THE COSTS OF PRIVACY

KENT WALKER*

Privacy is both an individual and a social good. Still, the no-free-lunch principle holds true. Legislating privacy comes at a

* Senior Vice President & General Counsel, Liberate Technologies. The opinions expressed herein are the author's and do not necessarily reflect those of Liberate. This essay is a revised version of remarks delivered at the Federalist Society Twentieth Annual Student Symposium on "Is Technology Changing the Law?" at Boalt Hall School of Law, March 9-10, 2001.

cost: more notices and forms, higher prices, fewer free services, less convenience, and, often, less security. More broadly, if less tangibly, laws regulating privacy chill the creation of beneficial collective goods and erode social values. Legislated privacy is burdensome for individuals and a dicey proposition for society at large.

Information flows in subtle and nuanced ways, and well-intentioned regulations can easily go awry. After all, enforcing privacy restricts the free flow of information. Putting First Amendment implications aside, limiting the communication and use of personal information strikes at the heart of the New Economy, known formerly as "the Information Revolution." Many of the privacy laws proposed or enacted to date have been overbroad, inefficient, bureaucratic, and inconsistent. A review of the numerous hidden issues associated with typical elements of "fair information practices"—notice, consent, access, and third-party transfer—reveals the difficulty of translating these general notions into sensible policy.

I argue not against privacy but in favor of striking a reasoned balance between privacy and other countervailing interests; not against regulation but in favor of carefully tailored regulations to address specific problems at minimal cost.

I. THE INDIVIDUAL, COLLECTIVE, AND SOCIAL COSTS OF PRIVACY REGULATION

Most people want to know things about others but simultaneously want to block others from knowing personal information about them. The desire to exercise complete control over one's personal information is understandable as a means of maintaining a zone of privacy and reducing the possibility that information will be misused. But to what degree should we incorporate such preferences into actual regulations? More important, what would we lose—individually, collectively, and socially—from legislating broadly in this arena?

The question cannot be answered by a blithe invocation of privacy rights. We have no inalienable right to keep others from talking about us. You have no legal right to prevent your local baker from telling an assistant that you like cinnamon rolls. Nor do you have a legal right to demand to see if you are on your local florist's list of good customers. Leaping to

assertions of nonnegotiable rights unfortunately tends to preempt reasoned discussion of the costs and benefits of regulatory action.[1]

The alternative—tallying the costs and benefits of new information regulations—would seem uncontroversial. Yet a cost-benefit perspective is notably absent from the contemporary debates over information privacy. For example, the Federal Trade Commission omitted such a review before issuing its May 2000 Privacy Report calling for privacy legislation.[2] As Commissioner Orson Swindle noted in dissent:

> [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 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.[3]

The following sections undertake a cost-benefit analysis of regulating the use of personal information in the New Economy.

A. Individual Costs

The costs to individual consumers of regulating the use of personal information are relatively clear.[4] Such regulation would likely increase both direct and indirect costs to the individual consumer, reduce consumer choice, and inhibit the

---

1. *See, e.g.*, AMITAI ETZIONI, THE LIMITS OF PRIVACY 183-200 (1999); Declan McCullagh, *Expert: Go Easy on Privacy Regs*, WIRED NEWS (Sept. 19, 2000), *at* http://www.wired.com/news/politics/0,1283,38893,00.html (citing Professor Richard Epstein and arguing that in the area of privacy, one should consider the likely outcomes of governmental regulation before "staking out extreme positions").

2. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000), http://www.ftc.gov/os/2000/05/testimonyprivacy.htm [hereinafter PRIVACY ONLINE REPORT].

3. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE—DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE 16 (May 2000), http://www.ftc.gov/os/2000/05/privacyswindle.htm [hereinafter PRIVACY ONLINE REPORT—SWINDLE DISSENT].

4. *See, e.g.*, PAUL H. RUBIN AND THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION (2001), *available at* http://www.pff.org/RubinLenardpdf.

growing trend toward personalization and tailoring of goods and services. Laws that make it harder for you to share contact information also make it less likely that you will receive the discounts and offers that interest you—whether free videos, discounts on kids' toys, a deal on a new computer, or cut-rate airfare. These kinds of tailored offers reduce the cost of living for millions of Americans.

From a macroeconomic perspective, targeted offers reduce marketing and distribution costs for sellers, and thus ultimately reduce the prices of all goods and services. Auctions, reverse auctions, and other pricing innovations that make it easier for buyers and sellers to exchange information not only reduce online prices but also create competitive pressures that reduce offline prices as well. Online exchanges that help buyers and sellers locate each other also facilitate the sale of perishable goods—airline tickets, hotel rooms, and long-distance time—that would otherwise go to waste. Some of this targeting and tracking is automatic, as when a supermarket provides a discount coupon for jelly on the back of a receipt given to someone buying peanut butter, but much of it requires depositing information into a database for later retrieval.

Recent studies have shown the significant costs of erecting elaborate systems to track and monitor personal information but have not considered the second-order costs of the burdens imposed on individual consumers. Costs for the online sector alone have been estimated at $9-36 billion.[5] The costs of the recently adopted privacy regulations in the health industry, even as liberalized by the Bush Administration, are estimated at $17.6 billion.[6] Such costs are passed on to consumers in the form of higher prices and, ultimately, reduced consumer choice.[7]

---

5. *See* Robert W. Hahn, *An Assessment of the Costs of Proposed Online Privacy Legislation* 23 (May 7, 2001), *at* http://www.actonline.org/pubs/hahnstudy.pdf.

6. *See HIPAA Privacy Standards*, (updated Jan. 24, 2001), *at* http://www.privacilla.org/hipaaprivacy.htm.

7. FTC Commissioner Orson Swindle noted this effect when he observed:

> [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 [FTC'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

Beyond higher costs and reduced access, information restrictions threaten to burden the personalization and tailoring of goods and services—one of the signal advantages of the new technology infrastructure. Federal Reserve Board Chairman Alan Greenspan has cited the use of detailed data to fine-tune product specifications to most individual customer needs as one of the reasons for the rapid rise in U.S. productivity over the last decade.[8] From a personal perspective, there is comfort and convenience in knowing that, like your local restaurant, your retailer knows your name, knows your "usual," and knows that you like a table by the window.

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."[9]

Having some personal information accessible online—using third parties to warehouse information like billing and shipping addresses, credit card numbers, and individual preferences—has advantages. It can dramatically simplify the purchasing experience, ensure that you get a nonsmoking room, or automate the task of ordering a kiddie meal each time your child boards a plane. Giving others information about your purchases lets you receive notice of recalls, facilitation of technical support, and discounts on related products. In the not-too-distant future, information sharing may let intelligent agents do your shopping and store valuable information resources on a free-floating network accessible from anywhere.

---

want? What costs will it impose on consumers who do not care about privacy or are willing to make some tradeoffs?

PRIVACY ONLINE REPORT—SWINDLE DISSENT, *supra* note 3, at 24 (emphasis omitted).

8. *See High-tech Industry in the U.S. Economy: Hearing Before the Joint Economic Committee, U.S. Congress*, 105th Cong. (1999) (statement of Federal Reserve Board Chairman Alan Greenspan), *available at* http://www.federalreserve.gov/boarddocs/testimony/1999/19990614.htm.

9. Edward C. Baig et al., *Privacy*, BUS. WK., Apr. 5, 1999, at 86. Excite's later acquisition and subsequent bankruptcy does not affect the example's demonstration of the value of such personalization.

Even the kinds of programs that might be deemed unacceptable uses of customer information—like Amazon.com's foray into charging different shoppers different prices for the same books—offer overall savings to users. After receiving unfavorable press coverage, Amazon dropped the practice, which was merely a variant of other types of benefit programs for loyal customers.[10] Through Green Stamps, loyalty programs, and premier frequent-flyer clubs, many companies have traditionally offered different promotions and levels of service to different customers. Classical economics holds that such price discrimination is efficient, resulting in the socially optimal production of the goods or services in question.[11] 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."[12] The distributional effects might even be progressive because the more affluent are typically less price sensitive and, thus, likely to be charged more.

Although overbroad privacy regulations certainly threaten to burden all of these individual advantages, such costs have been widely discussed. The collective and social costs of privacy regulation are less obvious but no less real or important.

B. Collective Costs

Broad-brush privacy laws risk upsetting a delicate balance of incentives that produce many collective benefits. Three issues arise in the collective cost analysis: 1) informational network effects that make technologies more valuable as the number of users increases; 2) the difficulty of handling informational externalities so that social actors face the true costs of their choices; and 3) the need to have a critical mass of participants sharing personal information before a collective information benefit is worth providing. These phenomena highlight how the regulation of personal information comes at a high

10. *See Different Prices for Different Folks*, MSNBC (July 17, 2001), *at* http://www.msnbc.com/news/601667.asp.

11. *See, e.g.*, HAL R. VARIAN & CARL SHAPIRO, INFORMATION RULES 40-43 (1999).

12. Paul Krugman, *What Price Fairness?*, N.Y. TIMES, Oct. 4, 2000, at A35.

collective cost.

1. Network Effects

Information is the quintessential network good with its exchange frequently benefiting others not party to a specific transaction. Network effects arise with any technology or system whose value increases with the number of people who use it. The doctrine of network effects—discussed in technology circles as Metcalfe's Law (the power of a network increases with the square of the number of its users) or in antitrust debates over the Microsoft case as the lock-in effect (the more users of a technology, the more attractive the technology becomes)—applies in spades to both the flow of information and efforts to impede that flow.[13]

The telephone system and the postal service are two traditional examples of network effects. The more people who have phones, the more valuable your phone becomes. Similarly, the more people who can receive your letter, the more value the postal service offers you. The rise of the Internet and modern information-processing technologies (whether used in high-tech online databases or the information exchange that underlies the credit card authentication and check clearing performed by banks) did not invent the phenomenon, but they have accentuated its benefits. By making information more exchangeable, more "network-able", they have created new offerings of goods and services while reducing the price of others.

For example, consider collaborative filtering, which powers Amazon.com's surprisingly useful book recommendations by analyzing the other books purchased by people who bought the same book you have.[14] The accuracy of the recommendations increases according to the number of participants. If Amazon had to get the consent of each user, participation rates would fall (because of the free-rider problems described below[15]) and the quality and value of

13. For a general discussion of network effects, see Mark Lemley & David McGowan, *Legal Implications of Network Economics*, 86 CAL. L. REV. 479 (1998).

14. *See* Chris Suellentrop, *The Next Killer App*, SLATE MAGAZINE (Oct. 25, 2000), *at* http://slate.msn.com/default.aspx?id=92027.

15. *See infra* Part I.B.2 (discussing externalities and free-rider problems related to network effects).

collaborative filtering would decline for everyone. Several emerging business models are mixing individual and collective benefits by using the power of networks to reduce the costs of goods. MobShop.com and similar services let consumers join together to enroll for bargains—the more people interested in something, the lower the price. Disputes between eBay, Fair Market, and AuctionWatch over the rights to each others' listings demonstrate the value of building large auction networks—the more participants, the more variety for buyers and the more sellers get for their goods.[16] Similarly, e-commerce companies like Ariba and CommerceOne seek to create networks of interested buyers and sellers communicating information about their offerings and preferences.

2. *Externalities*

Social policy generally aims to avoid or minimize mismatches in which one person is able to derive benefits or escape costs at the expense of others. The failure to internalize these externalities variously takes the form of free riding[17] (in which an individual derives benefits from a collective benefit without paying the costs), the Tragedy of the Commons effect[18] (in which an individual derives benefits while imposing costs on the community), or the Chinese Restaurant Problem (in which an individual pays only a portion of the costs of the benefits received). The exchange of personal information presents all of these issues.

The most straightforward example is the unlisted telephone number. Delisting your telephone number is like concealing your street address: it makes it harder to find you. Being difficult to find may be advantageous when direct marketers

16. For information on the dispute between eBay and Auctionwatch, see Hiawatha Bray, *EBay Blocks Move to Index its Net Auctions*, BOSTON GLOBE, Nov. 10, 1999, at C2.

17. A classic free rider problem exists when "there is no way to provide the service without benefiting everyone." ROBERT S. PINDYCK & DANIEL L. RUBINFELD, MICROECONOMICS 652 (3d ed. 1995).

18. *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.

want to call during dinner—but what about friends, relatives, or business associates who have mislaid your number or with whom you would have gladly shared your number but never did? A world without telephone directories would lack an important and useful tool for facilitating communication. Even if participation in telephone directories were handled on an "opt-in" basis, the result would be smaller, less-useful directories (akin to current off-brand commercial directories). The use of caller ID poses a similar problem, pitting users seeking to block unwanted calls against callers who "block" display of their numbers, with both imposing their preferences on the other.

Although there is often little individual incentive to participate in the aggregation of information about people, an important collective good results from the default participation of most people. One problem is the tendency to want a free ride—sharing nothing about yourself but wanting access to information about others. Opt-out policies for information exchange—leaving someone's information available for compilation unless they object—can provide exactly the right set of incentives to counter-balance such free-riding and produce the optimal social outcome. People with strong privacy preferences will not participate, while those with milder preferences will, resulting in the collection 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.

The world of email offers an example of the difficulties that might be created if we removed these counter-balancing incentives. It is hard to track down someone's email because there is no substantial counterpart to the phone book for email addresses; this occurs largely because most corporations will not allow broad access to their databases of employee email addresses for fear that headhunters will poach their workforce. In furthering their own interests, they complicate the lives of others outside the corporate walls hoping to reach those inside. The lack of a means to capture the benefits of widely available information disadvantages outsiders.

3. Critical Mass

The aggregation of information often requires a critical mass

to be worthwhile. A phone book with only one out of ten numbers would hardly be worth using, and thus would not be worth printing. Privacy laws that make it more difficult to assemble a critical mass of information or a critical number of users eviscerate the basis for the creation of new types of consumer benefits.

Many new systems for processing information depend on universal, or at least strong majority, acceptance to be workable. For example, Intelligent Transportation Systems seeks to ease traffic congestion by using peak pricing—charging higher prices at rush hour.[19] To accomplish this without inefficient back-ups at tollgates, cars need 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 less congestion all drivers face. Unless a minimum number of drivers participate, it is not worthwhile to institute or maintain the system. The classic Tragedy of the Commons aspect of such situations is clear.

If we use new laws to eliminate the counter-balancing incentives necessary to encourage individuals to permit their information to be available to others, we create a range of unanticipated problems as these carefully balanced systems unravel.

C. Social Costs

Perhaps the most important consequence of potential privacy laws is also the least remarked upon. Privacy advocates trumpet the advantages of creating new privacy rights while businesses emphasize the costs and loss of convenience that would result. There are few advocates, however, to speak for the social costs exacted by growing individualism and isolation.

There is a vicious cycle at work here. Declining levels of trust in institutions breed increased interest in privacy, but increasing levels of privacy (and consequent declines in accountability and security) further decrease trust. Surveys taken since 1978 by Dr. Alan Westin, the leader of the modern

19. *See* Claire Starry, *The Emerging In-Vehicle Intelligent Transportation Systems Market*, BUS. ECON., Apr. 1, 2001, at 49.

privacy movement, "have shown that the higher a respondent's general distrust of institutions and fears of technology abuse by organizations, the greater will be the concerns about privacy."[20] Although the social causes for such concerns may be diverse—such as growing affluence that allows people to pursue private rather than communal pursuits, technologies like television that encourage isolation, the move from small town familiarity to urban anonymity, or media coverage of negative stories about business and government—the consequences are very real.

New limits on information sharing may exacerbate our declining sense of community, security, accountability, and trust.

1. Loss of Community

How does information exchange facilitate community? Online communities are flourishing; America Online's Member Directory boasts more than 32 million users.[21] Members post personal information about themselves to encourage other people to contact them about topics of mutual interest and to provide background information about themselves when they contact other users. More generally, the wider availability of contact information (whether telephone numbers, physical addresses, or e-mail addresses) promotes both offline and online interaction (like getting reacquainted with someone you knew in high school or college). Every time you join a list-serv, a group e-mail list of friends, or a discussion group of colleagues, you are sharing information about your interests. Providing information about ourselves gives texture to our public persona, permits tailoring of information, and provides traction to others who seek to engage us. Other, noncommercial projects like the "SETI@home" initiative, which uses the power of idle computers to help in the search for extra-terrestrial life, the Human Genome Project's effort to map the intricacies of human chromosomes, or ad hoc initiatives to crack specific types of encryption or solve other complex mathematics

20. *Opinion Surveys: What Consumers Have to Say About Information Privacy: Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce*, 107th Cong. 3-4 (2001) (statement of Dr. Alan Westin).

21. *See* America Online, *Who We Are, at* http://www.corp.aol.com/whoweare.html (last visited Dec. 31, 2001).

problems, entail the sharing of certain personal information to pool the resources of huge numbers of people in pursuit of a common goal.

Moreover, some communities are implicit. The collaborative filtering used by Amazon.com and other sites to track preferences for movies, music, and collectibles can allow a virtual community of admirers—whether of privacy literature, Kurosawa films, or Limoges china—to establish links and share ideas. Although such groups are quite different from our traditional images of community, they may be harbingers of the communities of the future. Indeed, the rise of the sort of "urban anonymity" to which we have become accustomed is arguably a passing phase between the closeness of small-town agrarian life and the individualized information society (and types of communities) made possible by computer technologies.[22]

At bottom, privacy reflects an individualistic ethos and disclosure a communitarian one. As Indiana University Professor and noted privacy scholar Fred Cate has noted:

> 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.[23]

Different social goals drive different regimes of privacy and disclosure. Where candor is at a premium, perfectly consequence-free anonymity may be most appropriate. Where there is a concern about disruptive behavior, pseudonymity may be best. Where trusting relationships are paramount, full disclosure and personal responsibility is likely preferred. This is a fine-grained calculus that requires more than one-size-fits-all legislation to address it adequately.

2. *Loss of Security*

Many people confuse security with privacy when, in fact, the

22. *The End of Privacy*, ECONOMIST, May 1, 1999, at 16 (citing George Gilder).
23. FRED CATE, PRIVACY IN THE INFORMATION AGE 30 (1997).

two are often in tension, if not squarely opposed. The very identifiers that raise the most controversy—social security numbers, driver's licenses, or universal health care cards—are essential in ensuring that the file for John M. Smith is not confused with the file for John N. Smith.

More broadly, authenticating your 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 personal information—a combination of birth date, social security number, and mother's maiden name—and you will soon be back in your room.

Distributed information can similarly reduce the costs of fraud and other economic crime. 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 to detect whether someone may have stolen your number. When your bank calls to report an unusual spending pattern on your credit card, you are getting proactive customer service that simply would not be possible if the bank did not have access to data about your purchasing history. Authentication—passwords, certificates, and digital signatures—plays a critical role in network security.

Although most Americans would gladly trade, and have in fact traded, some degree of privacy for greater security and accuracy of their data, particularly after the terrorist attacks of September 11, 2001, privacy concerns effectively defeated several earlier 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.[24] Microsoft disabled its globally unique identifier (GUID), which helped 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.[25]

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

24. *See* Baig et al., *supra* note 9, at 86.
25. *See id.*

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.

It is certainly correct that technology removes the gray areas to which we have grown accustomed. Authenticating technologies have the potential to identify their author, or at least the authoring machine, with a high degree of certainty, thereby increasing the security of sending financial or other sensitive information online.

The main result of increased identification would likely be less crime and anti-social behavior. 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. As noted above, the GUID in Microsoft Word enabled law enforcement to apprehend the creator of the Melissa virus. Deterring such crimes provides a real social benefit and necessarily weighs on the scales when evaluating legislation that would prevent or discourage the use of identifying information.

3. Loss of Accountability

Advocates of new privacy rights accept as a premise that anonymity is a good thing, a bulwark against snooping corporations and governments. Sometimes it is. Sometimes, however, it cuts against essential social ties of accountability and reputation. Communities rest not only, nor even chiefly, on laws but rather on social norms and mores, which work on a far more subtle basis than centralized command-and-control regulation could ever hope to do.[26] Norms and social sanctions help structure and order society, counteracting the tendency of pure economic man to free ride or abuse freedoms.[27] 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. Anonymity disables these critical social stabilizers, the social norms that encourage us to do the right thing. While anonymity has great value in

26. *See generally* Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 412-16 (1997).

27. *See id.*

protecting the free speech of dissidents and minority viewpoints, it cannot be a fundamental organizing principle for a well-ordered community.

Anonymity can also operate as the cloak of night—promoting negative behavior and disregard for the rules that organize social interaction. Imagine 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 is 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 stronger when you are in your neighborhood, your office, or your local store—anywhere you know the other shoppers and they know you.

Perhaps the best example on the Internet is the distinction between the behavior of those using webmail, which is typically free and anonymous, and subscription-based e-mail via an Internet service provider, which, for billing purposes, necessarily knows the true name and address of the subscriber. In my experience as counsel to Netscape and America Online, webmail users create a disproportionate amount of abuse and spam while subscription e-mail users, subject to the potential loss of their account and even criminal sanctions, are relatively less disruptive.

Problems result, however, where potential offline gains dwarf the value of online participation. The clearest example is stock chat rooms in which 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.[28] 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. This system, however, is still subject to manipulation and evasion—online auctions accounted for 87 percent of Internet fraud in 1999.[29]

---

28. *Market Manipulation, Particularly Online, Is Way Up, SEC Says*, WALL ST. J., Nov. 6, 2000, at A26.

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

The use of information networks—whether based on credit cards or social security numbers—provides a form of reputational credibility necessary to operate in the modern world. New privacy regulations would not change the need for reputational confirmation before someone will do business with you, although they may make it more burdensome to provide.

Moreover, as Professor Cate has noted, "[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.'"[30] In other words, the more regulation we have of information flows, the greater the opportunity for fraud and the higher the resulting costs for those dealing honestly.

4. Loss of Trust

The final consequence of increased privacy regulation of personal information is the loss of trust. Trust can be a direct result of communal exchanges, but it is also an approach to information sharing and a product of a society in which we feel comfortable sharing information.[31] Although 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 do not need to lock your car or your house at night with psychological and social benefits that go beyond not having your house burglarized or your car stolen. As a general rule, the fewer the locks, the happier the society.

Trust has its own tangible benefits. Nations lacking the widespread social lubricant of trust are forced to resort to

---

30. CATE, *supra* note 23, at 28 (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).

31. As Stewart Baker, former General Counsel to the National Security Agency, 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 unsigned letters to the editor. And none of us would want to walk in a city where all the pedestrians were masked.

Stewart Baker, Privacy, Anonymity, and the Attack on Authentication Technologies 2 (1999) (unpublished manuscript, on file with author).

cumbersome modes of exchange and enforcement to assure the performance of everyday commercial exchanges. Witness, for example, the virtual impossibility of using checks or credit cards in Russia. A bad-check percentage of 1 percent is acceptable; a bad-check percentage of 20 percent puts one 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 new forms of economic exchange. For example, the widespread use of credit cards in the United States reflects the trust engendered by a sophisticated financial clearing system. Europeans, lacking such a system, generally do not have credit cards and are far more constrained in their financial dealings. As a general rule, the fewer the locks, the happier the society.

In the privacy context, the question is who to trust to have access to personal information. In the commercial context, consumers generally trust a company not because it does not exchange or trade information but because it gives them what they want in a timely fashion. As a consumer, you effectively decide every day whether any given company will deliver the goods, follow through on the warranty, refund your money (if necessary), or notify you of product recalls. Consumers trust companies based not on a privacy policy, but on a constellation of brand, imagery, reputation, explicit statements, individual experience, and the risks involved in providing specific information. You trust L.L. Bean because its size makes it likely it will 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 legal action if a problem arises. As a repeat, long-term player in the catalog business, L.L. Bean has a strong incentive to keep its customers happy to promote future buying and reduce public complaints. Trust is established by economic incentives, reputation, and exposure to consequences. Not coincidentally, such trust is 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—reflecting your decent credit history—and your record of having done business with them in the past.

In comparison to these daily concerns, privacy consequences are often indirect, delayed, opaque, and, for most people,

relatively minor. While legal requirements mandating specific information practices are one way of promoting such trust, they are hardly the only or even the most effective way. A trust relationship typically reflects a complex and fine-grained assessment—not one readily replaced by universal government regulation or mandate.

Many privacy advocates call for narrowing circles of trust. In a complex, modern society, it is difficult, however, to tell in advance with whom you might want to have contact. The idea of trusting only those people you know 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, consequently, seeing a need to lock all of your windows lest a thief enter.[32] 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 in the kindness—or at least the honesty—of strangers.

In sum, laws that reduce information sharing and promote anonymity block the operation of reputational capital. If you can't judge other reputations, you're less likely to trust them and they're less likely to act in a trustworthy way. Upsetting this social ecosystem undercuts social institutions premised on trust.

II. THE THEORETICAL AND PRACTICAL PERILS OF ANTICIPATORY REGULATION

Although it is not at all clear that the government would do a better job than the private sector in overseeing the handling of personal information, regulatory initiatives would come at a cost. These costs are particularly high for many privacy laws that would impose sweepingly broad and theoretical limitations rather than narrow proscriptions focused on well-defined problems.

32. CHARLES JENNINGS & LORI FENA, THE HUNDREDTH WINDOW: PROTECTING YOUR PRIVACY AND SECURITY IN THE AGE OF THE INTERNET 26 (2000).

A. Critiques of Proposed Privacy Regulations

In 2000, the Federal Trade Commission proposed regulation concerning five requirements to provide adequate protection of online consumer privacy: notice, consent/choice, access, security, and enforcement.[33] The European-U.S. Safe Harbor Principles, also announced in 2000 following extended negotiations over how to apply the EU Privacy Directive to U.S. companies, added two requirements: onward transfer and data integrity.[34]

In some ways, both initiatives have been overtaken by recent events. Under the Bush Administration, the FTC has shown little interest in new privacy initiatives, and its earlier recommendations have not sparked parallel congressional action. Incoming FTC Chairman Timothy Muris has set forth a new privacy agenda for the agency that focuses on the enhanced enforcement of existing laws against spam, identity theft, and consumer fraud, while disavowing the Commission's earlier call for new legislation.[35] The European Union's Privacy Directive has been implemented unevenly with compliance spotty throughout the Union and some Member States not enforcing it at all.[36] Meanwhile, relatively few American companies have subscribed to the Safe Harbor Principles that went into effect July 1, 2001.[37]

Still, the two proposals remain relevant. They constitute the two most important recent efforts to establish comprehensive privacy codes, and one or more of the "Fair Information Practices" that they embody are incorporated into many bills currently pending before Congress.[38] Moreover, the prospect of

---

33. *See* PRIVACY ONLINE REPORT, *supra* note 2, at 20, 36-37.

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

35. Timothy J. Muris, Protecting Consumers' Privacy: 2002 and Beyond, Remarks at the Privacy 2001 Conference (Oct. 4, 2002), *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

36. Lisa Jucca, *Europe Leads Drive for Online Privacy Protection*, Washtech.com (May 15, 2001), *at* http://washtech.com/news/regulation/9765-1.html.

37. Robert MacMillan, *Microsoft to Adopt EU-US Data Protection Agreement*, NEWSBYTES (May 15, 2001), *at* http://www.newsbytes.com/news/01/165704.html.

38. A number of bills have been introduced in the 107th Congress that would impose various types of notice and consent requirements, including S. 1055, 107th Cong. (2001), H.R. 89, 107th Cong. (2000), H.R. 237, 107th Cong. (2000), and H.R. 2135, 107th Cong. (2001).

European enforcement of the EU Privacy Directive against American or European companies remains a threat.

Although all of the requirements of Fair Information Practices raise theoretical and practical concerns, four—notice, consent/choice, access, and onward transfer—are particularly problematic.

1. Notice

Both the FTC recommendation and the Safe Harbor Principles require 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.[39]

According to the Safe Harbor Principles:

> An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization 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.[40]

Consumer understanding of information flows is certainly valuable, if only because full information is a necessary precondition to the operation of efficient markets. Notice is thus the starting point for all of the Fair Information Practices, but even notice has its pitfalls.

After all, notice is difficult to accomplish in a meaningful

39. PRIVACY ONLINE REPORT, *supra* note 2, at 36.
40. SAFE HARBOR PRINCIPLES, *supra* note 34.

way. The key principle of notice is determining what is reasonably foreseeable and highlighting relevant variations from people's expectations. Implementing even that simple formulation is fraught with complexities. People's expectations vary greatly, particularly regarding new technologies and business models. What might be an insignificant alteration to one person could be quite material to the next. Put another way, notices are valuable only when they have an effect on behavior in the real world, when, as a result of learning something new, the reader acts differently. From this perspective, notices can be divided into three types: 1) those that tell people what they already know (and thus do not change behavior); 2) those that tell people what they do not know but do not care about (and thus do not change behavior); and 3) those that tell people what they do not know and do care about (and thus do change behavior).

Only the third category adds social value, but it is also the most rare. Far more common are notices in the first two categories—typically driven by concerns over liability. Such notices appear on the backs of baseball tickets and the pages of fine print included in the instructions of any consumer appliance. Warnings that you may be hit by a baseball at the ballpark or that you should be careful with power tools do not, however, make the world a better or safer place. They do not change real world behavior, because such risks are both immaterially remote and utterly foreseeable. Moreover, by making the boilerplate so expansive, we make it much less likely that most people will read through it to learn about unexpected but realistic risks.

The problems of privacy notices from this perspective fall into five categories: overkill, irrelevance, opacity, non-comparability, and inflexibility.

a. Overkill

Unfortunately, the most likely scenario for privacy notices is that, in the zeal to address all of the potential uses and risks of information flows, legislation will mandate overbroad disclosures. Most contemporary contracts are masses of unintelligible small print that no one bothers to read. All too often, regulators with different interests at different times deem various details—disclaimers, limitations of liability, privacy,

etc.—of great importance and require that each one be especially "clear and conspicuous." Such requirements generally translate into bold capital-letter type, resulting in a document with either a profusion of emphasis that effectively emphasizes nothing or a profusion of separate forms that are effectively unreadable in volume. Furthermore, who is to say that disclosure of privacy policies is more valuable to consumers than the disclosure of finance terms, limitations of liability, or other contract terms?

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 an information exchange. The result is likely to be about as readable—and as helpful—as the typical corporate SEC filing, which is to say not at all.

Any notices should be seen in the context of the overall consumer experience, highlighting the one or two items that are truly priorities for consumer consideration. Even more difficult, notices need to distinguish the unexpected from what is within the realm of the generally foreseeable. Otherwise, privacy notices will become digital mattress tags for the twenty-first century, unread and unloved.

b. Irrelevance

A second concern is that educating people about a complicated topic that they do not want to know about is like leading a satiated horse to unappealing 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 junk mail. Most consumers are simply not concerned enough about privacy issues to want to spend two or three minutes reviewing the privacy policies of the companies they do business with. The Platform for Privacy Preferences (P3P), which was designed to give consumers a way of expressing their detailed privacy preferences on the web, has largely died on the vine, a victim of the rigidity of its

categories and an overwhelming lack of consumer demand.[41]

The lack of consumer interest points to the tension between complete and accurate disclosure on the one hand and telling people what they want to hear 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."[42] In the online context, the information "transferred" and "collected" with virtually every visit to a site could include a user's operating system and its version number, its IP address, 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 while phone companies and cable services may track, if only temporarily, significant amounts of technical information incident to receipt of service. Even a requirement as simple as producing 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. Ultimately, regulators will need to do extensive line drawing as to what information transfers must be disclosed.

To minimize irrelevant legalese and maximize the real-world effect of notices, any requirements should stress practices and risks that are not 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. Common sense, the existing laws of negligence, and standard industry practice do provide some guidance. Unfortunately, in the interest of avoiding even a perceived privacy problem, most current privacy policies

41. As of September 28, 2001, the P3P website showed that, out of the millions of sites on the World Wide Web, barely 250 websites were using P3P and a large majority of those were very small sites with little traffic. *See* World Wide Web Consortium, *Web Sites Using P3P*, *at* http://www. w3.org/P3P/compliant_sites (Sept. 28, 2001).

42. PRIVACY ONLINE REPORT, *supra* note 2, at 24.

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." Such uses, so utterly within the reasonable foreseeable range, are useless and arguably effectively conceal notices of less intuitive practices.

c. Opacity

Both privacy advocates and those skeptical of privacy regulations have expressed frustration over the lack of clarity of many privacy policies.[43] The bedrock truth, however, is that it is difficult to track, let alone describe, all the information that is exchanged in a typical transaction, all the places that it is stored, and all the ways that it is used. The FTC has alluded to the difficulty in the technology context:

> In 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 [w]eb 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.[44]

For example, companies frequently have multiple policies that apply to different types of transactions. 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?

Like plain-English securities documents, "simplified" privacy policies are still likely to be heavy sledding. Perhaps, before passage of new notice statutes, legislators should be required to read through the detailed disclosures regarding the storage and use of personal information mandated by § 631 of the Cable Communications Policy Act of 1984.[45] Even where

---

43. *Id.* at 24-28; FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE—STATEMENT OF COMMISSIONER THOMAS B. LEARY CONCURRING IN PART AND DISSENTING IN PART 2-4 (May 2000), http://www.ftc.gov/os/2000/05/privacyleary.htm [hereinafter PRIVACY ONLINE REPORT—LEARY CONCURRENCE AND DISSENT].

44. PRIVACY ONLINE REPORT, *supra* note 2, at 22.

45. 47 U.S.C. § 551 (1994).

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.

d. Non-comparability

In his otherwise compelling and well-reasoned statement, FTC Commissioner Leary has called for disclosures of "greater clarity and comparability,"[46] noting that "[s]ome standardization of the disclosures would allow consumers to compare more easily the privacy practices of different vendors."[47] While this seems reasonable in theory, the simplification necessary for comparability comes at a significant cost in accuracy and flexibility. Fitting an individual company's policies onto the Procrustean bed of generalized abstractions inevitably renders policies more vanilla and less informative. 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 essentially 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.[48] As discussed below, these lines are less than clear and differ in different settings. 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? Does it depend on whether the company stands to profit from the notice?

This is the underlying tension between reliance on industry-standard guidelines, which would enable customers to read the guidelines and look in the right places, and a company-by-company approach, which would be more accurate but perhaps also harder for customers to follow. Boilerplate information is relatively unhelpful given the variety of business practices and types of information involved.

46. PRIVACY ONLINE REPORT—LEARY CONCURRENCE AND DISSENT, *supra* note 43, at 2.

47. *Id.* at 3.

48. PRIVACY ONLINE REPORT, *supra* note 2, at iii, 16.

e. Inflexibility

An example of what can go wrong with overbroad and static notice requirements is the Federal Aviation Administration (FAA) rule that flight attendants review with passengers the operation of seat belts before every flight. Unless a traveler has not been in a passenger car since 1962, he or she likely knows how a seat belt works. The obviousness of the message simply encourages passengers to tune out the rest of the marginally more relevant parts of the spiel, such as the location of the exits. It is a sobering illustration of regulatory inflexibility, and the prospect of applying that paradigm across a dynamic information economy is daunting. Further, even if one is comfortable 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.

The consequences of error can be draconian, especially when most privacy scandals to date reflect not malfeasance but inadvertence, reflecting the difficulty of knowing what's going on in an increasingly complex system. Several recent privacy controversies—Real Networks's 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 involved incidental or unexpected receipt of certain types of information. This phenomenon demonstrates the difficulty of tracking all of 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, offer lots of features, and transfer lots of information. In practice, this usually means lots of potential bugs and therefore many potential privacy violations. Many online privacy incidents are, in fact, software bugs or security exploits posted by hackers looking for problems with

software.[49] It would serve no purpose—and it would impose prohibitive costs—to turn every potential "privacy" problem into a violation of federal law or the target of a class-action suit.

The likely outcome: privacy policies will produce information that is unread by Americans and does not affect behavior and will result in the enrichment of the plaintiffs' bar with no benefits to consumers. Even under existing law, a plaintiff need merely show that a company's information practices varied from its notice, whether intentionally, inadvertently, or as a natural evolution over time, and that one or more consumers relied on the policy. Such regulation via lawsuit is a terrible outcome—uncertain, costly, resulting in a bad allocation of resources, and often not improving the underlying problem, if one exists.

Moreover, as notice requirements alone have proven unhelpful and burdensome, privacy advocates have upped the ante. Marc Rotenberg, head of the Electronic Privacy Information Center, which advocates additional privacy regulation, has downplayed the value of notice "without imposing any significant restrictions on how companies collect and use data."[50] Thus notice serves as an entering wedge: relatively uncontroversial, but also relatively unhelpful, and leading to calls for additional restrictions on information exchange in order to *really* safeguard privacy.

2. *Consent/Choice*[51]

Under the information regime proposed by the FTC Privacy Online Report:

> 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 consumers) and external secondary uses (such as disclosing

49. JENNINGS & FENA, *supra* note 32, at 232-33.

50. John Schwartz, *Privacy Policy Notices Are Called Too Common and Too Confusing*, N.Y. TIMES, May 7, 2001, at A1.

51. It has become fashionable for regulators to re-label what was once generally known as consent (suggesting an acquiescence consistent with opt-out approaches) as choice (suggesting a more affirmative election consistent with opt-in approaches).

data to other entities).[52]

The Safe Harbor Principles regarding choice require that:

> 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.[53]

The Principles require "opt-in" choice for "sensitive information," defined as "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."[54]

Both the FTC Privacy Online Report and the Safe Harbor Principles appear to contemplate simple and discrete transactions rather than the longer term and more multifaceted relationships between companies and customers that have become increasingly common. Further, neither proposal is clear about the scope of consent. If it means that a user is agreeing to the purposes set forth in a privacy notice, the consent requirement adds nothing to the user's existing right not to enter into the transaction. If it means more than this, the formulation is vastly overbroad and problematic. If a customer must affirmatively consent to any use even where notice is given, the customer has the ability to receive the good or service without permitting use of personal information—effectively getting in without paying the price of admission.

Commissioners Leary and Swindle have both highlighted the free-rider risks of an overly broad understanding of consent. 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,

52. PRIVACY ONLINE REPORT, *supra* note 2, at iii.
53. SAFE HARBOR PRINCIPLES, *supra* note 34.
54. *Id.*

> "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.[55]

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. . . . 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 . . . ."[56]

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 consumers 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

---

55. FTC, ONLINE PROFILING: A REPORT TO CONGRESS—PART 2: RECOMMENDATIONS—STATEMENT OF COMMISSIONER THOMAS B. LEARY CONCURRING IN PART AND DISSENTING IN PART (July 2000), http://www.ftc.gov/os/2000/07/onlineprofiling.htm#LEARY.

56. PRIVACY ONLINE REPORT—LEARY CONCURRENCE AND DISSENT, *supra* note 43, at 6-7 (citations omitted).

market.[57]

Such free-riding choice, which lets consumers use services but not provide information in payment, threatens businesses like the once popular Free PC, which while it was in business provided a free computer in exchange for the right to sell targeted ads based on users' demographic information. It harkens back to discredited notions of price controls to believe that we can cap the value of information received by vendors yet get the same goods and services in exchange. Like the notion of using new technologies to strip the advertisements from television shows or Internet sites, it is an attractive concept but not a viable long-term arrangement. It seems unlikely that eliminating such innovative ad-based business models would be in the public interest.

Perhaps the most controversial aspect of "choice" is the difference between requiring customers to "opt-in" to the collection and use of their data rather than "opting-out" if they object to it. While privacy advocates argue that opt-out approaches put too much of a burden on consumers to protect their privacy, opt-in approaches burden everyone who wants the advantages of shared information and imperil the viability of the businesses that provide those advantages.

Consumers' tendency to stay with the default option makes the question of "opt-in" versus "opt-out" privacy regimes critical. If a merchant chooses an "opt-out" regime in which the permission box is pre-checked and consumers need to uncheck it to withhold permission, a large majority of consumers will leave it checked. If the site chooses an "opt-in" regime, in which the permission box is unchecked and consumers need to check it to give permission, a large majority of consumers will leave it unchecked.[58]

Where mandated "opt-in" models drastically cut participation rates, far fewer companies will bother to solicit information. If only ten percent of customers provide information, it is likely neither a representative nor sufficiently

57. PRIVACY ONLINE REPORT—SWINDLE DISSENT, *supra* note 3, at 21-22 (emphasis omitted).

58. *See* Ari Schwartz & Paula J. Bruening, *On Consent, Choice, and Check Boxes: Sorting Out the Opt-In v. Opt-Out Debate* 4, 7, *in* CONGRESSIONAL INTERNET CAUCUS, PRIVACY BRIEFING BOOK (2001), *at* http://www.netcaucus.org/books/privacy2001/pdf/CDT.pdf.

substantial response around which to build a program. So how high we raise the bar of informed choice makes the decision for most Americans and dictates whether or not others will even have the opportunity to provide personal information in exchange for offered benefits.

Some argue that because businesses want to encourage consumers to agree to the use of information, an "opt-in" model will minimize the burden of people who want a choice different from the default. This suggestion, however, ignores the fact that the additional burden for consenting participants will reduce participation, in some cases dramatically. As a result, the good or service will not be offered at all or be offered at a higher price, with both alternatives unfairly penalizing those who would have willingly participated. Other privacy advocates have argued for a third way, in which "use" and "do-not-use" options are equally presented, with the customer having to choose one before continuing.[59] While unworkable in most contexts, the idea might be feasible for online transactions. Again, however, this approach misses the critical point that every additional button that a merchant requires a user to press cuts sales significantly—hence the importance of the wrangling over Amazon's patent of the "one-click buy." Adding a complex choice would lower sales, reduce choices, and raise prices.

The original FTC position and the continuing Safe Harbor position regarding consent give cause for concern. The Safe Harbor requires "opt-in" consent for use of sensitive information, including "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."[60] This definition of sensitive information does not necessarily dovetail with American sensibilities. Further, one can easily imagine a number of equally "sensitive" categories of information—what books you buy, what magazines you read, what Internet sites you visit, and what liquor purchases you make.

In some ways, the desire for choice and consent is a proxy for a desire to exercise more control over an increasingly complex

59. *See id.* at 5.

60. *See* SAFE HARBOR PRINCIPLES, *supra* note 34.

world. Having to control everything, however, is a hassle and carries costs. Do you want to pay for programming that can no longer be presented for free? When you are 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, much less have them imposed by government fiat.

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

Regarding access, the FTC's report recommended 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."[61]

The Safe Harbor Principles require 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.[62]

The FTC Privacy Online Report conspicuously refused to take a position regarding the range of detailed alternatives set out by its own Advisory Committee on Access & Security. The Committee had spelled out a range of access alternatives: 1) total access; 2) default to consumer access; 3) a case-by-case approach including sectoral considerations; and 4) access for correction.[63] The Commission's response was Delphic: "The

61. PRIVACY ONLINE REPORT, *supra* note 2, at iii.

62. SAFE HARBOR PRINCIPLES, *supra* note 34.

63. FTC, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY (May 15, 2000), http://www.ftc.gov/acoas/papers/finalreport.htm (citation omitted).

Commission believes that all of these implementation options will be useful to Web sites in developing procedures to facilitate consumer access to personal information collected from and about them, and that the options will be relevant to any determination as to the scope of 'reasonable access.'"[64] This effectively punts on the issue, as total access and access for correction are essentially polar opposites with total access requiring the construction of expensive mechanisms to permit collection of and instant access to insignificant data not used by the recipient and access for correction imposing minimal burdens in order to resolve mistakes that all parties would like to correct.

Other language in the FTC Privacy Online Report gives even greater 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.' 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.[65]

The risk, of course, is that we will engineer a system at significant cost to address the desires of a small fraction of the American public who are interested in looking at their credit reports on a daily basis.[66] Privacy advocates on the Advisory Committee argued that such a system would make the data practices better by enforcing accountability.[67] But part of the question must be accountability against what? If the information is not gathered in the regular course of business, it is unlikely to be used. If it remains unused, the chances of harm

64. PRIVACY ONLINE REPORT, *supra* note 2, at 31.

65. PRIVACY ONLINE REPORT—LEARY CONCURRENCE AND DISSENT, *supra* note 43, at 6.

66. *See* FTC, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY—CONCURRING STATEMENT OF STEWART BAKER (May 15, 2000), http://www.ftc.gov/acoas/papers/finalreport.htm [hereinafter FINAL 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." *Id.*

67. *See id.*

to consumers would already seem to be quite low.

Different degrees of access are appropriate for different types of information. Certain information is used for important decisions like the granting of credit; other information is trivial and may not be used at all. 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 including frequency of access, charges for access, and access to downstream participants who may have once received information.[68]

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.[69] Beyond that, consensus breaks down rapidly. Reflexively, one wants to be able to see everything about oneself immediately. This unstudied position, however, fails to take into account the costs of such a demand. 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 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 but they are not controlling . . . .[70]

The Safe Harbor Principles more reasonably 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."[71] Moreover, "[a]ccess needs to be provided only to the extent that an organization

---

68. *See id.*

69. 15 U.S.C. § 1681-1681u (1994) (requiring consumer reporting agencies to adopt reasonable procedures to ensure accuracy and confidentiality of consumer credit report).

70. U.S. Dep't of Commerce, *Safe Harbor Privacy Principles—Frequently Asked Questions 8: Access* (July 21, 2000), http://www.ita.doc.gov/td/ecom/FAQ8AccessFINAL.htm.

71. *Id.*

stores the information."[72]

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's report, Stewart Baker noted:

> As 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.[73]

Mandating access under these circumstances creates a risk of liability for companies damned (for privacy infringement) if they require clear and convincing proof of identity before giving access and damned if they do not and are exploited by a con man. While there is 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 that drive business practices in ways that may not benefit consumers.

4. Onward Transfer

While the FTC Privacy Online Report did not separately call out transfer to third parties, the Safe Harbor Principles require that:

> Where an organization wishes to transfer information to a third party that is acting as an agent, . . . 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.[74]

The FTC Privacy Online Report seemed to support limits on third-party transfers, although it failed to acknowledge the Safe Harbor Principles' exception for agents, an exploration that is essential in the era of the "boundary-less corporation" in which

---

72. *Id.*
73. FINAL REPORT—BAKER CONCURRENCE, *supra* note 66.
74. SAFE HARBOR PRINCIPLES, *supra* note 34.

third-party contractors, consultants, and outsourcers are integral parts of most major business operations. At a minimum, any U.S. regulations would need to carve out parties in privity with the data recipient and in compliance with its privacy policies, as described in the Safe Harbor approach. Even with this exception, it would be hard to be a vendor operating under such rules. Imagine United Postal Service workers reviewing and complying with dozens of different customer privacy policies for different deliveries. 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. Permitting information exchange among "affiliates" but not third parties (as under the Gramm-Leach-Bliley financial industry privacy regulations)[75] necessarily handicaps otherwise beneficial exchanges and gives big multinationals, with a wide range of affiliates, an edge over smaller companies who rely on unaffiliated third-party partners.

We have traditionally looked to personal relationships to govern the handling of information, thinking of the baker as a different person than the barber. That small-town imagery is misleading when it comes to most transactions, as we simply do not have those same relationships with the groups of people who comprise modern corporations. Therefore, last year's 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 for generations, was something of a red herring.[76] So long as information is being used within the intended scope of a transaction, the precise identity of those using it should not be critical, although material statements about future uses made to those supplying the information should continue to "run with the land" regardless of future transfers.

B. Regulating the Problem, Not the Possibility

If we should not have sweeping regulations mandating

75. *See* 15 U.S.C. §§ 6801-6810 (Supp. 2000).

76. Press Release, Office of New York State Attorney General, Toysmart Bankruptcy Settlement Ensures Consumer Privacy Protection (Jan. 11, 2001), http://www.oag.state.ny.us/press/2001/jan/jan11a_01.html.

notice, consent, and the like, is there not a feasible form of legal protection against misuse of personal information? In short, Chairman Muris's newly announced policy of strict enforcement of existing laws coupled with watchful waiting regarding the need for supplemental statutes gets it about right.[77]

Expressing skepticism about the need for new laws, Professor Eugene Volokh has powerfully argued that "[t]he 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)."[78] Recognizing that we are legislating in the shadow of the First Amendment suggests a powerful guiding principle for framing privacy regulations. Like any laws encroaching on the freedom of information, privacy regulations must be narrowly tailored and powerfully justified.[79] In other words, legislators should identify a specific and real harm and tailor any responsive laws narrowly. This is a difficult standard to meet when passing sweeping legislation in response to theoretical concerns rather than specific problems.

The privacy regulations enacted and proposed to date have generally met neither test, opening the Pandora's box of difficulties noted above.[80] Under the guise of proactive legislation, many proposed bills are solutions in search of problems, laying out broad-brush lists of principles not tailored to specific issues or industries. The problem is particularly severe for new technologies and for business models that are still maturing.

The first order of business for any regulator is to conclude

---

77. *See* Muris, *supra* note 35.

78. 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, 1051 (2000) (citations omitted); *see also* PRIVACY ONLINE REPORT—SWINDLE DISSENT, *supra* note 3, at 24-25.

79. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1233-34 (10th Cir. 1999), *cert. denied*, 528 U.S. 1188 (2000).

80. Among these problems are the many notices required by the Gramm-Leach-Bliley Act, the burdensome requirements set forth by COPPA that have reduced programming available to kids, and the paperwork burdens created by health care privacy requirements of notice and "opt-in" adopted at the end of 2000.

that markets are failing in their normal role of serving the public good. As FTC Commissioner Swindle has repeatedly observed, evidence of a market failure regarding information exchange is at best unclear.[81] Even if we have a market failure, the issue becomes whether legislation and regulation will do a better job or merely substitute their own failings—what some have called "government failure."[82]

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, without the difficulties of compilation, reproduction, and distribution that historically impeded information transfer.[83] Regulating that flow would certainly reintroduce some of the old-style friction into the equation, but that would be a high price to pay. Rather, the goal should be to remedy specific problems without damaging the infrastructure that creates both the problems and the benefits. As a Brookings Institution conference, discussing the conclusions of Fred Cate's *Privacy in the Information Age*, summarized it: "First, do no harm."[84]

Several regulations adopted to date, to say nothing of the raft of new proposals, flout this rule. Regulations promulgated under the Gramm-Leach-Bliley Act of 1999[85] demonstrate these difficulties. The privacy notice provisions of this Act forced financial institutions to send the typical middle-class American adult between 15 and 25 privacy notices in the years following its adoption.[86] Such notices included so much information (typically packed into leaflets accompanying monthly statements) and were so complex as to be effectively worthless. Importantly, the volume of notices was not made necessary because bankers were using personal information in

81. *See, e.g.*, FTC, ONLINE PROFILING: A REPORT TO CONGRESS—PART 2: RECOMMENDATIONS—DISSENTING STATEMENT OF COMMISSIONER SWINDLE (July 2000), http://www.ftc.gov/os/ 2000/07/onlineprofiling.htm.

82. Solveig Singleton & Jim Harper, *With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us* (Competitive Enterprise Institute Study, June 2001), http://www.cei.org/PDFs/with_a_grain_of_salt.pdf.

83. Esther Dyson, *Foreword* to JENNINGS & FENA, *supra* note 32.

84. CATE, *supra* note 23, at 204. The Brookings Institution conference was held on April 9, 1997.

85. 15 U.S.C. §§ 6801-6810 (Supp. 2000).

86. John Schwartz, *Privacy Policy Notices Are Called Too Common and Too Confusing*, N.Y. TIMES, May 7, 2001, at A1.

inappropriate or duplicitous ways; it was chiefly because providing detailed, accurate, and concise statements about a topic as complex and fast-changing as "information practices" is extraordinarily difficult.

Another example of the burdens of overbroad regulation comes from the Children's Online Privacy Protection Act (COPPA),[87] a motherhood-and-apple-pie effort to protect children from online marketing without their parents' consent. COPPA passed Congress by sweeping margins and has subsequently imposed substantial costs even on websites that do not target children.[88] As a result, many websites were forced to simply eliminate children's programming.[89] The COPPA example shows that the risks of overbroad regulation are real and not mere posturing by business interests. 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 have made too expensive and difficult to provide.

This is not to say that certain privacy problems are neither significant nor worthy of attention. For understandable rhetorical reasons, however, privacy advocates often evoke nightmarish images of the worst that might result from the 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.[90] After all, saying that information was gathered and nothing bad happened is terribly anticlimactic. We should not, however, let scary stories outweigh the real and immediate benefits to society from free information flow or dictate policy responses. The right balance

87. 15 U.S.C. §§ 6501-6505 (Supp. 1999).

88. *See* PRIVACY ONLINE REPORT—SWINDLE DISSENT, *supra* note 3, at 3 n.5; Lynn Burke, *An Ordeal: Copin' with COPPA*, WIRED NEWS (Sept. 20, 2000), *at* http://www.wired.com/news/business/0,1367,38832.00.html (discussing 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 could not afford the costs of COPPA compliance are turning off the interactive features that many children enjoy using).

89. *See* Burke, *Kids' Sites Cite COPPA Woes*, *supra* note 88.

90. *See* JERRY M. ROSENBERG, THE DEATH OF PRIVACY xi (1969); ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 61 (2000).

is usually far more subtle. For example, in writing about the widening use of social security numbers for identification and authentication, the noted communitarian scholar Amitai Etzioni argues:

> [National identification cards] 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. . . . By helping to sustain law and order, universal identifiers may thus play a role in curbing the type of breakdown in social order that can lead to totalitarianism.[91]

Exaggerated fears are particularly common regarding new technologies. Recent public opinion polls suggest that users who have actually bought something online are far less concerned about privacy than those who have only imagined doing so. This suggests that issues that many consider problems may be rooted in widespread technophobia and may decline over time. We have become comfortable with the 50-year-old institution of the credit card and casually give our Visa cards to waiters who disappear for 15 minutes and return with a bill. We have no assurances that the waiter has not surreptitiously copied down the number or made an extra imprint of the card, but familiarity, the feeling that the waiter risks punishment by doing this, and laws against credit card fraud combine to give us a sense of security sufficient to let the transaction proceed. We talk on the telephone, oblivious to the ability of a technician in a central office to eavesdrop, and, by using the United States mail, we entrust our most precious documents—our bank statements, our mortgage records, our love letters—to the security of paper and spit and leave them to the care of a dozen underpaid strangers to carry across the country. It should not work, but it usually does. More importantly, we trust that it will. Yet, in the world of technology we worry a great deal about such transactions.

It seems premature to choke off the evolving business, technological, and social responses to information concerns with the big stick of broad-brush legislation. It is better,

---

91. ETZIONI, *supra* note 1, at 127.

perhaps, to focus on prohibiting misuse and misrepresentation—because disclosure and the subsequent public backlash are in many cases the most effective deterrents—by imposing appropriate sanctions when they occur.

What kinds of misuse create real world problems? Recent examples of more focused measures include federal and state legislation seeking to limit the universally deplored phenomenon of spam while respecting First Amendment limitations. Other laws established specific procedures, liability, and remedies for economic harm resulting from identity theft or other misuse of personal information, which seem an abuse at the heart of many Americans' concerns about privacy.[92] Still other proposals advocated the creation of ombudspersons and clearinghouses to resolve problems resulting from the misuse of information. There is broad agreement in each of these areas on the existence and nature of a problem and a great likelihood that the remedy is not worse than the disease. Such legislation is certainly less exciting than restructuring the Information Revolution by fiat, but the balance of benefits and costs seems far more attractive.

III. CONCLUSION

Like most good things in life, privacy comes at a cost. Restricting information exchange threatens a range of benefits, including many that are indirect and not readily apparent. As Jane Jacobs, in writing about building urban landscapes, and Larry Lessig, in writing about building computer networks, have argued, the architecture of public space matters.[93] Our public policy choices will largely determine whether the architecture of information transfer not only protects privacy but also fosters the organic and multi-faceted development of new individual, collective, and social benefits.

The first step in analyzing the trade-offs involved in enacting new regulations is identifying the benefits of information

92. *See* Supervisory Letter, Richard Spillenkothen, Director, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, Identity Theft and Pretext Calling (Apr. 26, 2001), http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr0111.htm.

93. JANE JACOBS, THE DEATH AND LIFE OF GREAT AMERICAN CITIES (1961); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

exchange and the costs of regulation as well as the benefits of privacy in a particular instance. The likely result is not a broad-brush response but an appreciation of the need for a detailed evaluation of an extraordinarily complex technological and social phenomenon. Sometimes the right public policy answer is to do nothing at all. A premature insistence on regulatory control rather than on market approaches may distort or prevent the evolution of initiatives that produce lower prices, increase convenience, ensure security, and foster accountability and social trust. With those benefits hanging in the balance, individuals, businesses, and regulators should not give privacy an exclusive position at the bargaining table.