any more than privacy is. Perhaps the best metaphor came at the 1993 meeting of Computers, Freedom, and Privacy, a leading conference on the social implications of new technologies, where rancher, Grateful Dead lyricist, and sometime social theorist John Perry Barlow gave a speech warning of the potential excess of anonymity and privacy. In his small town, said Barlow, everyone knew everything, and it worked just fine. A small-scale riot almost broke out at the heresy, but there's much truth to the notion.

¶61 While community isn't always an unalloyed virtue, the ultimate question is one of balance and flexibility. Privacy reflects an individualistic ethos, openness and disclosure a communitarian one. It would be no better to have everything public than to have everything private. As Fred Cate puts it:

Despite its benefits, privacy may be seen as an antisocial construct. It recognizes the right of the individual, as opposed to anyone else, to determine what he will reveal about himself. As a result, privacy conflicts with other important values within the society, such as society's interest in facilitating free expression, preventing and punishing crime, protecting private property, and conducting government operations efficiently.<sup>50</sup>

Different social goals drive different regimes of privacy and disclosure. Where candor is valued above all, perfectly consequence-free anonymity may be most appropriate. Where there's a concern about flaming or disruptive behavior, pseudonymity may be best. Where trusting relationships are paramount, full disclosure and personal responsibility is likely called for. But in crafting the rules for the different parts of the world, and in making our individual choices about how we act in that world, certainly the claims of community deserve significant weight.

#### F. Security

¶62 Many people's primary concern with their records is avoiding mistakes. The very identifiers that most concern many privacy advocates— Social Security Numbers, driver's licenses, or universal health care cards— are the keys to ensuring that the information for John M. Smith isn't confused with the information for John N. Smith.

¶63 More broadly, authentication of one's identity is essential to combating fraud and confirming the legitimacy of a request. Locked yourself out of your hotel room without your ID while swimming in the pool? Give the clerk some information (some combination of birthday, Social Security Number, and mother's maiden name) to authenticate your identity, and you're back in your suite.

<sup>49</sup> *The Big Leap*, ECONOMIST, Jan. 15, 2000, at 18 (quoting Gilder).

<sup>50</sup> CATE, *supra* note 8, at 30.

¶64 Distributed information can reduce the costs of fraud and other economic crime. Many websites store passwords and hints to authenticate return visitors. And analysis of patterns of transactions can help to reduce fraud and other sorts of economic crime. For instance, cellular phone companies flag variations from your usual calling patterns in trying to detect whether someone may have surreptitiously stolen your number. The classic ad that shows a concerned Citibank Visa representative calling a customer to report an unusual spending pattern on his credit card illustrates proactive customer service that simply wouldn't be possible without data about his purchasing history.

¶65 In the network environment, confirming your own identity is an essential part of most commercial transactions because it prevents someone else from ordering goods on your credit card. Most network security administrators will tell you that authentication is a critical part of network security. Passwords are integral to controlling access to any electronic system. Signed e-mail confirms from a trusted authority both that the purported author actually sent a document, and that the document hasn't been altered in transit. The advent of identification and authentication technologies thus facilitates all electronic transactions, especially those where trust and security are at a premium. In fact, in many ways a security perspective argues for more, not less, shared information using longer and stronger passwords, unique identifiers, and longer Social Security Numbers (which would be harder to fake and include a check digit).

¶66 While most Americans would gladly trade (and have in fact traded) some degree of privacy for greater security and accuracy of their data, privacy concerns effectively defeated several recent moves toward widespread authentication through negative media stories, threats of lawsuits, and appeals to pro-privacy government agencies. Intel largely disabled the serial number in its Pentium III chip, which would have aided firewall security and identified stolen systems. Microsoft disabled its globally unique identifier (or GUID), which helps the network know where to store a document and represented the key clue in tracking down and apprehending the author of the damaging Melissa virus. And the Internet Engineering Task Force dropped a proposal to add identifying numbers of computer hardware to Internet addresses (which would have helped to address the exploding demand for website addresses).

¶67 Such technologies operate as digital fingerprints, not unlike the paper, ink, and handwriting of a traditional letter, which all provide indicia of authorship. It is not at all clear that we want or need to increase the default level of anonymity, making every document the equivalent of the kidnapper's ransom note pasted together from scraps torn from magazines. Jeffrey Rosen has argued that technology takes away privacy and that anonymity can redress the balance,<sup>51</sup> but that equation seems flawed. Technology promotes more information exchange in some areas, less in others. For example, we have never previously had methods of creating a document or sending a mass communication that gave no clues about its source. On the other hand, technology removes the areas of gray to which we're accustomed. Authenticating technologies have the potential to identify their author (or at least the authoring machine) with a high degree of certainty, removing the residual ambiguity of handwriting analysis or identification of typewriter keys and

<sup>51</sup> ROSEN, *supra* note 4, at 167-68.

thereby increasing the security of sending financial or other sensitive information online.<sup>52</sup>

¶68 From the perspective of law enforcement, the result is likely to be a reduction in crime. Prepaid calling cards helped to establish the guilt of the Oklahoma City bombers. The Vehicle Identification Number and truck rental information were used to track down the bombers of the World Trade Center. And, as noted above, the GUID in Word enabled law enforcement to apprehend the creator of the Melissa virus. Deterring such crimes provides a real social benefit, and necessarily weighs in the balance against new decisions to prevent or discourage the use of identifying information.

### G. Accountability

¶69 Social norms encourage us to do the right thing. Prevailing norms and social sanctions help structure and order society, counteracting the tendency of pure economic man to free-ride or abuse freedoms.<sup>53</sup> Communities rest not only (nor even chiefly) on laws, but rather on norms and mores, which work on a far more subtle and fine-grained basis than centralized command-and-control regulation can ever hope to achieve. People mow their lawns not because of laws requiring them to do so, but because of what the neighbors might think (and their own internalized sense of propriety).

¶70 Anonymity disables these critical social stabilizers. Anonymity prevents the connection of personal information with the person, and arguably represents the central element of most privacy claims. While anonymity has great value in protecting the free speech of dissidents and minority viewpoints, it cannot be a fundamental organizing principle for a well-ordered community.<sup>54</sup> Not for nothing do we think of evening as the more dangerous time of day. Anonymity can operate as the cloak of night, often promoting negative behavior and disregard for the rules that organize social interaction.

¶71 Imagine, if you will, a society of complete anonymity. We already have a pretty good proxy: the freeway—the arena of rudeness, abuse, discourtesy, road rage, and the occasional drive-by shooting. It's hard to imagine people acting in the grocery store the same way that they behave on the freeway, pushing their carts ahead of others in line and making nasty gestures to people in the aisles. The incentives for good behavior grow even stronger when you're in your neighborhood, your office, or a local store where you know the other shoppers and they know you.

¶72 As Stewart Baker has written:

[W]e may sometimes value anonymity for ourselves, but we almost always mistrust it for others. A signed love letter is flattering; an anonymous love letter is creepy. Respectable newspapers rightfully refuse to publish

<sup>52</sup> Robert Lemos, *Digital signatures a threat to privacy?*, ZDNET NEWS FROM ZDWIRE, Apr. 7, 2000, available at 2000 WL 4020034, and <http://www.zdnet.com/zdnn/stories/news/0,4586,2523596,00.html>.

<sup>53</sup> See generally Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 412-416 (1997).

<sup>54</sup> For contrasting views emphasizing the importance of anonymity as a fundamental human right, compare Al Teich et al., *Anonymous Communications Policies for the Internet: Results and Recommendations of the AAAS Conference*, 15 INFO. SOC'Y 2 (1999), available at <http://www.slis.indiana.edu/TIS/abstracts/ab15-2/teich.html>, with Lee Tien, *Who's Afraid of Anonymous Speech?*, 75 OR. L. REV. 117 (1996). See also McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (holding prohibition on anonymous political speech unconstitutional).

unsigned letters to the editor. And none of us would want to walk in a city where all the pedestrians were masked.<sup>55</sup>

¶73 Socrates maintained that he always behaved in the same way in public as in private— that is, he had internalized the effects of social sanction, and did what he should do, not what he could get away with.<sup>56</sup> In other words, he acts in a way that he would be proud to have others know about.

¶74 As Adam Smith concluded in *Reputation*:

While a man remains in a country village, his conduct may be attended to, and he may be obliged to attend to it himself . . . . But as soon as he comes to a great city, he is sunk in obscurity and darkness. His conduct is observed and attended to by nobody, and he is therefore likely to neglect it himself, and to abandon himself to every low profligacy and vice.<sup>57</sup>

¶75 On the Internet, perhaps the best example is the distinction between the behavior of those using webmail (typically free and anonymous) and subscription-based e-mail via an Internet service provider (who for billing purposes necessarily knows the true name and address of the subscriber). In my experience, webmail users create a disproportionate number of complaints about abuse and spam, while subscription e-mail users, subject to the potential loss of their account and even criminal sanctions, are relatively less disruptive.

¶76 In an effort to establish an intermediate sort of accountability, many chat rooms and similar institutions operate with pseudonymity, where participants sign in with a *nom de screen* and use that name throughout their interaction with the group. While the social constraints thereby imposed are weak, they typically suffice in an environment where all that's at stake is the interaction of the players. Those that value the online interaction act as responsible and contributing repeat players, to whom reputational capital is important. However, where potential offline gains dwarf the value of online participation, problems result. The easiest example is stock chat rooms, where thousands of investors regularly try to "pump and dump"— driving up prices with false takeover talk in order to sell at a premium— or spread false negative rumors to profit through short-selling. Another example comes from the online auction house eBay, which has set up an elaborate system of user feedback designed to quickly establish "reputations" for sellers as trustworthy. But this system, based on pseudonyms, is still subject to manipulation and evasion: online auctions accounted for 87 percent of internet fraud in 1999.<sup>58</sup>

¶77 As Fred Cate notes, "[t]he opportunity to mislead is inherent in legal protection for 'the claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,'"<sup>59</sup> and creates a cost that public policy must take into account.

<sup>55</sup> Stewart Baker, *Privacy, Anonymity, and the Attack on Authentication Technologies* (1999) (unpublished manuscript).

<sup>56</sup> Plato, *Apology of Socrates* 33a.

<sup>57</sup> Quoted in SYKES, *supra* note 5, at 241.

<sup>58</sup> *Online Auctions No. 1 in Internet Fraud*, CNN.com, Oct. 2, 2000, at <http://www.cnn.com/2000/TECH/computing/10/02/i.fraud/i.fraud.sidebar/index.html>.

<sup>59</sup> CATE, *supra* note 8, at 28.

## H. *Trust*

¶78 Trust— an eighth benefit of the exchange of personal information— differs a bit from the others, but is worthy of mention. It can be a direct result of such exchange, but it is also an approach to information sharing and a product of a society in which we feel comfortable sharing information. While it may be premised on community, security, and accountability, trust has a value that goes beyond the concrete benefits of those virtues. In a rural environment, it might take the form of feeling that you don't need to lock your car or your house at night, with psychological and social benefits that go beyond not having your car stolen.

¶79 But trust takes tangible manifestations as well. Nations lacking the widespread social lubricant of trust are forced to resort to cumbersome modes of exchange and strict and legalistic means of enforcement to assure the performance of everyday commercial exchanges. Imagine the world if you were a merchant who thought it likely that most of your customers sought to cheat you— you wouldn't accept checks or credit cards, and you would invest large sums in security guards and alarms. A bad-check percentage of 1% is acceptable; a bad-check percentage of 20% puts you on the road to an all-cash or barter-based economy. In a high-trust society, the costs of authentication and confirmation drop dramatically, enabling whole new forms of economic exchange. By way of example, the widespread U.S. use of credit cards reflects the trust engendered by a sophisticated financial clearing system. Europeans, lacking such a system, are far more constrained in their financial dealings. As a general rule, the fewer the locks, the happier the society, and vice-versa.

¶80 The question is whom you trust to have access to your information. In the commercial context, people generally trust a company not because it doesn't exchange or trade information, but because it gives them what they want in a timely fashion. You determine every day whether a company will deliver the goods, refund your money, follow through on the warranty, pay out the insurance claim, or notify you of product recalls. Many consumers already trust many companies, based not on a privacy policy but rather on a constellation of brand, imagery, reputation, explicit statements, individual experience, and the specific risks involved in providing specific information. You trust L.L. Bean largely because they're big. They have skin in the game and a stake to protect. Their size makes it likely that they'll be more reliable than a fly-by-night operation, and you know where they live (affording at least the theoretical potential for calls, visits, and even legal action if there's a problem). Perhaps most significantly, as repeat, long-term players in the catalog business, L.L. Bean has strong incentive to keep customers happy, promoting future buying and reducing public complaints. You may have had positive dealings with them in the past, and their marketing— painting a picture of pleasant, helpful, and reliable folks— helps to crystallize the impression. In sum, trust is established by economic incentives and exposure to legal action, which all result from your knowledge of who and where they are. Not coincidentally, it's a reciprocal relationship. Should you call for help in resolving a question or problem, a company's trust in you is established by their knowledge of your valid credit card number— likely reflecting a decent credit history— and your record of having done business with them in the past.

¶81 In comparison to these daily concerns, privacy consequences are often indirect, delayed, opaque, and (for most people) relatively minor. Certainly, more legal requirements mandating given practices are one way of promoting such trust, but hardly the only or necessarily the best way. A trust relationship typically reflects a

complex and fine-grained assessment— not one readily susceptible of one-size-fits-all government regulation or mandate.

¶82 Many privacy advocates call for narrowing circles of trust. But in a complex modern society, it's difficult or impossible to tell in advance whom you might want to have contact you, or who might have something of interest to offer. The idea of limiting trust to people you have known for years is unduly circumscribed and unworkable. The authors of *The Hundredth Window* take as their guiding metaphor an image of living in a castle next to a rich and vibrant bazaar, and the consequent need to lock all of your windows lest a thief enter.<sup>60</sup> Yet the world contains more honest men than thieves, and there is value to living in a society of unlocked doors just as there are costs to living in a society of barred windows. Sometimes it is not only necessary but wise to trust the kindness— or at least the honesty— of strangers.

### III. THE COSTS OF INFORMATION REGULATION

¶83 It's always easy to find fault with the status quo, and the business world's halting efforts to come to grips with the rapid proliferation of information flows has certainly provided fodder for critics. But it's not at all clear that the government would do a better job than the private sector in overseeing the handling of such information, and regulatory initiatives would come at a cost. What then are the costs of regulating the exchange, storage, and use of personally identifiable information?

¶84 FTC Commissioner Orson Swindle has forcefully articulated a number of the costs of information legislation.<sup>61</sup> While my discussion is not limited to questions of online privacy, the various reports of the U.S. Federal Trade Commission, the dissents from those reports, and the report of the FTC's Advisory Committee, nicely frame many of the larger issues raised by general privacy regulation. Professor Eugene Volokh has made a powerful case that "The United States already has a 'code of fair information practices,' and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits)."<sup>62</sup>

¶85 The first order of business for any regulator is to conclude that markets are failing in their normal role of serving the public good. Neither the European Union nor the other governmental agencies that have legislated to date appears to have made findings that would support such a conclusion. As FTC Commissioner Swindle has repeatedly observed, evidence of a market failure regarding information exchange is at best unclear.<sup>63</sup> And private companies are devoting increasing time and resources to address privacy concerns.<sup>64</sup> FTC Commissioner Thomas Leary noted this in May, 2000:

<sup>60</sup> JENNINGS & FENA, *supra* note 2, at 26.

<sup>61</sup> PRIVACY ONLINE REPORT— SWINDLE DISSENT, *supra* note 17, at 20-26.

<sup>62</sup> Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (citations omitted); *see also* PRIVACY ONLINE REPORT— SWINDLE DISSENT, at 24-25.

<sup>63</sup> *See, e.g.*, U.S. FED. TRADE COMM'N, ONLINE PROFILING— DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE, at 2 (June, 2000), available at <http://www.ftc.gov/os/2000/06/profiling2000.htm> [hereinafter ONLINE PROFILING REPORT— SWINDLE DISSENT].

<sup>64</sup> George Vradsburg, Testimony before the U.S. Senate Commerce Committee (Oct. 3, 2000), available at <http://www.senate.gov/~commerce/hearings/1002vra.pdf>.

[The overall thrust of the Report is that any privacy policy should, at a minimum, recognize substantive consumer rights in each of these areas. What the Report does not do is adequately explain why. . . . The Report does not explain why an adequately informed body of consumers cannot discipline the marketplace to provide an appropriate mix of substantive privacy provisions.<sup>65</sup>

At best, the Report vaguely argues that “the industry’s limited success in implementing fair information practices online, *as well as ongoing consumer concerns about Internet privacy*, make this the appropriate time for legislative action.”<sup>66</sup> Basing legislation on poll numbers rather than analysis is treacherous for all the reasons identified above.

¶186 But even assuming the existence of a market failure, the issue becomes whether legislation and regulation will do a better job or merely substitute their own failings for those of the market. In her foreword to *The Hundredth Window*, Esther Dyson writes that privacy used to result from friction, but that the flow of information is increasingly friction-free.<sup>67</sup> Certainly, regulating that flow would reintroduce some of the old-style friction into the equation, but whether that is a desirable outcome is unclear. As a Brookings Institution conference discussing the conclusions of Fred Cate’s *Privacy in the Information Age* summarized it: “First, do no harm.”<sup>68</sup> While he advocates a narrow legislative response, Cate himself draws a similar conclusion:

Individual responsibility, not regulation, is the principal and most effective form of privacy protection in most settings. The law should serve as a gap-filler, facilitating individual action in those situations in which the lack of competition has interfered with private privacy protection. In those situations, the law should only provide limited, basic privacy rights . . . . The purpose of these rights is to facilitate— not interfere with—the development of private mechanisms and individual choice as a means of valuing and protecting privacy.”<sup>69</sup>

¶187 In this Part, I address some overarching concerns of substituting regulation for market mechanisms before turning in the final Part to some of the specific issues raised by the “Safe Harbor Privacy Principles” agreement between the United States and the European Union and recent legislative proposals by the U.S. Federal Trade Commission.

#### A. *Trade-Offs and Inextricable Intertwinement*

¶188 The first issue to confront is the loss or dilution of many of the benefits described above. Simson Garfinkel has argued that privacy is compatible with information exchange, just as environmental protection has proved compatible with (and arguably necessary to) economic development, despite the contrary

<sup>65</sup> U.S. FED. TRADE COMM’N, *PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE— STATEMENT OF COMMISSIONER THOMAS B. LEARY CONCURRING IN PART AND DISSENTING IN PART*, at 4 (May, 2000), available at <http://www.ftc.gov/os/2000/05/privacyleary.htm> [hereinafter *PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT*].

<sup>66</sup> U.S. FED. TRADE COMM’N, *PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE*, at 38 (May, 2000), available at <http://www.ftc.gov/os/2000/05/testimonyprivacy.htm> emphasis added [hereinafter *PRIVACY ONLINE REPORT*].

<sup>67</sup> Esther Dyson, *Foreword to JENNINGS & FENA*, *supra* note 2, at xi.

<sup>68</sup> CATE, *supra* note 8, at 204.

<sup>69</sup> *Id.* at 131.

protestations of businesses in the 1960s.<sup>70</sup> This may be true, but it is likely so only up to a point. While the benefits of regulations often outweigh their costs, there's rarely a free lunch.

¶89 Certain regulatory approaches may promote consumer confidence and provide a reliable basis for information exchange at a relatively low cost. Others may exact costs that undermine information exchange entirely. For example, the Children's Online Privacy Protection Act (COPPA), a motherhood-and-apple-pie effort to protect children from online marketing without their parents' consent which passed Congress by sweeping margins, has forced many websites to simply eliminate children's programming.<sup>71</sup> While businesses often predict that regulation will cause problems, this example shows that the risk of overbroad regulation is real. The loss to society is the elimination of non-controversial opportunities for kids to design their own home pages, maintain e-mail accounts, and the like, opportunities that the burdensome provisions of COPPA (and subsequent implementing regulations adopted by the FTC) have made too expensive and difficult to provide.

¶90 The proscriptions of some privacy advocates often reflect an unrealistic sense of what is possible, or discount the interest of many people in benefits other than privacy. As an example, one author recommends reducing the incidence of identity theft by requiring you to show up to have your photo taken and put on the back of a credit card.<sup>72</sup> Citibank has tried it, without much commercial success or consumer interest. Its failure is not attributable to one writer's suggestion that "it would effectively end the industry's marketing strategy of sending credit cards to new customers through the mail,"<sup>73</sup> but rather because going down to your local bank to get a credit card is a pain in the neck, and consumers don't appear to be overly concerned with the risk of misuse (since credit card companies typically cover any exposure over \$50).

¶91 Similarly, contrary to the widespread suggestion that merchants and financial institutions demand social security numbers and other identifying information on a whim, such practices are typically done to provide some form of authentication, thereby reducing the risk of fraud and unauthorized access to accounts and saving money for legitimate consumers. It may not be the best way, but it's better and more convenient for all concerned than most current alternatives. Privacy advocates harshly criticize many of the alternatives, such as biometric identification, leaving a real question as to what sort of authentication could pass muster.

¶92 Before rushing to the absolutist position that individuals should always control "their" information, both regulators and individuals need to consider the trade-offs and nuances. Entering into the world, or into any version of the social compact, means that others will see your face and speak your name. Someone in the Montana outback knew Theodore Kaczynski's face and what groceries he liked to buy. You don't get to control those things. Surely you can minimize what others

<sup>70</sup> GARFINKEL, *supra* note 3, at 12.

<sup>71</sup> PRIVACY ONLINE REPORT—SWINDLE DISSENT, *supra* note 17, at 3; Lynn Burke, *An Ordeal: Copin' With COPPA*, WIRED NEWS, Sept. 20, 2000, at <http://www.wired.com/news/business/0,1367,38832,00.html> (noting the difficulties of using credit card verification for children); Lynn Burke, *Kids' Sites Cite COPPA Woes*, WIRED NEWS, Sept. 14, 2000, at <http://www.wired.com/news/print/0,1294,38666,00.html> (stating that some big sites "simply got rid of the parts of their sites" that would have required COPPA compliance, while small sites that couldn't afford the \$200,000 a year in infrastructure and overhead that COPPA compliance would have cost say: "We are turning off the very interactive features that kids are mad to get on.")

<sup>72</sup> GARFINKEL, *supra* note 3, at 32.

<sup>73</sup> *Id.*

know about you, but typically only at the cost of foregoing the associated benefits. And the decision to accept those tradeoffs is usually not a grudging bargain or a necessity of life, but rather a positive part of what we want society to be.

¶93 Legislators should consider the reality of regulatory costs and the resulting contraction of services and opportunities before, not after, they act. As shown by the FTC’s Advisory Committee on Access and Security, the issues created by even seemingly simple rules quickly grow complicated when set against the extraordinarily wide variety of information exchange practices that run throughout modern society.<sup>74</sup>

#### B. *Inequities*

¶94 A related area of inquiry is whether it makes sense to legislate requirements that will apply to all information exchange in furtherance of benefits valued only by some people. While the FTC has pointed to public opinion surveys to justify its concern with online privacy,<sup>75</sup> Commissioner Swindle has criticized this approach as both relying on slanted questions and running contrary to observed consumer behavior.<sup>76</sup> Such polls typically ask about whether people “are concerned” about privacy or whether privacy is “not important, somewhat important, or very important”— without asking whether they’d be willing to pay the costs of restricting information exchange.

¶95 Even correcting for these problems, there has doubtless been a recent spike in consumer concern. But this reflects a whirl of alarmist media accounts that do not necessarily provide a full appreciation of the trade-offs and costs involved. Certainly, privacy advocates would argue that the increase in concern reflects increasing consumer understanding of the potential risks in the use of personal data, although such data have been widely used for marketing purposes (e.g. mass mail) for a generation. As noted above, many people unfamiliar with the issues confuse protection of “privacy” with “security.” As noted above, privacy and security (which depends upon authentication and access to confirmatory information) are often at odds. Many might thus favor enhanced biometric access controls, which promise more robust security, even over the objections of privacy advocates. Yet binary surveys of whether people favor more “privacy” fail to reflect these more complex preferences.

¶96 Perhaps a more fundamental problem— related to Commissioner Swindle’s concern with poll results contrary to real-world behavior— is that such assumptions of universal interest in privacy suggests a universal willingness to sacrifice benefits of information exchange for the benefits of greater privacy. But Alan Westin’s surveys suggest that this generally isn’t true. Only one-quarter of the American public are “privacy absolutist”; the other three-quarters are willing to exchange personal information for other benefits.<sup>77</sup>

<sup>74</sup> FED. TRADE COMM’N, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY, available at <http://www.ftc.gov/acoas/papers/finalreport.htm> [hereinafter ADVISORY COMMITTEE REPORT].

<sup>75</sup> U.S. FED. TRADE COMM’N, SELF-REGULATION AND PRIVACY ONLINE, at 3 (July, 1999) available at <http://www.ftc.gov/os/1999/9907/privacyonlinetestimony.pdf> [hereinafter SELF-REGULATION]; PRIVACY ONLINE REPORT, *supra* note 66, at 2.

<sup>76</sup> PRIVACY ONLINE REPORT— SWINDLE DISSENT, *supra* note 17, at 10-12.

<sup>77</sup> See *supra* note 15.

¶97 Where the justification is solid, the degree of intrusion and potential harm to privacy interests low, and the procedural safeguards sufficient, many people have little objection to the gathering of personally identifiable information. In other words, “[w]hen consumers see a big payoff . . . some of them are more than willing to trade their personal information. ‘As long as you give people something in return, they’re thrilled,’ says Bill Gross, the Pasadena (Calif.) entrepreneur who founded idealab!, an incubator for Internet startups.”<sup>78</sup> A recent survey of the field noted:

One reason simple protective measures fail is that consumers aren’t sure they want them. Although they are worried that their privacy may be violated, they realize that personalized service on the Web can be very attractive. A Web site that recalls your tastes and buying habits can save you time and find bargains that suit you. What you see may depend on where you live, where you browse, what images tend to hold your eyeballs, and whether you have the loot to do more than look.<sup>79</sup>

After great *sturm und drang* over the government’s proposals regarding encryption, perhaps the most basic form of privacy protection available for anyone using e-mail or surfing the web, consumers have virtually ignored even the most user-friendly encryption options.

¶98 Americans may not be ready for the kind of downtown surveillance cameras designed to deter street crime that are increasingly common in the United Kingdom. But San Francisco, one of the country’s most liberal cities, last year installed “red-light runner” cameras, triggered by the movement of a car through an intersection after a red light. Put up in response to several well-publicized incidents involving red-light runners who killed pedestrians, the cameras have been very popular. Initial concerns were raised when the police sent the photos to violators’ homes. In a few instances, the photos showed passengers that raised some questions with the violator’s spouse—a problem solved when police shifted to providing the photos only on an as-requested basis. The example demonstrates Westin’s point: most Americans are privacy pragmatists, willing to have information gathered where they see a real benefit and appropriate safeguards in place.

¶99 A *New York Times* article on the topic concluded that “there probably are real differences among people in the extent to which they are willing to entrust private information to others.” It cited Anthony G. Greenwald, a social psychology professor at the University of Washington, who has used the Web to conduct experiments among volunteers.

Because some are more trusting than others, there should be a segmentable market for things that will attract the more trusting (online shopping, music via Napster, opening messages that may contain viruses). And there is also a market for things that appeal to the less trusting (alarm systems, unlisted phone numbers, etc.).<sup>80</sup>

¶100 If many Americans are willing to freely exchange their personal information, or do not feel the need to opt-out or regularly check to see what information others have about them, they will bear the costs of measures that they don’t perceive as beneficial. There are certainly some efficiency and consistency advantages from

<sup>78</sup> Edward C. Baig et al., *supra* note 16, at 87-88.

<sup>79</sup> *Id.* at 86.

<sup>80</sup> Tim Race, *New Economy*, N.Y. TIMES, July 24, 2000, at C4.

requiring universal standards to be built into our systems for handling information. But if those standards come from government rather than the market, there will almost certainly be efficiency losses as well. We should ask whether it makes sense for government agencies to substitute their judgment for the pragmatic and ad-hoc decisions of individuals as to whether any given trade-off is worthwhile, given the benefits they stand to receive. Of course, this suggests that regulations requiring notice, designed to make the terms of the trade-off clear to individuals, may be appropriate, as discussed below.

### C. *Traps for the Unwary*

¶101 The general costs and issues of regulations are compounded in the realm of information. The Information Revolution is more than a catchphrase— it describes the integral role of information throughout the economy. As noted, information is fast-moving, amorphous, and liquid. The hardest aspect of posting a “privacy policy” is tracking all the different uses to which information may be put and constantly confirming that those uses align with the policy. This is especially true in the era of the “borderless corporation,” in which third-party contractors, consultants, and outsourcers are essential to most major business operations. It’s much easier to collect and distribute personally identifiable information than to keep it contained.<sup>81</sup> This makes the job of ensuring compliance with any rule particularly difficult. Any given requirement immediately becomes a trap for the unwary, requiring significant resources to continually track internal information practices to assure compliance.

¶102 Most “privacy scandals” reflect the difficulty of knowing what’s going on in an increasingly complex system. Several recent privacy “scandals”— Real Networks receipt of music download information, Netscape’s receipt of file download information, the existence of a “web bug” in Microsoft’s Office suite, TrustE’s violation of its own policy, various sites’ use of Coremetrics to analyze web traffic— did not involve claims that anyone had actually misused data. Rather, they reflected incidental or unexpected receipt of certain types of information. This phenomenon demonstrates the difficulty of tracking all the information that is being transferred while ensuring constant alignment between stated privacy policies and constantly evolving practices. New software programs have lots of code, lots of features, and transfer lots of information. In practice that normally means lots of potential bugs (and thus lots of “potential” privacy violations). Many “online privacy incidents” are in fact software bugs or security “exploits” posted by hackers looking for problems with software.<sup>82</sup> It would serve no purpose— and impose prohibitive costs— to turn every potential privacy problem into a violation of federal law, regardless of the intent of the “violateur.”

¶103 Other privacy controversies reflect decentralization, outsourcing, a lack of extensive infrastructure regarding privacy policies, or difficulties in communicating a consistent approach with third parties.<sup>83</sup> Note that most of these reflect accident, the needs of fast growing businesses, or new business realities, and may not be amenable to correction in response to regulation. Regulation in this context just sets the stage for lawsuits and significant costs. In *The Hundredth Window*, Charles

<sup>81</sup> JENNINGS & FENA, *supra* note 2, at 186.

<sup>82</sup> *Id.* at 231.

<sup>83</sup> *Id.* at 26, 155-156.

Jennings and Lori Fena suggest that such costs appropriately internalize privacy externalities. But as argued above, it's not at all clear whether everyone sees these costs as externalities, especially in the absence of actual injury.

¶104 The 2000 online survey conducted by the FTC may give a hint as to how those problems would be compounded by a regulatory regime. The FTC Survey, which took pains to repeatedly claim that it was bending over backwards to give website operators the benefit of the doubt, contained many detailed requirements that were not met by major companies that thought they had posted perfectly adequate privacy disclosures. For example, the Survey required websites to not just describe uses of information within the intended scope of a transaction, but to detail disclosures to third parties. This provision (taken literally) is virtually meaningless and unworkable in modern society. If a company employee reveals a customer's name to a contractor, has a third-party disclosure occurred? The "choice" provisions of the Survey similarly required separate opt-in/opt-out provisions for marketing purposes and third-party purposes.<sup>84</sup> The Survey's "access" section focused not on the actual availability of access, but on notice about that access.<sup>85</sup> And while the FTC conceded that the existence of security provisions was significantly more important than security notice— and acknowledged the warning of its own Advisory Committee that detailed disclosures of security can invite security breaches— it still graded sites on whether they provided notices about security, not on security itself.<sup>86</sup>

¶105 Regulating the flow and exchange of information in the world is an exceptionally challenging task. It's very difficult to frame principles of universal application. While the framework described above represents one attempt, those with other social agendas will have very different hierarchies of values. Even where there is agreement on a single approach, many factors can influence the implementation: the vagaries of the precise nature of the information, the precise nature of the notice provided and the consent obtained, the exact scope of the purpose for which the information was gathered, the degree to which the information was individualized or aggregated, the perceived legitimacy of the individual's desire to withhold the information, and many other criteria. It is a challenging task to steer between the Scylla of one-size-fits-all regulation and the Charybdis of detailed industry-by-industry proscription.

#### D. *Overbreadth*

¶106 For understandable rhetorical reasons, privacy advocates often dwell on the catastrophic nightmare scenarios facilitated by unlimited exchange of personal information, from Hitler's misuse of the European Census to Sherman's use of census data to facilitate his March through Georgia.<sup>87</sup> After all, saying that information was gathered ". . . and nothing bad happened" is terribly anticlimactic. Such rhetoric, however, does not provide a sound ground for public policy. Such alarms are reminiscent of the NRA's opposition to gun control on the basis that widespread gun ownership might help repel a foreign invasion or defeat domestic tyranny. Well, it might. But the prospects are so remote, and the short-term

<sup>84</sup> PRIVACY ONLINE REPORT, *supra* note 66, at 15-16.

<sup>85</sup> *Id.* at 16-18.

<sup>86</sup> *Id.* at 17-19.

<sup>87</sup> JERRY M. ROSENBERG, THE DEATH OF PRIVACY 1 (1969); SMITH, *supra* note 21, at 61.

benefits to society from the alternative so significant, that the worst-case scenario shouldn't dictate planning.

¶107 Certainly the remote potential of catastrophic misuse is a factor to consider, but one that must be deeply discounted given its remoteness. It is better, perhaps, to focus on prohibiting misuse and misrepresentation (since disclosure, and the subsequent public backlash, is in many cases the most effective deterrent) and imposing appropriate sanctions when they occur. Just as we don't prohibit libraries because of the possibility of copyright infringement, we should not build the system based on the exception.

¶108 It does not seem sensible to avoid initiatives with clear social benefits because of the distant chance for misuse. For example, regarding the proliferation of uses of the Social Security Number for identification and authentication purposes, the noted communitarian scholar Amitai Etzioni writes:

[National identification cards are] quite common in European democracies and have been in place for quite some time without undermining these democracies. [They] do not transform democratic societies into totalitarian ones . . . . Totalitarian governments do not creep up on the tails of measures such as ID cards, they arise in response to breakdowns in the social order, when basic human needs, such as public safety and work opportunities, are grossly neglected. When a society does not take steps to prevent major social ills and strengthen social order, an increasing number of citizens demand strong-armed authorities to restore law and order. By helping to sustain law and order, universal identifiers may thus play a role in curbing the type of breakdown in social order than can lead to totalitarianism.<sup>88</sup>

But to privacy advocates, the collection of even the most innocent information contains the potential for abuse:

Companies aren't really sure what to do with all this information. Plans that they've articulated are incredibly bland— along the lines of sending Pepsi coupons to Coke customers. . . . But in fact, there is a gold mine of information buried in this transaction data, . . . [making for] a multivariable science experiment, with the store's customers doubling as laboratory rats.<sup>89</sup>

¶109 Given the costs identified above, it seems more sensible to act to solve specific problems— where there is broad agreement that the problem exists and that the remedy is not worse than the disease. Recent examples of more focused measures include federal and state legislation limiting spam, laws establishing remedies for economic harm resulting from identity theft or other misuse of personal information, and the creation of ombudspersons and clearinghouses to resolve problems resulting from the misuse of information.

¶110 Broader regulation carries a palpable danger of overbreadth, especially given how hard it is to assess recent, let alone future, business models. This overbreadth can be in language (do we really want to prohibit a local baker from remembering that Mrs. Murphy likes angel food cake?) or in effect (e.g., COPPA's shutting down of unobjectionable websites because of the costs entailed by compliance). In many cases, the harm to be avoided is unclear, but the burdens of trying to do so are real. The difficulty in controlling information (the kernel of truth behind the old

<sup>88</sup> ETZIONI, *supra* note 14, at 127.

<sup>89</sup> GARFINKEL, *supra* note 3, at 158.

chestnut that “information wants to be free”) means that creating new “controls” interferes with core functions of the new economy— interactivity, personalization, customization, neural networks, collaborative filtering, and the availability and exchange of medical and financial information needed for new services. It limits marketing, leading to higher costs and fewer offers. Everyone in the bazaar has to whisper, and can do so only between 12:00 and 2:00 in the afternoon— like old New England blue laws (still in effect in much of Europe) that forced all stores to close at 6:00 and on Sunday.

#### E. *Ineffectiveness*

¶111 People are inventive at finding ways around laws that block popularly desired benefits, and regulations may have a hard time cabining information. Since 1974, Congress has passed a series of privacy initiatives covering access to student data, notice of investigation of bank records, cable television records notice and access, a ban on polygraphs for hiring, a ban on disclosure of video rental records, limits on the use of automated calls in phone sales, and requirements that state DMVs let drivers opt-out of rental names/addresses. According to noted privacy expert Robert Ellis Smith, of all of these laws, “only the anti-polygraph law and the telemarketing law have really worked as intended.”<sup>90</sup> (Neither law dealt with information privacy). While Smith attributes these failures to what in hindsight appear to be “loopholes,” it’s at least as plausible that such initiatives are of limited utility because the regulatory compliance costs outweigh the limited privacy benefits.

¶112 The likelihood of some level of noncompliance and circumvention is particularly noteworthy, given the FTC’s determination that 90% compliance with online profiling regulations is insufficient and warrants legislative action.

[B]ackstop legislation addressing online profiling is still required to fully ensure that consumers’ privacy is protected online. For while NAI’s [Network Advertising Initiative] current membership constitutes over 90% of the network advertising industry in terms of revenues and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles.<sup>91</sup>

Such a conclusion makes sense only if you assign little or no cost to legislative solutions, and it threatens to make a sham of deference to market operation. After all, “when has self-regulation ever ensured that every member of an industry will adopt industry standards?”<sup>92</sup>

#### F. *Online/Offline Imbalance*

¶113 While the EU rules and US-EU Safe Harbor Principles apply online and offline, the FTC has focused on regulation of privacy on the internet rather than offline privacy considerations. Some of this focus doubtless reflects the sexiness of electronic commerce and the understandable desire to be involved in an expanding industry. But other than the issue of online profiling (whereby clickstream data is received by websites and which the FTC has separately addressed in a different set

<sup>90</sup> SMITH, *supra* note 21, at 332.

<sup>91</sup> ONLINE PROFILING REPORT, *supra* note 18, at 10; *see also* PRIVACY ONLINE REPORT, *supra* note 66, at 34-36.

<sup>92</sup> PRIVACY ONLINE REPORT— SWINDLE DISSENT, *supra* note 17, at 2.

of reports), the FTC has never articulated a basis for treating offline privacy differently from online privacy. Yet traditional commerce raises all of the same issues, and the online community has actually done a far better job of communicating privacy notices and other elements of privacy policies to users than the local department store or gas station. After all, when was the last time that either told you what it does with your credit card information?

¶114 The FTC's online-centric approach risks heightening unjustified public concerns, many rooted in widespread technophobia. We casually give our credit cards to waiters who disappear for 15 minutes and return with a bill. Of course, we have no assurances that the waiter hasn't surreptitiously copied down the number or made an extra imprint of the card. But familiarity, the feeling that the waiter risks something by doing this, and laws against credit card fraud combine to give us a sense of security sufficient to let the transaction proceed. Similarly, we entrust our most precious documents—our bank statements, our mortgage records, our love letters—to the security of paper and spit, leaving them to the care of a dozen underpaid strangers to carry across the country. It shouldn't work— but it usually does. And, more importantly, we trust it to. We talk on the phone, oblivious to the ability of an administrator in a central office to eavesdrop. And we wander through stores, unconcerned that a nefarious stranger could be following us around, noting our purchases and planning to use that information to blackmail us. Yet in the world of technology, we worry a great deal about these same transactions.

¶115 Treating “technology” differently not only risks setting different and more demanding rules for the New Economy (which arguably needs them less), but could lead to the adoption of rules that we would never accept in the offline world because we would better understand their implications in daily life. As P. Bernt Hugenholtz of the University of Amsterdam has said in the context of regulation of technologies like Napster that affect existing intellectual property arrangements:

People are always scoffing that the technology moves so much faster than the law, but that's ridiculous. In fact the law is moving faster than the technology, which is both ironic and a very bad sign . . . . All academics I've ever met— no matter what their political stance— agree on one thing: all this Internet-related legislation is very, very premature. You'd think they'd at least see what the car looked like before trying to drive it.<sup>93</sup>

¶116 The legislative and regulatory difficulties are thus compounded when legislators seek to pass preventative legislation in the technology environment. Such legislation can result in the wrong bill at the wrong time in the wrong forum, with local legislators responding to media discussion of ill-defined “privacy” concerns before specific problems have emerged. Given the international reach of the Internet, a mishmash of inconsistently detailed local, state, national, and international regulations can kill or cripple what would have otherwise been beneficial new initiatives.

¶117 On several occasions, FTC Commissioner Leary has written persuasively on the perils of differential regulation of online activity:

If the Internet is subjected to requirements that do not apply pro tanto to offline commerce, the regulatory imbalance could itself inhibit the growth of the Internet and undercut our common objective [of promoting the growth of Internet usage] . . . . Of course, some privacy issues are particular to the Internet. . . . Any legislative or regulatory scheme can and

<sup>93</sup> CATE, *supra* note 8, at 131.

should ensure that consumers are adequately informed about these Internet capabilities. . . . [But more generally, the] distinction between online and offline privacy is illogical, impractical and potentially harmful . . . . The Report's recommendation would require Amazon.com to comply with the fair information practice principles but not the local bookstore which can compile and disseminate the same information about the reading habits of its customers. . . . Enforcement actions would depend on the source of and method used to collect a particular piece of consumer data rather than on whether there was a clear-cut violation of a company's announced privacy policy or mandated standards.<sup>94</sup>

After warning that such regulation would put internet companies at a competitive disadvantage, Leary also tellingly traced the political history of the FTC's interest in the in-the-news topic of online commerce:

The Report's recommendation limits itself to online privacy for reasons that seem primarily historical. The Commission first looked at the online world at a public workshop in 1995, followed by subsequent workshops in 1996 and 1997. Then, starting in 1998, Commission staff conducted annual surveys of Internet sites and their privacy policies to measure in a rough way the state of industry self-regulation. Each survey has been reported to Congress. The Report's legislative recommendation flows from that series of surveys. The surveys have provided a lot of useful information, and undoubtedly spurred industry attention to online privacy issues, but the scope of these particularly surveys should not dictate the parameters of a legislative proposal.<sup>95</sup>

#### G. *Value of Existing Approaches*

¶118 Current U.S. privacy laws and regulations are hardly an academician's dream. They're beset by differing industry-by-industry regulation, overlapping and contradictory federal and state approaches, arcane distinctions, and historical accidents. But the easy-to-ridicule inconsistencies of current U.S. privacy protections actually embody a more consistent philosophy than generally supposed— one relatively in line with an approach to privacy that sets great store in protecting a person's inner thoughts and expression. We therefore provide the highest degree of protection for communications via ECPA's wiretap restrictions and criminal prohibitions on private eavesdropping. We provide intermediate protection for records with the greatest risk of abuse (financial and medical records) and those dealing with the expression of ideas (videotapes, albeit not books or magazines), and generally little protection for commercial dealings. In contrast to sweeping European-style statements of principles to which society must adhere, the American sectoral approach has thus traditionally concentrated on specific remedies to specific problems. We do, however, broadly prohibit abuse of personal information to perpetrate injuries, whether in traditional crimes such as fraud, embezzlement, or trespass, or, increasingly, in contemporary crimes such as identity theft and misrepresentations regarding the use of information that result in harm to consumers.

<sup>94</sup> PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 65, at 1, 8, 9, and 9-10 (citations omitted).

<sup>95</sup> *Id.* at 10-11.

¶119 As for the criminal law, the “objectively reasonable expectation of privacy” approach set forth in *Katz v. United States*, 389 U.S. 347 (1967), is a notoriously bootstrapping test.<sup>96</sup> As Jeffrey Rosen argues:

[A] vision of privacy that took seriously the text of the Fourth Amendment might emphasize that there is an irreducible core of constitutional protection against unreasonable searches and seizures of persons, houses, electronic papers, and effects that is necessary for freedom, regardless of how much or how little privacy people subjectively expect in these areas in the light of changing technologies of surveillance.<sup>97</sup>

But, understandably, he doesn’t say what that judge-made rule would be, or how it should arbitrate contending claims over what limits to privacy were appropriate. For all the criticism it has endured, *Katz* has served fairly well in basing judicial understandings of privacy on the rules accepted by the broader society and its gradual assimilation of new social arrangements accompanying new technologies. The civil analog of *Katz*, the traditional torts based on negligence or misconduct that deviates from accepted professional practices and results in harm, offer a reasonably satisfactory means of redressing most real privacy-oriented grievances.

#### H. *Bureaucratic Expansion*

¶120 Any legislation, particularly legislation on such a controversial and politically sexy topic, carries the significant risk that any bill will become a legislative Christmas tree hung with special provisions. “Privacy” in its many forms could well become the government’s regulatory wedge into the New Economy. Compounding this likelihood is the problem of regulatory self-selection (as people focusing on privacy issues tend to be proponents of greater controls on the exchange of personal information) as well as the inevitable empire-building endemic to any human enterprise. There is, unfortunately, no agency in charge of making life simple.

¶121 In the current environment where privacy constitutes an emotional and ideological issue, there’s a significant likelihood that the in-the-trenches creation of regulations and the implementation and enforcement of those regulations would be done by people self-selected for their advocacy of privacy interests. After all, there are plenty of full-time privacy advocates, but few people with the job of making the world a convenient place. The regulatory arena is even less subject to public scrutiny than the lawmaking process. And once enacted, regulations exact a creeping cost that is difficult for consumers (or politicians) to see, let alone roll back.

¶122 In what was doubtless a politically astute move, the FTC’s recommendation avoided setting forth any specifics that could be used to demonstrate the concrete costs of information controls. After acknowledging the complexity and difficulty of framing regulations, the “Commission recommend[ed] that any legislation be phrased in general terms. . . . [T]he definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency [presumably a coy reference to the FTC itself] in promulgating its rules or regulations.”<sup>98</sup>

<sup>96</sup> See Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 411 (1974).

<sup>97</sup> ROSEN, *supra* note 4, at 64.

<sup>98</sup> PRIVACY ONLINE REPORT, *supra* note 66, at 37.

¶123 Such statements evoked appropriate outrage from the dissenters: Commissioner Leary noted that “[i]t is not appropriate to defer all the tough issues for future rule-making.”<sup>99</sup> Commissioner Swindle criticized the majority’s “conclusory— yet sweeping— legislative recommendation.” “The Commission owes it to Congress— and the public— to comment more specifically on what it has in mind before it recommends legislation that requires all consumer-oriented commercial Web sites to comply with breathtakingly broad laws whose details will be filled in later during the rulemaking process.”<sup>100</sup> In response to the Online Profiling Report, he noted “[a]gain, the devil is in the details” left open.<sup>101</sup>

¶124 In reviewing the need for new legislation and new regulation, Congress will need to wrestle with the daunting implications of creating a new regulatory enforcement bureaucracy. After all, policing privacy comes down to setting forth rules to control the flow of information, the lifeblood of the Information Revolution and the New Economy that it has created, as well as the daily exchanges of society. The implications of throwing grit in the gears of that economy must be soberly considered.

¶125 The point is not that regulation is wrong or counterproductive. In some circumstances, consistent and reliable regulatory regimes can benefit the development of commerce (and thus consumers) by fixing expectations, allowing meaningful future planning, and reducing risks. Building privacy considerations into the design of a system can be cheaper than trying to retrofit after the fact. But the complexity of the topics, the difficulty of harmonizing disparate interests and perspectives, and, perhaps most importantly, the fine-grained nature of the trade-offs in each situation counsels in favor of careful study and against broad-brush regulation. The overbreadth of such regulation risks chilling not only innovative and quickly evolving business models, but the free exchange of information necessary to promote individual, community, and social goals. If it’s too hard, businesses and people just won’t do it.

#### IV. A CRITIQUE OF CONTEMPORARY INFORMATION REGULATION PROPOSALS

##### A. *The Evolution of Information Regulation*

¶126 Over the past thirty years, a number of European, Canadian, and U.S. governmental agencies have suggested varying formulations of “privacy rules,” normally expressed through the rhetoric of “Fair Information Practice Principles” (presumably consigning those rash enough to prefer other approaches to advocacy of “Unfair Information Practices”).

¶127 In 1973 a Commission convened by what was then the Department of Health, Education, and Welfare issued a report on “Records Computers and the Rights of Citizens,” including a “Code of Fair Information Practice.” Those principles include avoiding secret systems, providing access to data, preventing different uses,

<sup>99</sup> U.S. FED. TRADE COMM’N, ONLINE PROFILING: STATEMENT OF COMMISSIONER THOMAS B. LEARY CONCURRING IN PART AND DISSENTING IN PART, at 2 (July, 2000), available at <http://www.ftc.gov/os/2000/07/onlineprofiling.htm#LEARY> [hereinafter ONLINE PROFILING REPORT—LEARY CONCURRENCE AND DISSENT].

<sup>100</sup> PRIVACY ONLINE REPORT— SWINDLE DISSENT, *supra* note 17, at 1.

<sup>101</sup> ONLINE PROFILING REPORT— SWINDLE DISSENT, *supra* note 63, at 2.

permitting correction, ensuring data reliability, and implementing precautions against misuse.<sup>102</sup>

¶128 In 1980, the Organization for Economic Cooperation and Development set forth its Fair Information Practices: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.<sup>103</sup>

¶129 In 1995, the Privacy Working Group of the National Information Infrastructure Task Force issued its *Principles for Providing and Using Personal Information*,<sup>104</sup> directly addressing information privacy and setting out a large number of principles. These included Information Privacy (noting the need to respect individual privacy in the handling of information), Integrity, Quality, Acquisition (only for specific purposes), Notice, Protection, Fairness, Education, Awareness, and Empowerment.

¶130 Also in 1995, following four years of internal debate, the European Union set forth its Privacy Directive,<sup>105</sup> the product of the European central government's trust of government over business. The Directive sets forth a painfully abstruse and detailed collection of principles, exceptions, and exclusions.<sup>106</sup> While the Directive took effect in 1998, a number of European states have not enacted implementing legislation. However, because of the economic importance of Europe and the negotiations between the United States and Europe over a safe harbor for compliance with these principles, the Directive's provisions emerged as a focus of negotiation that ultimately produced the July 2000 agreement on a Safe Harbor for U.S. companies doing business in Europe. This spring, the Canadian Parliament passed the *Personal Information Protection and Electronic Documents Act*, including a voluntary Model Code of recommendations with eleven different factors.<sup>107</sup>

¶131 Many of these varying governmental principles were either contradictory or included a number of elements subsequently deemed relatively less important.<sup>108</sup> As FTC Commissioner Leary has cautioned, contemporary U.S. regulators must be careful to conduct their own independent analysis of the potential benefits of new regulations rather than merely relying on prior reports, many generated at times or

<sup>102</sup> GARFINKEL, *supra* note 3, at 7; SMITH, *supra* note 21, at 329.

<sup>103</sup> See Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, at <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (last modified Jan. 5, 1999).

<sup>104</sup> PRIVACY WORKING GROUP, PRESIDENT'S INFORMATION INFRASTRUCTURE TASK FORCE, *PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION* (1995).

<sup>105</sup> Council Directive 95/46, 1995 O.J. (L 281) 31, available at [http://www.privacy.org/pi/intl\\_orgs/ec/final\\_EU\\_Data\\_Protection.html](http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html).

<sup>106</sup> *Id.*

<sup>107</sup> *Canadian Parliament Enacts Privacy Legislation*, CYBERSPACE LAW, Apr. 2000, at 9.

<sup>108</sup> SELF-REGULATION, *supra* note 75, at 3 & n.17 (citing various governmental reports). As an example of such overbreadth, a British Columbia privacy commission called for government enforcement of the following principles: Publicity and transparency for personal info systems; Necessity and relevance; Reducing collection, storage and use of Personally Identifiable Information to the extent possible; Finality as to purpose and use; Responsible keepers; Control over linkages, transfers, and interconnections; Informed consent; Accuracy and completeness; Data trespass and remedies for violations; Special rules for sensitive personal information; Right of access to and correction of personal information; Right to be forgotten, including the ultimate anonymization or destruction of almost all personal information. DAVID H. FLAHERTY, *PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES* (1989) (emphasis omitted).

in countries distrustful of market mechanisms and advocating a greater role for government regulators.<sup>109</sup>

The fact that the fair information practices have been favorably regarded in the regulatory community for almost thirty years (Report at 8-9), does not justify mandatory legislation. A provenance from the 1970s is scant cause for comfort, because government regulators, here and throughout the world, had much less faith in free market institutions then than they have today.<sup>110</sup>

¶132 It is worth noting that the sclerosis that grips European labor, capital and product markets— leading to unemployment rates twice that in the United States and a one-third lower per capita domestic product— results in large measure from the aggregate effects of exactly such well-intentioned regulations.<sup>111</sup> Moreover, many national notions of privacy are culturally dependent or result from historical accidents. When a German citizen moves, he or she has to check in at a police station in his or her new town. French phone bills show only the last four digits of numbers called (a legacy of the Vichy investigation of the Resistance).

¶133 The proliferation of these various guidelines, with their significant differences in scope and approach, reflects the lack of a consensus even between U.S. and European policymakers, let alone policymakers elsewhere. Moreover, the interpretation of these guidelines is very unclear, and their implementation in the United States and interaction with existing and future federal and state privacy regulations remain equally murky.

#### B. Critiques of Proposed FTC and Safe Harbor Regulations

¶134 The FTC has proposed regulation concerning five principles: Notice, Consent, Access, Security, and Enforcement. The Safe Harbor Principles, following the EU Privacy Directive, add two more: Onward Transfer and Data Integrity. I review each in turn.

##### 1. Notice

¶135 Both the FTC recommendation and the Safe Harbor principles call for notice to consumers regarding the use of their information. According to the FTC:

Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.<sup>112</sup>

According to the Safe Harbor notice principle:

An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization

<sup>109</sup> PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 65, at 5.

<sup>110</sup> *Id.*

<sup>111</sup> *Old World, New Economy*, ECONOMIST, Sept. 2, 2000, at 20 (discussing the need for European structural reform to improve its labor, product and capital markets).

<sup>112</sup> PRIVACY ONLINE REPORT, *supra* note 66, at iii.

with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party . . . [FN: It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.]<sup>113</sup>

¶136 All participants in the debate over privacy believe that notice is important. Some believe this because notice is a prerequisite for other Fair Information Practices; others because full information is a necessary precondition for markets to operate efficiently.

¶137 Despite the agreement, notice is hard to accomplish. Notices can be divided into three types: those that tell people what they already know, those that tell people what they don't know but don't care about (and thus don't change behavior), and those that tell people what they don't know and do care about. Because different people know different things, there's necessarily some overkill, but only notices that fall into the third category are typically worth the effort.

¶138 The most likely scenario is the first one— that in our zeal to address all the potential uses and potential risks of information flows, we'll insist on overbroad disclosures. Regulators and risk-averse businesspeople and lawyers are notorious for adding warning upon warning to the point that most contemporary contracts are masses of unintelligible small print that no one bothers to read. There's a risk that "everything is more important than everything else." All too often, various regulators with different interests at different times deem various things (disclaimers, limitations of liability, privacy, etc.) of great importance and require that each one be especially "clear and conspicuous." This generally translates into writing in bold capital letters, resulting in a document with either a profusion of emphasis that effectively emphasizes nothing, or a profusion of separate forms (like the blizzard of paper you sign when you get a mortgage) that are unreadable due to their volume. Who's to say that disclosure of privacy policies is more valuable to consumers than the disclosure of finance terms, limitations of liability, or the next flavor of the month?

¶139 An example of what can go wrong with overbroad notice is the Federal Aviation Administration rule that flight attendants review with passengers the operation of seat belts before every flight. When Pacific Southwest Airlines attendants started their seat-belt spiel: "For those of you who have not been in a passenger car since 1962 . . ." they were pointing out the absurdity of telling people what they already knew. They captured a dramatically increased share of passengers' attention for the part of the talk that gave out useful information (like where the exits were). But within a few weeks, they had incurred the wrath of the Federal Aviation Administration and had to stop. It's a sobering illustration of regulatory inflexibility that, forty years later, we're still giving notice of how a

<sup>113</sup> U.S. DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (July 21, 2000), at <http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm> [hereinafter SAFE HARBOR PRINCIPLES].

seatbelt operates. Applying that paradigm across a fast-developing information economy is daunting.

¶140 Litigation-averse business people may make this situation worse. Unfortunately, the likely corporate response to any notice requirement (and concomitant expansion of liability) will be to describe every possible problem that could arise as a result of information exchange. The result is likely to be about as readable (and about as helpful) as the typical corporate SEC filing— which is to say, not at all. Liability-driven notices are commonplace— they appear on the backs of baseball tickets and the pages of fine print included in the instructions of any consumer appliance. But warnings that you may get hit by a baseball at the ballpark, or that you should be careful with power tools, don't make the world a better or safer place. Nor do they change real world behavior. (Has anyone ever looked at the back of a baseball ticket and said "No, you're right. I might get hit by a ball and not be able to sue the baseball team, and so I'm not going to the game today?" It never happens.) Worse, by making the boilerplate so expansive, we make it much less likely that most people will read the material to learn about unexpected risks.

¶141 Regulatory burdens typically take the form of the Death of a Thousand Cuts. In this context, unfortunately, more is worse. The proliferation of notices and warnings numb us to the truly important warnings of serious and unexpected risks. But legislators, regulators, and advocates too often declare victory and go home, understandably failing to undertake the Sisyphean and unrewarding task of periodically reviewing regulations to ensure that they are still necessary and meaningful. (There's a reason that legal codes inevitably get longer year after year.) Regulators need to balance their interest in a particular topic in view of the overall consumer experience, and take a disciplined approach to determining which one or two items are really priorities for consumer consideration. Otherwise, privacy notices will become the digital mattress tags for the 21st century, unread and unloved.

¶142 A second concern is that educating people about a complicated topic that they don't want to know much about is like leading a horse to water. The "privacy policy" pages of most websites, along with their legal terms, are typically among the least trafficked. The statements distributed by merchants in monthly bills are widely disregarded by consumers as more junk mail. The Platform for Privacy Preferences ("P3P"), intended to give consumers a fine-grained way of expressing their detailed privacy preferences on the web, has largely died on the vine, a victim of an overwhelming lack of consumer interest.

¶143 Aware of this situation, both privacy advocates and those skeptical of privacy regulations have expressed frustration over the lack of clarity of many privacy policies.<sup>114</sup> It's hard to track all the information that we exchange, all the places it's stored, and all the ways it's used. The FTC has alluded to the difficulty:

[I]n light of the complexity of actual business practices and the myriad ways in which companies can handle personal information, it is difficult to categorize the many disparate information practices embodied in the privacy disclosures that were analyzed. Many Web sites have multiple information practices that differ according to the nature or source of the information at issue or the context in which it was collected.<sup>115</sup>

<sup>114</sup> PRIVACY ONLINE REPORT, *supra* note 66, at 24-28; PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 65, at 2-4.

<sup>115</sup> PRIVACY ONLINE REPORT, *supra* note 66, at 22.

For example, companies frequently have multiple policies that apply in different circumstances (perhaps one approach for a sweepstakes entry, another for making a purchase). Alternative technologies further compound the problem. What does it mean to have “reasonably prominent” notice of privacy policies in the context of the tiny screen of a cellular phone used to browse the Internet?

¶144 Like “plain-English” securities documents, “simplified” privacy policies are still likely to be heavy sledding. Before passing notice regulations, legislators should be required to attest that they have been able to read through the detailed disclosures regarding the storage and use of personal information mandated by Section 631 of the Cable Communications Policy Act of 1984. Even where written in a user-friendly fashion (crammed full of friendly pronouns, short sentences, and bold graphics), these disclosures include an irreducible minimum of complexity that few consumers will be interested in reading through.

¶145 This problem points up the tension between completeness and accuracy on the one hand, and brevity and readability on the other. The May 2000 FTC Report acknowledged: “As with many consumer disclosures, there is a tension between providing full and accurate information about a site’s information practices and providing short and easily understandable disclosures that consumers are likely to read and understand.”<sup>116</sup> In the online context, the information “transferred” and “collected” with virtually every visit to a site would include a user’s operating system and its version number, its IP address (requiring a discussion of the difference between static and dynamic IP addresses, and how they differ from e-mail addresses), browser type and version number, time-stamp information, prior web pages visited, information previously stored on the user’s last visit to a site, plus any information affirmatively provided by the user. Similarly, offline merchants may track purchasing patterns, buying codes, catalog versions and store locations, and the phone company or cable service may track (if only temporarily) significant amounts of technical information incident to your receipt of service. It may be a worthy effort, but no one should hold out too much hope for sterling results. Ultimately, regulators will need to do extensive line-drawing as to what information transfer must be disclosed.

¶146 Trying to cut this Gordian knot, Commissioner Leary has called for disclosures of “greater clarity and comparability.”<sup>117</sup> He notes that “[s]ome standardization of the disclosures would allow consumers to compare more easily the privacy practices of different vendors.”<sup>118</sup> This seems a reasonable approach, but it’s again easy to underestimate the difficulties entailed. The FTC analysis gives a laundry list of notice topics (what is collected, how it’s collected, how it’s used, what other entities do with it, etc.), and suggests a simple two-by-two matrix of uses, divided between “internal” and “external” uses and “primary” (for the intended transaction) and “secondary” (marketing) uses. But is a transfer to a third-party agent “internal” or “external”? Is a notice of a recall “primary” or “secondary”? What about notice of a software bug? A software upgrade (which may include a bug fix)? Does it depend on whether the company stands to profit from the notice?

¶147 Standardized boilerplate (some of which has already been generated by industry efforts) is relatively unhelpful given the variety of business practices and types of information involved. By comparison, the labeling of food products— in a setting

<sup>116</sup> *Id.* at 24.

<sup>117</sup> PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 65, at 2.

<sup>118</sup> *Id.* at 3.

where there was general consensus on the need and the value to consumers, generally high consumer interest, and a relatively manageable number of criteria to be displayed— took years of negotiation and debate.

¶148 Even a requirement as simple as “reasonably prominent notice of the types of information gathered and the uses to which it is put,” if taken literally, could result in pages of information about the detailed technical information incidental to online transactions, while the discussion of uses risks being either so high-level as to be meaningless or so specific as to be mind-numbing. What is “reasonable” in this context? What degree of detail does a consumer need to know about what’s happening? Without the sort of clear prioritization and line-drawing described above, years of rule-making and court decisions will be needed to sort this out. And even making the sweeping assumption that the rules are clear, the ever-changing nature of information exchange in response to new business models and new consumer demands will inevitably create new traps for the unwary and require a new corporate bureaucracy devoted to tracking information flows.

¶149 To minimize irrelevant legalese, and maximize the real-world effect of notices, any requirements should stress practices and risks that aren’t commonly appreciated. This is an admittedly floating benchmark that will shift over time as people learn more about new technologies and as technologies and business models continue to evolve. But common sense, the existing laws of negligence, and standard industry practice provide some guidance. Unfortunately, in the interest of avoiding a “privacy” problem, most current privacy policies typically tell consumers what they already assume: “When you put your information in the ‘shipping address’ form, we will use it to ship the product you have ordered. We may share it with the delivery carrier for that purpose.” Some regulatory safe harbor that recognizes that all information need not be disclosed all the time would make such notices far more effective.

¶150 Such safe harbors may, of course, become default industry standards. As Commissioner Leary notes, the FTC’s “Green Guides” on environmental disclosure have changed manufacturing practices, and arguably done so in a way that makes optimal use of market mechanisms.<sup>119</sup> This heightens the importance of getting notice requirements right. Setting the rules for precisely what companies must disclose, and how they must disclose it, may have the effect of dramatically skewing business arrangements. Wrongly done, such rules may undermine the benefits of information exchange described in Part II and incur many of the regulatory costs described in Part III.

## 2. *Consent/Choice*

¶151 It has become fashionable for regulators to relabel what was once generally known as “consent” (suggesting a more positive agreement consistent with opt-out approaches) as “choice” (suggesting a more affirmative election consistent with opt-in approaches). As the FTC Privacy Online Report argues:

Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to

<sup>119</sup> *Id.* at 5.

consumers) and external secondary uses (such as disclosing data to other entities).<sup>120</sup>

Regarding “choice,” the US-EU Safe Harbor Principles provide as follows:

An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. [FN: It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.]<sup>121</sup>

For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.<sup>122</sup>

¶152 Both the FTC recommendations and the Safe Harbor principles seem to contemplate simple and discrete transactions, rather than the increasingly common longer-term and more multifaceted relationships between companies and customers. And both leave the scope of “consent” somewhat unclear. If “consent” means that a user is agreeing to the purposes set forth in privacy notices, the “consent” requirement adds nothing. If it means more than that, what exactly does it mean? That a customer must affirmatively consent to any use even where notice is given? Or consent to uses that are not expected (notwithstanding their disclosure in a notice)? But if so, what is the purpose and value of notice?

¶153 Commissioners Leary and Swindle have both highlighted the risks of an overly broad understanding of consent: a free-rider problem that is part of the larger inequities discussed in Part IIB. As Commissioner Leary put it in the context of online profiling:

If mandated “Choice” simply refers to some mechanism whereby a consumer can either grant or refuse permission for online profiling, I would have no problem with it. A consumer should have the ability to exit the site before the fact of the visit becomes part of a profile. If, however, “Choice” means that a consumer can exercise this choice (either by opting out or failing to opt in) and still obtain the same benefits as a consumer less solicitous of privacy, it could be unfair. Consumers who object should not have a legally guaranteed right to “free ride” on possible value and corresponding benefits made possible by the cooperation of those who do not object. Put another way, it should not be illegal to reward consumers who are willing to be profiled. The question of appropriate rewards or

<sup>120</sup> PRIVACY ONLINE REPORT, *supra* note 66, at iii.

<sup>121</sup> SAFE HARBOR PRINCIPLES, *supra* note 113.

<sup>122</sup> *Id.*

penalties attendant upon the exercise of various options can be extremely complicated.<sup>123</sup>

In the more general context of online privacy, he noted:

The [Privacy Online] Report recognizes, for example, that it may be appropriate to provide affirmative benefits if a consumer agrees to certain personal disclosures. If the collection of data is one thing that makes it possible for a vendor to offer lower prices, consumers who are particularly tender of privacy would otherwise be able to free ride on the value created by those who are not. (If a supermarket issues a card that offer discounts to people who use it, in exchange for compilation of useful data, consumer 'choice' surely does not involve the right to get the discount without supplying the data.) On the other hand, if the premium for permission to use information is too generous, or the penalty for refusal too severe, consumer 'choice' really involves nothing more than the 'choice' to refuse dealings with the vendor. The issue of what is or is not a reasonable price differential is complicated, but may be too difficult to bother with in a situation where a particular vendor competes with a number of others that have their own policies. Does this mean that reasonableness should depend on the market power of the vendor?<sup>124</sup>

Commissioner Swindle echoed the free-riding concern:

What are the likely effects on online commerce of Mandated Choice? Would sites have to extend the same level of services and benefits to all consumers, regardless of whether some are unwilling to provide information? To the extent sites rely on the sale or use of information to offset the costs of providing services, would they discontinue services to all or to some consumers? Would all consumer have to pay more for services previously offset by the sale or use of information? Could sites shift costs only to those consumers who demand a higher level of privacy, whether in the form of fees for using the site or by reducing the level of benefits and services offered to those who choose a higher level of privacy? Or is privacy an absolute right so that all participants in online commerce—retailers and consumers—should bear the costs of Mandated Choice exercised by some consumers? If so, in the name of "Choice," this legislation may reduce the choices available to consumers in the online market.<sup>125</sup>

Such free-riding choice, which lets consumers receive goods or services without providing information in "payment," threatens businesses based on that exchange. Examples include the once hugely popular Free PC (now out of business) offering free computers in exchange for demographic information used to target ads and various ISP's (such as Net Zero) offering free dial-up Internet access on a similar business model. As Commissioner Leary noted, the exchange of personal information for discounts and free goods has parallels in traditional retail markets. The outstanding example is the supermarket discount card, which—as most consumers are aware—is used to study their purchasing patterns. These kinds of offers and discounts have frequently proven quite popular. A privacy rights advocate might argue that these economic benefits (which are often relatively more attractive to the poor) create "two classes of privacy," with poorer people more

<sup>123</sup> ONLINE PROFILING REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 99, at 2.

<sup>124</sup> PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 65, at 6-7 (citations omitted).

<sup>125</sup> PRIVACY ONLINE REPORT— SWINDLE DISSENT, *supra* note 17, at 21 (emphasis omitted).

likely to participate and thus give up some privacy. But from anything other than an absolutist rights-oriented perspective, prohibiting such discounts and business models (which in the case of Free PC helped to bridge the Digital Divide by providing free computers) seems both paternalistic and contrary to the public interest.

¶154 Perhaps the most controversial aspect of “choice” is the question of requiring customers to “opt-in” to the collection and use of their data rather than “opting-out” of such collection and use if they object to it. Privacy advocates argue that opt-out approaches put too much of a burden on consumers to protect their privacy. But opt-in approaches obviously burden everyone who wants the advantages of sharing information.

¶155 Peoples’ tendency to stay with the default option makes the question of “opt-in” versus “opt-out” privacy regimes critical. If a website chooses an “opt-in” regime, in which the permission box is prechecked and users need to uncheck it to withhold permission, a large majority of users will leave it checked. If the site chooses an “opt-out” regime, in which the permission box is unchecked and users need to check it to give permission, a large majority of users will leave it unchecked.

¶156 In the real world, this behavior means that where we require “opt-in” models, most companies won't bother to solicit information. If only 10% of your customers are providing information, it's likely neither representative nor substantial enough for you to build a program around. So where we put the bar of “informed choice” in fact makes the decision for most Americans, and dictates whether or not others will even have the opportunity to provide personal information in exchange for perceived benefits. How we interpret the European requirement of “unambiguous” consent is critical to this equation.

¶157 The FTC and Safe Harbor positions in this area give cause for concern. The Safe Harbor requires “opt-in” consent for use of sensitive information (“medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual”).<sup>126</sup> Its definition of “sensitive” information doesn't necessarily dovetail with American sensibilities. And its examples are pretty clearly only the camel's nose under the tent. One can easily imagine a number of other categories of information that are arguably “sensitive”: what books you buy, magazines you read, the clickstream traffic of your internet browser, what liquor purchases you make. In fact, the FTC has already said that “[o]pt-in procedures may be more appropriate where the information at issue is particularly sensitive— for example, the collection and use of children's personal information or sensitive medical information. . . . As noted below, hybrids may also have a role, combining elements of both opt-in and opt-out.”<sup>127</sup>

¶158 The Commission went on to note with apparent approval a proposal regarding “hybrid” choice, which stated:

Where past expectations about the nature and use of information would be changed (e.g., in cases of a material changes [sic] in privacy policy or a merger of previously non-identifiable clickstream [data] with personally identifiable information), opt-in choice has been required. By contrast,

<sup>126</sup> Exhibit B, Open Letter from Ambassador David L. Aaron (Nov. 15, 1999), at <http://www.export.gov/safeharbor/Principles1199.htm>.

<sup>127</sup> PRIVACY ONLINE REPORT, *supra* note 66, at 6 n.16.

where only future expectation [sic] are implicated (e.g., the prospective merger of PII and non-PII), opt-out choice has been provided.<sup>128</sup>

But such heightened requirements are very much open to debate.

There is no consensus as to what constitutes ‘sensitive’ information, and the definition appears to depend on personal preferences. . . . There should be no special requirement of explicit consent for the use of such an ill-defined category of data. . . . The same features that may make information sensitive may also heighten the importance of its availability.<sup>129</sup>

¶159 In some ways, the desire for “choice” and “consent” is a proxy for a desire to exercise more control over an increasingly complex world. But having to control everything is a hassle, and carries costs. Do you want to pay for programming that can no longer be presented for free? When you’re online, do you want to be asked every five seconds about a bit of data? People may say they want education and easy-to-use technological tools to take charge of their online privacy, but their actual conduct suggests that they’re not willing to sacrifice anything for them.

¶160 Finally, the ambiguity of determining which uses are “beyond the scope of” or “incompatible with” the purpose for which data was collected again presents a problem. The question is very complicated and depends on a number of variables, with open-ended regulations inviting litigation and detailed regulations likely to get it wrong.

### 3. Access

¶161 Regarding access, the FTC’s online legislative recommendation is that “Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.”<sup>130</sup>

¶162 The US-EU Safe Harbor Privacy principles provide that:

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated.<sup>131</sup>

¶163 The FTC’s Report conspicuously refused to take a position regarding the range of thoughtful and detailed alternatives set out by its own Advisory Committee on Access & Security. The Committee had spelled out access alternatives of: (1) Total Access; (2) Default to Consumer Access; (3) a Case-by-Case Approach Including Sectoral Considerations; (4) Access for Correction.<sup>132</sup> The Commission’s response was Delphic: “The Commission believes that all of these implementation options will be useful to Web sites in developing procedures to facilitate consumer access to

<sup>128</sup> *Id.* at 7 n.19.

<sup>129</sup> CATE, *supra* note 8, at 117-18.

<sup>130</sup> PRIVACY ONLINE REPORT, *supra* note 66, at iii.

<sup>131</sup> SAFE HARBOR PRINCIPLES, *supra* note 113.

<sup>132</sup> ADVISORY COMMITTEE REPORT, *supra* note 74.

personal information collected from and about them, and that the options will be relevant to any determination as to the scope of ‘reasonable access’.”<sup>133</sup>

¶164 But other language in the Report gives grounds for concern. In the words of Commissioner Leary:

[T]he Report endorsed by the majority states flatly that ‘the Commission believes that fair information practices require that consumers be afforded *both* an opportunity to review information *and* an opportunity to contest the data’s accuracy or completeness— *i.e.*, to correct or delete the data.’ (Report at 32). This is an extraordinarily broad claim, which could in many cases lead to vast expense for trivial benefit and which provides an ominous portent for the content of any substantive rules.<sup>134</sup>

¶165 The risk, of course, is the one identified in Part IIB— that of engineering a system of significant cost (ultimately borne by all consumers) to address the desires of a small fraction of the American public who are interested in looking at their credit reports.<sup>135</sup> Privacy advocates argue that such a system would make the data practices better by enforcing accountability. But part of the question is accountability against what? If the information isn’t gathered in the regular course of business, it’s unlikely to be used. And if it remains unused, the chances of misuse that harms consumers already would seem to be quite low.

¶166 Certainly, different degrees of access are appropriate for different types of information. Certain information is the basis for important decisions like the granting of credit; other information is trivial, and may not be used at all. An employee of a corner store may have noticed you on your last visit— should that be subject to inquiry? (“Did any of your employees recognize me on my last visit here?”) What about the phone records of local calls that your phone company keeps for a day? Surfing records that a website recorded ten minutes ago, and won’t be keeping beyond your browsing session? Some information is easily gathered in real time through existing systems, other information is compiled only rarely or not at all. The Advisory Committee Report acknowledges these complexities as well as others, such as frequency of access, charges for access, and access to downstream participants who may have once received information.

¶167 There seems to be a social consensus that people should have the ability to review and correct important personal information about them on a regular basis— a consensus reflected in the Fair Credit Reporting Act of 1970.<sup>136</sup> Beyond that, consensus breaks down rapidly. Certainly there’s the reflexive view that “I want to access everything about me.” But this fails to take into the costs of such a claim. Total access at all times to everything is simply overkill. The Frequently Asked Questions section accompanying the Safe Harbor principles recognizes these limitations:

[T]he right of access . . . allows individuals to verify the accuracy of information held about them . . . . [T]he obligation of an organization to

<sup>133</sup> PRIVACY ONLINE REPORT, *supra* note 66, at 31.

<sup>134</sup> PRIVACY ONLINE REPORT— LEARY CONCURRENCE AND DISSENT, *supra* note 65, at 6.

<sup>135</sup> FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY, CONCURRING STATEMENT OF STEWART BAKER, at <http://www.ftc.gov/acoas/papers/finalreport.htm> [hereinafter ADVISORY COMMITTEE REPORT— BAKER CONCURRENCE]. The Advisory Committee “heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer.”

<sup>136</sup> 6 U.S.C. §§601-622 (2000).

provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness . . . . Expense and burden are important factors and should be taken into account although they are not controlling.<sup>137</sup>

The Safe Harbor principles therefore require access only when it “is readily available and inexpensive to provide” unless the information is sensitive or used for decisions that “significantly affect the individual.”<sup>138</sup> Moreover, “[a]ccess needs to be provided only to the extent that an organization stores the information.”<sup>139</sup>

¶168 Finally, the access issue provides a concrete example of the difference— and tension— between privacy and security. In a statement concurring with the Advisory Committee report, Stewart Baker noted “[a]s the Report says: ‘Giving access to the wrong person could turn a privacy policy into an anti-privacy policy.’ If access to personal data is turned into a legislative right, Americans’ personal data will be at risk of exposure to con men, private investigators, suspicious spouses— anyone who has the *chutzpah* and the scraps of information needed to plausibly impersonate their target.” Mandating access under these circumstances creates a risk of liability for companies damned if they require clear and convincing proof of identity before giving access, and damned if they don’t and are exploited by a con man. While there is thus a need for liability protections and a safe harbor for access practices, the reality of American litigation means that the combination of access standards and safe harbors will effectively become requirements, driving business practices in ways that may not clearly benefit consumers.

#### 4. Security

¶169 The FTC’s final online legislative recommendation is that: “Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.”<sup>140</sup> Similarly, the Safe Harbor principles provide that: “Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.”<sup>141</sup>

¶170 Security (especially “reasonable” security) is obviously a fine idea. And it was the only point of consensus among the variety of experts represented on the FTC’s Advisory Committee. But there is no compelling evidence that the government needs to take a role: “The Committee did not hear any evidence that consumers had actually suffered significant losses from exposure of their personal data on the Internet (it appears that losses from the well-publicized hacker thefts of credit card information fell mainly or exclusively on merchants and banks).”<sup>142</sup> Any requirements specified by security are likely to be expensive and not well-tailored to the needs of any individual company. They will therefore likely exclude at least some smaller competitors from the marketplace.

<sup>137</sup> U.S. DEP’T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES – FAQ #8, Question/Answer #1, at <http://www.ita.doc.gov/td/ecom/FAQ8AccessFINAL.htm>.

<sup>138</sup> *Id.*

<sup>139</sup> *Id.* at Answer #4.

<sup>140</sup> PRIVACY ONLINE REPORT, *supra* note 66, at iii.

<sup>141</sup> SAFE HARBOR PRINCIPLES, *supra* note 113.

<sup>142</sup> ADVISORY COMMITTEE REPORT— BAKER CONCURRENCE, *supra* note 135.

¶171 Consumers can already sue a company whose system was hacked, alleging that it was negligent or spent too little money to ensure the security of its systems. Such private sector enforcement— again, coupled with adverse publicity, which may take an even steeper toll— is the real enforcement mechanism for meaningful security. It is difficult to imagine a form of security notice that would be detailed enough to give reasonable comfort while still being intelligible to most users and not disclosing information useful to those interested in breaking in. In the related context of security for federal computer systems, such disclosure has been harshly criticized: “Why would an arm of the government spread the word about vulnerabilities that ‘put critical operations and assets at risk’ in a report that is available for the reading pleasure of very cracker, hacker, and terrorist from here to Libya?”<sup>143</sup>

¶172 Over time, if security becomes a concern for consumers, privacy sector security audits will likely become more common, producing a kind of Good Housekeeping Seal of Approval for security practices. But since security is typically more a matter of individual behavior than the technology and systems in place, third parties may be uncomfortable certifying another’s security practices, making the risk harder to insure against and driving up costs. But we’re a long way from that particular market failure, and it’s not at all clear that the FCC rather than a professional information technology group is in the best position to set benchmark security standards.

#### 5. *Enforcement*

¶173 The FTC has not laid out its position on enforcement, but presumably envisions receiving civil and criminal enforcement authority. Moreover, statutory benchmarks or regulatory benchmarks or safe harbors could, expressly or implicitly, create private rights of action for any variance from their terms.

¶174 Regarding enforcement, the Safe Harbor Principles provide:

In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual’s complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.<sup>144</sup>

¶175 Enforcement was briefly a major sticking point between the U.S. and the EU in negotiations over the Directive, until the Europeans concluded that they didn’t want to be the world’s privacy policemen and deferred in the first instance to the traditional regulatory authority of the Federal Trade Commission, which had bared its fangs in the Geocities enforcement action.<sup>145</sup> The existence of traditional

<sup>143</sup> Mick Brady, *U.S. Security Scare: Dumb and Dumber*, E-COMMERCE TIMES, Sept. 14, 2000, <http://www.ecommercetimes.com/news/viewpoint2000/view-000914-1.shtml>.

<sup>144</sup> SAFE HARBOR PRINCIPLES, *supra* note 113.

<sup>145</sup> Geocities complaint available at <http://www.ftc.gov/os/1998/9808/geo-cmpl.htm>; Geocities consent decree available at <http://www.ftc.gov/os/1998/9808/geo-ord.htm>.

remedies for misrepresentation and detrimental reliance also rebuts critics of TrustE, BBBOnline, and other industry-sponsored privacy initiatives. Such efforts have had significant success in encouraging major websites to post statements of what they intend to do with personally identifiable information. Once companies make such statements to the public, they then become subject to all of the traditional enforcement power of the FTC under Section 5 of the Federal Trade Commission Act, state regulatory analogues, and consumer class-actions. If a company says that it's not going to do something with personal information but then proceeds to do it, and a consumer relies on the misrepresentation to his or her detriment, that's fraud and the company can be prosecuted as they would be in any other fraudulent transaction.<sup>146</sup> The need for some showing of actual harm to consumers is a healthy counterweight to the risk of enforcement actions based on technical violations.

¶176 Even more powerful sanctions against misuse of personal information come in the form of adverse publicity. Think of just the public privacy “scandals” of recent years— Lotus Marketplace, P-Trak, state DMV sales of driver’s license records, Real Networks Real Download software, the DoubleClick/Abacus merger, Geocities, various Microsoft and Netscape browser bugs, Toysmart.com, the outsourcing of site analysis to Coremetrics, and inadvertent violations by TrustE of its own privacy policy. While not one resulted in any significant harm to consumers, the companies involved virtually all took significant hits to their stock prices, and in every case the programs were either withdrawn or promptly fixed.<sup>147</sup> Governmental programs deemed to have privacy risks— such as the FBI’s “Library Awareness” program or the Department of the Treasury’s “Know Your Customer” program— met similar fates. Even privacy advocates concede that “[t]he bad publicity generated by a ‘privacy outrage’ far outweighs any possible revenue that a company might earn from its customers” and recommend a strategy of “publicize and litigate” in response to potential privacy problems.<sup>148</sup>

¶177 As I have noted at several points, this reliance on market-based public opinion echoes the argument of John Hart Ely’s *Democracy and Distrust*. While we can hypothesize potentially horrible results of the legislative process— such as a law requiring every citizen to have a kidney removed— the best safeguard is not judicial activism in the form of substantive due process (with all of its attendant costs), but rather reliance on the more pedestrian realities of democracy that make such an outcome highly unlikely. Similarly, in the commercial context, the best safeguard against outrageous misconduct or misuse of personal information is the force of public reaction. Certainly the media has not been shy about publicizing even theoretical privacy problems at a rate that far outstrips their real impact on the lives of Americans. As recent privacy stories demonstrate, these consequences (and the inevitable follow-on lawsuits) are often more severe than any regulatory response, and come without the burdens, bureaucracy, and market-distortions that regulation inevitably entails for the many good actors as well as the few bad ones.

¶178 There’s little evidence that existing laws have proven insufficient in deterring privacy problems, or that there’s a need for additional private rights of action. It is

<sup>146</sup> The FTC has filed an increasing number of actions against companies and individuals to halt fraud on the Internet. Ann Bartow, *Learning Law in Cyberspace* n.5 (July 31, 1999), <http://www.cyberspacelaw.org/bartow>.

<sup>147</sup> See generally, Marcia Stepanek, *None of Your Business*, BUS. WK., June 26, 2000, at 78 (reviewing business costs of privacy problems, including reduced stock price, lawsuits, and adverse media stories).

<sup>148</sup> GARFINKEL, *supra* note 3, at 172.

simply not that case that there's no justice unless some plaintiff lawyer gets rich. The world of personally identifiable information is rife with "eggshell plaintiffs" who may allege outsize damages from the mishandling of what would seem to be trivial information. Even being seen at the movies with someone during the day may be hugely damaging if it causes you to lose your job or get a divorce. And it's virtually impossible for the recipient of such information to know whether it's sensitive or not. Moreover, since many problems are inadvertent (given the increasingly difficult task of managing information flows), it's unclear whether additional sanctions will further reduce privacy problems, or merely transfer funds from deep corporate pockets to the deep pockets of trial lawyers.

#### 6. *Onward Transfer*

¶179 The Safe Harbor principles provide:

To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing . . . . [FN: It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.]<sup>149</sup>

¶180 The FTC seems to support limits on third-party transfers, although it fails to acknowledge the Safe Harbor principles' exception for agents, which is essential in the era of the borderless corporation. At a minimum, any U.S. regulations will need to carve out contractors, consultants, agents, and vendors in privity with the data recipient and complying with its privacy policies, as described in the Safe Harbor approach. Even with the exception, it will be hard to be a vendor: imagine United Postal Service workers reviewing and complying with dozens of different customer privacy policies for different deliveries. Moreover, many if not most companies have a number of corporate affiliates—formally distinct corporate entities that are still legally responsible for one another's actions. Prohibitions on interaffiliate transfers of personal information (as under the Gramm-Leach-Bliley financial industry reforms)<sup>150</sup> handicap a number of otherwise beneficial exchanges.

¶181 We perceive the grocer differently from the barber, and look to personal relationships to govern the handling of information. We don't have those same relationships with the groups of people who make up modern corporations. The recent controversy over Toysmart.com's entry into bankruptcy and its related effort to sell its customer list to another company (which bankrupt companies have done

<sup>149</sup> SAFE HARBOR PRINCIPLES, *supra* note 113.

<sup>150</sup> Pub. L. No. 106-102, 113 Stat. 1338 (1999).

for generations), is thus something of a red herring. So long as information is being used within the “intended scope” of a transaction, the precise identity of those using it shouldn’t matter, although material statements about future uses made to those supplying the information should continue to “run with the land” regardless of future transfers.

### 7. Data Integrity

¶182 For their final component, Data Integrity, the Safe Harbor principles provide as follows:

Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. Personal information must be relevant for the purposes for which it is to be used.<sup>151</sup>

¶183 Again, the goal is unexceptionable, but “the devil is in the details.” What is meant by “reasonable steps,” and what degree of contact is required? Does this rule apply to downstream recipients of data? If so, for how long? Does it matter whether the information is “sensitive” or not? Filling in these blanks is necessary to give any meaningful sense of the costs of such a requirement.

## V. CONCLUSION

¶184 Privacy— like most good things in life— entails costs. Many of the benefits of information exchange are immediate, tangible, and readily apparent. Others are more systemic and inherent in the operation of the market. Yet others are collective or communal, requiring collective action to bring them about. It’s a fundamental irrationality of human nature to take for granted the good things we enjoy and complain about the imperfections. But in the exchange of information, the two are often inextricably intertwined.

¶185 As Jane Jacobs (writing about building urban landscapes) and Larry Lessig (writing about building computer networks) have argued, the architecture of public space matters.<sup>152</sup> Our public policy choices will largely determine whether the architecture of information transfer not only protects privacy but also fosters the delicate and intangible evolution of organic community. The right amount of privacy and anonymity empowers both individuals and the community.

¶186 Decisions over the handling of information involve both marketplace economic interests and civil and political interests less susceptible of market-based analysis. The first step in analyzing the trade-offs involved in enacting new regulations is identifying the benefits of new technologies or ways of doing business in order to weigh them in the balance with the benefits of privacy and the costs of regulation. The argument is not against privacy— indeed, in some circumstances, it may call for expanding the boundaries of privacy. But it does suggest the need for a fine-

<sup>151</sup> SAFE HARBOR PRINCIPLES, *supra* note 113.

<sup>152</sup> JANE JACOBS, *THE DEATH AND LIFE OF GREAT AMERICAN CITIES* (1961); LAWRENCE LESSIG, *CODE, AND OTHER LAWS OF CYBERSPACE* (1999).

grained evaluation of an extraordinarily complex technological and social phenomenon.

¶187 A premature insistence on regulatory control over market approaches to the problem may distort or prevent the evolution of initiatives that produce lower prices, increase convenience, provide more secure records, and foster new and widely beneficial civic and political interchange. With those benefits hanging in the balance, individuals, businesses, and regulators should tread carefully in giving privacy an exclusive position at the table.