Internet Privacy and the State

PAUL M. SCHWARTZ*

INTRODUCTION

> "Of course you are right about Privacy and Public Opinion. All law is a dead letter without public opinion behind it. But law and public opinion interact—and they are both capable of being made."[1]

Millions of people now engage in daily activities on the Internet, and under current technical configurations, this behavior generates finely grained personal data. In the absence of effective limits, legal or otherwise, on the collection and use of personal information on the Internet, a new structure of power over individuals is emerging. This state of affairs has significant implications for democracy in the United States, and, not surprisingly, has stimulated renewed interest in information privacy.[2]

Yet, the ensuing debate about Internet privacy has employed a deeply flawed rhetoric. Most policy discussions in this area are based around one or more of the following sets of alternatives. First, we are asked to consider whether our policies for cyberspace should depend on the market or

---

* *Professor of Law, Brooklyn Law School.* *Research for this Article was made possible by the Dean's Research Fund of Brooklyn Law School. I wish to thank Dean Joan Wexler for this generous support and her enthusiasm for this project. This Article benefitted from the suggestions of Robert Gellman, Ted Janger, Joel R. Reidenberg, Laura J. Schwartz, Spiros Simitis, Peter Spiro, William M. Treanor, Spencer W. Waller, Benjamin H. Warnke, and David Yassky. Barry Reichman helped me develop the graphic material. I am thankful to these colleagues and friends for their assistance as I am to those scholars who have improved my thought by commentary on this Article: Anita L. Allen, Fred H. Cate, Amitai Etzioni, Michael J. Gerhardt, and Lance Liebman. Most of all, Stefanie Schwartz provided essential inspiration.*

1. Louis D. Brandeis, Letter of December 28, 1890, *in* 1 LETTERS OF LOUIS D. BRANDEIS 97 (Melvin I. Urofsky & David W. Levy eds., 1971).

2. For a selection of scholarly works, see FRED H. CATE, PRIVACY IN THE INFORMATION AGE 50-51 (1997); AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE at vii (1998); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) [hereinafter Schwartz, *Privacy in Cyberspace*].

the State. Second, we are invited to decide whether these policies should favor "bottom-up" or "top-down" regulation. At certain times, only one set of these alternatives is put forth; at other moments, both are presented. Occasionally, as part of this debate, a third policy set is produced—whether industry self-regulation is more desirable than a formal legal response by the State.[3]

Discussion of the first set of alternatives leads to a contrast between the market's invisible hand and the State's heavy hand. Consideration of the second set of alternatives encourages a comparison between self-rule by cyber-citizens shaping a new democratic realm and the unresponsiveness of bureaucrats. As for self-regulation, it can be used to oppose proposals based on the State or top-down regulation. Most typically, however, self-regulation is presented as an improvement on the inflexibility of formal legal mandates. Somewhat mysteriously, the relation of self-regulation to the market or to bottom-up regulation is usually passed over in silence.

Beyond Internet privacy, the same or similar rhetorical moves are often made in the more general debate about Internet governance.[4] Faced with these choices, only someone with nostalgia for Soviet-style central planning would disagree with the conventional wisdom that we should favor the market, bottom-up decision-making, and self-regulation in cyberspace. From this perspective, the role of the State, if not nonexistent, is to be as constrained as possible.

In this Article, I argue that the rhetoric of the debate about Internet privacy sets up the wrong alternatives and encourages the wrong conclusions. In particular, this rhetoric slights the State's important role in shaping both a privacy market and privacy norms for personal information in cyberspace. My argument unfolds in three parts. First, I identify the flaws in the leading paradigm of information privacy, which conceives of privacy as a personal right to control the use of one's data. I term this paradigm "privacy-control" and devote this Article's Part I to a critique of it.

Second, I turn to the development of a substantive concept of information privacy. This task is inescapable; the merits of different regulatory regimes are only understandable in reference to a sought after outcome. In Part II, I seek to characterize information privacy as a constitutive value that helps both to form the society in which we live in and to shape our individual identities.

After developing this theory of constitutive privacy, I turn in Part III to possible tools for structuring the necessary kind of privacy rules. Here, I argue that the State has a special role in two areas: (1) creating and main-

3. The structure of this debate can also be presented graphically, and I have done so in Table A, Part III.A, *infra* p. 844.

4. For an initial example, see Jason L. Riley, *Bookmarks*, WALL ST. J., Oct. 1, 1999, at W6 (reviewing TIM BERNERS-LEE, WEAVING THE WEB (1999)).

taining conditions for a functioning privacy market, and (2) developing privacy norms that prevent access to personal information that would cause too great a rate of preference falsification in society. The second point seeks to correct norm theorists who view privacy generally as an obstacle to norm formation.[5] In my view, however, limits on the sharing of personal data are necessary to protect private knowledge and private preferences and, thereby, to prevent norm entrepreneurs from being excessively meddlesome, that is, zealously expanding out the areas regulated by norms or inducing excessive levels of compliance with norms.[6]

In 1890, immediately after publication of his masterpiece, *The Right of Privacy*, Louis Brandeis considered, in a letter to his future wife, the ties between privacy, law, and public opinion.[7] Although he conceded that law depended on the public's support, Brandeis argued that law and public opinion "are both capable of being made."[8] Brandeis wrote *The Right of Privacy* to change law and alter public opinion. This Article's far more modest goal is to promote a view of law and social norms not as adversaries, but as interrelated concepts, both of which are open to modification.[9] Indeed, the State, as part of its development of privacy standards for the Internet, is not a force that invariably opposes the market or social norms, but is capable of playing an important and positive role in helping to form both.

---

5. *See, e.g.*, ROBERT C. ELLICKSON, ORDER WITHOUT LAW 285 (1991) (noting how legal rules can "affect how easy it is for people to obtain the information they need to engage in informal social control" and calling for "improved circulation of accurate reputational information); Richard A. Posner, *Privacy*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 103, 105 (Peter Newman ed., 1998) [hereinafter PALGRAVE DICTIONARY OF ECONOMICS & LAW] [hereinafter R. Posner, *Privacy*] ("Legal protection of the right to conceal discrediting information is problematic for the further reason that it undermines social control by means of norms, an important substitute for legal control of behaviour.").

6. Regarding meddlesomeness, see generally TIMUR KURAN, PRIVATE TRUTHS, PUBLIC LIES: THE SOCIAL CONSEQUENCES OF PREFERENCE FALSIFICATION 23-24 (1995). On the problem of excessive levels of compliance with norms, see Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 419-24 (1997). The issue of levels of compliance is present in Cass Sunstein's unforgettable discussion of rich and happy people in East Hampton driving in their expensive cars in August to the recycling center, formerly known as the East Hampton Dump, to take "a long time" to separate their garbage. Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 906 (1996).

7. *See* Brandeis, *supra* note 1, at 97. For the classic article, see Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

8. Brandeis, *supra* note 1, at 97.

9. As Kaushik Basu writes:

> [T]he state may be viewed as one of the many different instruments through which individuals create order among themselves. Instead of thinking of the law and social norms as alternative systems, or worse, as adversaries, it is possible to treat the legal system as part of the general theory of norms.

Kaushik Basu, *Social Norms and the Law*, *in* PALGRAVE DICTIONARY OF ECONOMICS & LAW, *supra* note 5, at 480.

I. THE FLAWS OF PRIVACY-CONTROL

By generating comprehensive records of online behavior, information technology can broadcast an individual's secrets in ways that she can no longer anticipate—let alone control. Moreover, information technology on the Internet affects privacy in ways that are different from anything previously possible.

Consider these examples:

- An individual's activities in cyberspace create records within her own computer as well as on networked computers. For example, the Office of the Independent Counsel gained access to numerous deleted e-mails of Monica Lewinsky's and published these documents in the "Starr Report."[10] The investigators recovered some of these documents from Lewinsky's computer and others from the recipient's computer—a friend in Japan to whom Lewinsky had sent the messages.[11]

- The private sector currently captures and makes commercial use of personal information on the Internet.[12] Web sites and direct marketers are increasingly linking cyber-data collections to personal information collected in the offline world.[13] These entities are both selling individual profiles and developing marketing lists that are sorted according to dimensions such as political affiliations, medical conditions, body weight, ethnic groups, or religious beliefs. Few legal restrictions exist on the collection and sale of personal data by Web sites or cyber-data

10. As an example of the use of the e-mails by the Office of the Independent Counsel (OIC), it cited to them to show Ms. Lewinsky's "emotional attachment" to President Clinton. *See* OFFICE OF THE INDEPENDENT COUNSEL, THE STARR REPORT: THE FINDINGS OF INDEPENDENT COUNSEL KENNETH W. STARR ON PRESIDENT CLINTON AND THE LEWINSKY AFFAIR 40 n.45 (1998). The text of the e-mails themselves were included in the OIC's referral to the House of Representatives and are printed at THE STARR REPORT: THE EVIDENCE 437-59 (Phil Kuntz ed., 1998) [hereinafter STARR REPORT EVIDENCE].

11. *See* STARR REPORT EVIDENCE, *supra* note 10, at 437-59.

12. In recognition of this issue, the Department of Commerce and Federal Trade Commission held public workshops on one of its aspects, the profiling of visitors by Web sites. *See* Department of Commerce, Federal Trade Commission, *Public Workshop on Online Profiling* (visited Nov. 8, 1999) <http://www.ftc.gov/os/1999/9909/FRN990915.htm>. For media coverage, see *FTC Tackles Online Profiling*, WIRED.COM (visited March 1, 1999) <http://www.wired.com/news/reuters/0,1349,32415,00.html>.

13. *See, e.g.*, Ted Kemp, *Behind the DoubleClick Merger: Buying behavior is Abacus' key asset*, DMNEWS, June 21, 1999, at 1, *available in* LEXIS, News Library, DM News File (analyzing purchase by leading marketer of online advertisements of "a firm that manages the largest catalog of consumer catalog buying habits in the United States").

marketers.[14] As a recent development concerning commercialization of personal information collected on the Internet, DoubleClick, a leading online advertising company, reversed its previously stated position and temporarily cancelled its plans to link its databases of personal information with those of Abacus, an offline direct marketer which it had purchased in 1999.[15] While numerous private lawsuits have been filed against DoubleClick, which is also being investigated at present by the Federal Trade Commission and Attorneys General of Michigan and New York, the pertinent law and the extent of any legal restrictions on its behavior are murky.[16]

- The technology that allows Web snooping tends to be introduced with little fanfare or independent scrutiny. Controversy sometimes erupts, but generally leads to only partial modification of the technology—one that does not fully prevent a future deleterious effect on privacy. Thus, at best, there has been only a partial resolution of such issues as Intel Pentium III's assignment of a permanent ID (the "Processor Serial Number") to individual computers[17] and Microsoft Word's creation of Globally Unique ID's (GUIDS) for individual documents, including information about the Ethernet addresses of the person saving the document.[18] Privacy experts have also protested so-called "Web bugs," also known as "clear GIF," which allow Internet advertising services to gather data from multiple Web sites without computer users' knowledge.[19]

---

14. *See* Kang, *supra* note 2, at 1230; Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1626-37; Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 115 (1995).

15. *See* Chris Oakes, *DoubleClick Plan Falls Short*, WIRED.COM (Feb. 14, 2000) <http://www.wired.com/news/business/0,1367,34337,00.html>. In the words of Michigan's Attorney General, "DoubleClick's privacy policy is a moving target, and consumers should be extremely cautious about relying on the company's vague promises." Grant Lukenbill & Ken Magill, *Michigan Latest to Open Fire on DoubleClick*, DMNEWS, Feb. 18, 2000, at 1, *available in* <http://www.dmnews.com/articles/2000-02014/6549.html>.

16. *See* Richard B. Schmitt, *Online Privacy: Alleged Abuses Shape New Law*, WALL ST. J., Feb. 29, 2000, at B1.

17. *See* Big Brother Inside, *Protect Your PC's Privacy* (visited Mar. 1, 2000) <http://www.bigbrotherinside.com>; Center for Democracy and Technology, *Privacy Advocates Letter on Pentium III* (Jan. 28, 1999) <http://www.cdt.org/privacy/intel.letter.shtml>.

18. On the Microsoft GUID, see Richard M. Smith, *Fingerprinting of Office 97 Files* (visited Mar. 1, 2000) <http://www.tiac.net/users/smiths/privacy/office97.htm>; Richard M. Smith, *Windows 98 Knows Who You Are*, BYTE.COM (March 12, 1999) <http://www.byte.com/features/1999/03/win98priv.html>.

19. Richard M. Smith, a computer consultant, first labeled this technology "the Web bug" and brought public attention to its privacy-robbing features. *See* Richard M. Smith, *The Web Bug FAQ* 1 (Nov. 11, 1999) <http://www.tiac.net/users/smiths/privacy/wbfaq.htm>. The Web bugs allow infor-

Here, then, are just a few of the critical areas of information use and processing in cyberspace: (1) the storage of personal data on networked computers, including one's own P.C.; (2) the collection and marketing of personal data by Web sites and direct marketers; and (3) the introduction of new snooping software and technology. Moreover, the Internet's underlying technical architecture, which causes individuals on it to simultaneously collect and transmit information, also promotes the collection of personal data.[20] Regardless of the area of data use, however, the same question arises concerning the underlying purpose of information privacy. What are the ends to be sought in shaping the use of personal information?

A conventional answer exists with respect to the proper kind of *means*, namely, the preference of solutions around the market, bottom-up, and self-regulation. Agreement also exists about the *ends* that information privacy should seek. The leading paradigm on the Internet and in the real, or offline world, conceives of privacy as a personal right to control the use of one's data. I refer to this idea as "privacy-control." This liberal autonomy principle seeks to place the individual at the center of decision-making about personal information use. Privacy-control seeks to achieve informational self-determination through individual stewardship of personal data, and by keeping information isolated from access. Privacy-control also encourages a property approach to personal information that transforms data into a commodity. Finally, the privacy-control paradigm supports a move to an intellectual property regime for privacy. This regime would center itself around a view of personal information as a resource to be assigned either to the person to whom it refers, or to a marketing company or other commercial entity.[21]

The weight of the consensus about the centrality of privacy-control is staggering. Initially, however, I wish to point to only a few examples. First, an example from the offline world: the Supreme Court, in a leading Freedom of Information case, declared, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[22] Second, the Clinton Administration drew squarely on this paradigm by defining privacy as "an individ-

---

mation to be gathered even from pages displaying no ads and are typically only 1-by-1 pixel in size. *See id*. at 3; *see also* Robert O'Harrow, Jr., *Fearing a Plague of 'Web Bugs'; Invisible Fact-Gathering Code Raises Privacy Concerns*, WASH. POST, Nov. 13, 1999, at E01.

20. *See* Kang, *supra* note 2, at 1246; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) [hereinafter Lessig, *Law of the Horse*]; Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 780 (1999), *available in* <http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/htjl/note.html> [hereinafter Reidenberg, *Restoring Privacy*].

21. *See generally* William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203, 1213 (1998); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. (forthcoming 2000), *available in* <http://www.sims.berkeley.edu/~pam/papers/privasip_draft.doc>.

22. United States Dep't of Justice v. Reporter's Comm., 489 U.S. 749, 763 (1988).

ual's claim to control the terms under which personal information . . . is acquired, disclosed, and used."[23] Similar examples can be found in the scholarship of Charles Fried, Richard Posner, Frederick Schauer, Alan Westin, and others.[24]

Despite this agreement, privacy-control has proved a deeply flawed principle. The three significant problems with this idea can be termed: (1) the autonomy trap; (2) the data seclusion deception; and (3) the commodification illusion.

A. *The Autonomy Trap*

As developed in caselaw, policy proposals, and scholarship, the concept of individual control of personal data rests on a view of self-determination as a given, pre-existing quality. As Fred Cate expresses this notion, for example, data privacy must be constructed around "the primacy of individual responsibility and nongovernmental action."[25] As a policy cornerstone, however, privacy-control falls into the "autonomy trap." By this term, I wish to refer to a cluster of related consequences flowing from the reliance on the paradigm of control of personal data in cyberspace: (1) the strong limitations existing on informational self-determination as it is construed at present; (2) the fashion in which individual autonomy itself is shaped by the processing of personal data; and (3) the extent to which the State and private entities remove certain uses or certain types of personal data entirely from the domain of two-party negotiations.

1. *Limitations on Informational Self-Determination*

Despite the belief that cyberspace is a "friction free" medium, pervasive restrictions exist in it regarding freedom of choice regarding information privacy. Yet, for self-reliant consent to fulfill its assigned role for

---

23. U.S. DEPARTMENT OF COMMERCE, NATIONAL TELECOMMUICATIONS AND THE INFORMATION ADMINISTRATION, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION 2-3 (1995).

24. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining information privacy as the claim of "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."); Ken Gormley, *One Hundred Years of Privacy*, 1992 WISC. L. REV. 1335, 1356 ("[C]ontrol of information about oneself is critical in determining how and when (if ever) others will perceive us, which is in turn essential to managing our individual personalities."); R. Posner, *Privacy*, *supra* note 5, at 104 ("Economic analysis of the law of privacy . . . should focus on those aspects of privacy law that are concerned with the control by individuals of the dissemination of information about themselves."); Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 556 (1998) ("The privacy interest I address here is the power to control the facts about one's life.").

25. CATE, *supra* note 2, at 30. He adds, "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." *Id*.

shaping privacy, individuals must be able to choose between different possibilities—and significant reasons exist for doubt on this score. First, widespread information asymmetries exist regarding personal data processing and, as a result, most visitors to Web sites lack essential knowledge. These asymmetries are promoted by the obscurity of privacy notices and the highly technical nature of the issues that affect privacy in cyberspace.[26] In Neil Netanel's trenchant criticism, "most users are not even aware that the web sites they visit collect user information, and even if they are cognizant of that possibility, they have little conception of how personal data might be processed."[27]

Moreover, a collective action problem exists regarding privacy on the Internet.[28] A critical mass of sophisticated privacy consumers is not yet emerging. Even if isolated groups of such consumers were to exist, others would have trouble locating them and drawing on their superior knowledge under current conditions.[29] The rest of us cannot free-ride on the efforts of those who are more savvy about data privacy on the Internet. As I discuss in Part III.B., elements of a market solution to this shortcoming are beginning to emerge. Possibilities for collective action are emerging around Trusted Third Parties, also called "infomediaries," as well as new filtering technology that allows expression of privacy preferences, including one's adoption of pre-set filters that reflect the suggestions of privacy advocates. The question remains, however, as to whether sufficient use of these mechanisms will be made by privacy first-movers to overcome the collective action problem. At present, a bad privacy equilibrium remains set in place.

Beyond information asymmetries and the collective action problem, another limitation on the choice-making of individuals in cyberspace concerns bounded rationality.[30] In particular, when faced with standardized

26. As James Glave, a reporter for wired.com, has written, "[t]he vast majority of the Internet-viewing public still has no idea how to judiciously use their personal information, or even why they should." James Glave, *Wired News Privacy Report Card*: *Consumers Must Be Educated. Grade: C.*, WIRED.COM 2 (visited Dec. 22, 1998) <http://www.wired.com/news/print_version/politics/story/16963.html?wnpg=all>. The lack of knowledge of processing practices is, moreover, a systematic consequence of the social and institutional structure of personal data use. For an analysis, see Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 532-34 (1995); Schwartz, *Privacy in Cyberspace*, *supra* note 2.

27. Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. (forthcoming 2000) (manuscript on file with author).

28. For a general discussion of collective action problems, see CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 59-61 (1997).

29. Part of the difficulty is that groups on the Internet often lack the stability necessary for ongoing collective action. For discussion of this issue, see Netanel, *supra* note 27. *See generally* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 50-51 (1997) [hereinafter Schwartz, *Personal Health Care Economics*] (discussing collective action problems for privacy in the health care setting).

30. For a concise introduction, see David M. Kreps, *Bounded Rationality*, *in* PALGRAVE DICTIONARY OF ECONOMICS & LAW, *supra* note 5, at 168-69.

terms, individuals left by privacy-control to fend for themselves will frequently accept whatever industry offers them. As scholarship in behavioral economics has demonstrated, consumers' general inertia toward default terms is a strong and pervasive limitation on free choice.[31]

Consent also implies the possibility of refusal. If "voice", i.e. protest and other forms of complaint, does not lead to change, "exit" should be possible. Yet, industry standard setting largely disfavors privacy at present. Internet companies generally benefit from developing standards, including new software, that preserve the current status quo of maximum information disclosure.[32] Once online industry is able to "lock-in" a poor level of privacy on the Web as the dominant practice, individuals may not have effective recourse to other practices. They can protest, but collective action problems on the Internet, as I have suggested above, are widespread. Moreover, there is nowhere else to go—except to leave cyberspace.

I wish to conclude my analysis of this aspect of the autonomy trap, the limitations on informational self-determination, with an example of this process in action. The recently released *Georgetown Internet Privacy Policy Survey*, sponsored by the Federal Trade Commission (FTC), illustrates the results of ignoring constraints that exist on choices for privacy in cyberspace.[33] As background to my discussion of this survey, I wish to note that online industry's campaign for self-regulation of privacy has emphasized the value of posting "Privacy Notices."[34] This practice involves a Web site's home page featuring a hypertext link to a document that spells out how it collects and uses personal information. Provision of access to these notices is considered by industry to form the basis for self-reliant choice by those who visit these sites.

Not surprisingly, in light of industry's promotion of this practice, the Georgetown Survey found that Web sites with the most passenger traffic

---

31. *See* Russell Korobkin, *The Efficiency of Managed Care "Patient Protection" Laws*, 85 CORNELL L. REV. 148, 148-59 (1999); Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583, 1587-92 (1998).

32. I have developed this argument at greater length in Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1687-96.

33. *See* FTC, *Self-Regulation and Privacy Online: A Report to Congress* (July 1999) <http://www.ftc.gov/os/1999/9907/privacy99.pdf> [hereinafter FTC SELF-REGULATION REPORT]; GEORGETOWN INTERNET PRIVACY POLICY SURVEY: REPORT TO THE FEDERAL TRADE COMMISSION (June 1999) <http://www.msb.edu/faculty/culnan/gippshome.html> [hereinafter GEORGETOWN SURVEY].

34. For example, the Online Privacy Alliance has emphasized the value of posting a privacy statement as a strategy of preventing governmental regulation. It advises Internet companies, "[g]overnment officials will be judging how successful self-regulation may be by how many companies have posted privacy policies on their web sites and how many have joined the Alliance and adopted its guidelines." Online Privacy Alliance, *Frequently Asked Questions* 2 (visited Feb. 4, 2000) <http://www.privacyalliance.com/facts/>.

were increasingly offering click-on "Privacy Notices."[35] Moreover, the FTC and much of the media accepted this development as simple proof of the success of self-regulation.[36] In the words of Robert Pitofsky, the FTC's Chairman, this development indicated "real progress" and an indication that "self-regulation is working."[37]

Yet, many reasons exist *not* to share in this optimism. Even on their own terms, these documents are often flawed. Privacy policies frequently fail to reveal the substantive nature of the site's actual practices and may never be read, let alone understood, by the majority of those who visit the site. Web sites also frequently reserve the right to change their privacy policies. Finally, the concept of notice is increasingly accepted not merely as an *element* of consent in cyberspace, but as the full basis for it.

In light of these flaws, the true argument in favor of the Privacy Policy can only be as follows: when a Web site says something about its data processing practices—even if this statement is vague or reveals poor practice—the visitor to the site is deemed to be in agreement with these practices so long as she sticks around. This summary, despite its ironic tone, is no exaggeration. Its accuracy is indicated, for example, by the Georgetown Internet Privacy Policy Survey which counts any kind of disclosure of information practices as notice. Thus, a site that said "[w]e reserve the right to do whatever we want with the information we collect" was deemed to have provided notice of information practices.[38]

---

35. *See* FTC SELF-REGULATION REPORT, *supra* note 33, at 7; GEORGETOWN SURVEY, *supra* note 33, at 8.

36. *See* FTC SELF-REGULATION REPORT, *supra* note 33, at 1. For media reports, see Jeri Clausing, *Gain for On-Line Industry on Privacy Issue*, N.Y. TIMES, July 13, 1999, at A10; Jeri Clausing, *Gains Seen in Consumer Privacy on Internet*, N.Y. TIMES, May 13, 1999, at A20; Grant Lukenbill, *Privacy Laws Inappropriate at This Time, FTC Tells Congress*, DMNEWS, July 19, 1999, at 1, *available in* LEXIS, News Library, DM News File.

37. FTC, *Self-Regulation and Privacy Online, FTC Report to Congress* ¶ 3 (July 13, 1999) <http://www.ftc.gov/opa/1999/9907/report1999.htm> [hereinafter FTC Press Release]. A similar conclusion is found in the FTC's report to Congress. *See* FTC SELF-REGULATION REPORT, *supra* note 33, at 8. The FTC itself argued that "self-regulation is the least intrusive and most efficient means to ensure fair information practices online." FTC Press Release, *supra* ¶ 4 (quoting FTC SELF REGULATION REPORT, *supra* note 33).

In contrast, FTC Commissioner Sheila Anthony declared that "[n]otice, while an essential first step, is not enough if the privacy practices themselves are toothless." Statement of Commissioner Sheila F. Anthony, concurring in part and dissenting in part, *Prepared Statement of the Federal Trade Comm'n on "Self-Regulation and Privacy Online," Before the Subcomm. on Telecomms., Trade, and Consumer Protection of the Comm. on Commerce, U.S. House of Representatives* 1 (July 13, 1999) <http://www.ftc.gov/os/1999/9907/pt071399anthony.htm>. At present, her judgment is decidedly in the minority on the FTC. *See id*.

38. GEORGETOWN SURVEY, *supra* note 33, at 9.

A number of other reasons exist as to why we should refrain from rejoicing about the Georgetown Survey's results. To begin with, the study indicates that a high percentage of Web sites collect personal information. *See id*. at 10.

Second, the FTC's focus on notice slights other fair information practices, which are the building blocks of modern information privacy law. For example, fair information practices typically re-

In this fashion, privacy-consent neglects the actual conditions of choice regarding the processing of personal information, and permits notice to become an alibi for "take-it-or-leave-it" data processing. Notice is emerging as the cornerstone for a legal fiction of *implied consent* on the Internet. A given course of conduct is said to signal acquiescence and, therefore, implied consent. Such acquiescence is considered to exist because one has surfed beyond the home page of a Web site with a link to a privacy policy. The autonomy trap seizes on the idea of such "notice" to create a legal fiction of consent.

2. *Constrained Informational Self-Determination Through Data Processing*

The second aspect of the autonomy trap is that it leads to a reduced sense of the possible. The meaning that we attribute to individual autonomy is itself strongly shaped by the existing means by which personal data are processed. In this fashion, a dominant trend in personal data use in cyberspace can be changed from our "is" to our "ought." As Jerry L. Mashaw notes in his critique of unadorned public choice theory, "repeated exposure to representations or ideas lead to a process of habituations or accumulation that is as subtle as it is profound."[39] In cyberspace, we are repeatedly exposed to the concept that if self-regulation leads to notice, a good level of privacy must exist in cyberspace. In time, a decision to go online and surf the Web may itself be considered a decision to accept all use anywhere of one's personal data that this activity generates.[40]

---

quire the creation of access and enforcement interests for those whose information are processed, as well as the setting of limits on so-called "secondary uses" of personal data. The Georgetown Survey indicates, however, that less than ten percent of surveyed sites offer even a subset of fair information practices in addition to notice. *See* GEORGETOWN SURVEY, *supra* note 33, at 10. The Survey refers to this finding in confusing terms as the percentage of the Web sites that "contained at least one survey element for notice, choice, access, security and contact information." *Id*.

Third, this Survey failed to examine whether Web sites offered access and enforcement policies, and whether Web sites are allowing individuals to limit release of their personal data to affiliated enterprises. *See id*. at 14. This last issue is of particular significance at a time when mergers and consolidations are almost daily events among communication companies. *See, e.g.*, Kemp, *supra* note 13, ¶ 1 (analyzing purchase by leading marketer of online advertisements of "a firm that manages the largest catalog of consumer catalog buying habits in the United States").

Finally, as the Center for Democracy and Technology notes, this study, like others of its ilk, provides no information about whether companies actually follow the privacy policies that they propose. *See* Center for Democracy & Technology, *Behind the Numbers: Privacy Problems on the Web*, § B, 9-11 (July 27, 1999) <http://www.cdt.org/privacy/990727privacy.shtml>. For general criticisms of notice-consent in the context of Internet privacy, see Reidenberg, *Restoring Privacy*, *supra* note 20, at 779-80.

39. JERRY MASHAW, GREED, CHAOS, AND GOVERNANCE 3 (1997).

40. The author of an op-ed column in the *Wall Street Journal* demonstrated such reasoning: "Each time they visit a site, Web users control what information they relinquish and how it is used. To begin with, users do not have to use Web sites in the first place." Justin Matlick, *Don't Restrain Trade in Information*, WALL ST. J., Dec. 2, 1998, at A22. Matlick adds, "[n]ew privacy regulations would be at

In real space, the use of informed consent forms for data processing in health care provides an example of the phenomenon by which privacy is first defined down, and then an existing practice becomes an acceptable standard.[41] A parallel can be drawn between this practice and a similar trend in cyberspace. An information disclosure form is now a standard part of visits to physicians' offices and hospitals, and signing one is a sine qua non for receiving medical treatment.[42] The idea that this process in the health care context represents valid consent is troubling, however, on a number of grounds.

First, the information release form is presented at the time when one is least likely to risk not receiving health care services. In the worst cases, hospitals and physicians present this form to individuals suffering from medical emergencies or great pain.[43] Under these circumstances, the duress regarding the form is explicit; at other times, though hidden, it is nevertheless present. Moreover, information disclosure forms are generally worded in vague terms that justify any future use of the disclosing party's personal medical data. As an empirical study of this process concludes, "[p]atients likely do not know the rules of the game, and health providers who do know are not making an effort to inform them."[44]

Health care information forms do not *inform* for consent; instead, they help to create a process of *uninformed, coerced agreement* to all future data use. The parallel with the "Privacy Notice" on the Internet is clear. While few individuals are in pain while surfing the Web, the same element of

---

best redundant. At worst, they would raise the start-up costs of Web-based businesses . . . that don't need privacy policies." *Id*.

A further example of this acceptance of a defined-down view of privacy was demonstrated by Esther Dyson. A leading guru of information technology and Acting Chairperson of the Internet Corporation for Assigned Names and Numbers (ICANN), she has observed, "[i]t's inevitable that people will simply become more comfortable with the fact that more information is known about them on the Net." ESTHER DYSON, RELEASE 2.0: A DESIGN FOR LIVING IN THE DIGITAL AGE 216-17 (1997). Dyson notes with some hope, "we may all become more tolerant if everyone's flaws are more visible." *Id.* at 217.

41. It also indicates the ultimate flaw in the autonomy trap: privacy-control taken alone is an inadequate means in the Information Age for structuring complex systems of personal data use. I will discuss this issue in Part I.C., *infra* p. 830.

42. *See* Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy and Health Care Reform*, HASTINGS CENTER REP., Nov.-Dec. 1993, at 13, 15; Jon F. Merz et al., *Hospital Consent for Disclosures of Medical Records*, 26 J.L. MED. & ETHICS 241 (1998); Schwartz, *Personal Health Care Economics*, *supra* note 29, at 49.

43. As the National Committee on Vital and Health Statistics observed in a report on health privacy to the Secretary of Health and Human Services, many observers "are troubled by the collection of authorizations from patients in pain who are seeking care or who do not have a realistic opportunity or the knowledge or skills to negotiate disclosure rules with providers or employers." National Committee on Vital and Health Statistics, *Health Privacy and Confidentiality Recommendations* 8, § D, ¶ 5 (June 25, 1997) <http://aspe.os.dhhs.gov/ncvhs/privrecs.htm>.

44. Merz et al., *supra* note 42, at 246; *see also* Robert Gellman, *Personal, Legislative, and Technical Privacy Choices: The Case of Health Privacy Reform in the United States* 129, 132-36, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE (Colin J. Bennett & Rebecca Grant eds., 1999).

take-it-or-leave-it consent to personal data processing found in the health care environment is also present in cyberspace. Since it is difficult to identify Web sites with good privacy policies as opposed to those with bad ones, the clearest privacy choice is between staying off the Internet or surrendering one's privacy by going on it. In fact, at present, a general right to access one's personal information exists neither in the health care context nor in cyberspace.

The Clinton Administration's recently announced health care regulations seek to change this baseline for medical data.[45] In addition, as I will discuss in this Article's Part III.B, Congress has mandated access to data for parents who wish to see personal information gathered in cyberspace about their children at commercial Web sites oriented towards children.[46] No such plan exists, however, to require similar access generally in cyberspace. Such restricted choice is not inevitable, however, and I will argue below that the State should seek to stimulate a privacy market so greater possibilities will emerge.

3. *Mandatory Requirements for Use of Personal Data*

The final point regarding the autonomy trap concerns the extent to which the State and private entities remove certain kinds of personal data use entirely from the domain of two-party negotiations. Such immutable restrictions on privacy-control are now present in cyberspace and real space alike. For example, whether or not patients agree, a complex web of statutes and contracts already requires that personal medical information be shared for public health purposes, third party payment, fraud investigation, and other reasons.[47] On the Internet as well, existing law, such as the Electronic Communications Privacy Act (ECPA), removes some disclosures from the realm of private negotiations.[48] ECPA requires, for example, that "[a] provider of electronic communication service," including ISPs, release personal information pertaining to their customers when a court order so requires.[49]

Properly managed, notice and consent have a role within a framework of fair information practices. Yet, notice and consent alone are insufficient

---

45. *See* Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (1999).

46. *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (codified as amended at 15 U.S.C. §§ 6501-6506 (Supp. IV 1998)); *see also* Part III.B, *infra* p. 852.

47. For a useful chart and discussion of uses and flows of personal health information, see NATIONAL RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 65-78 (1997) [hereinafter NRC, FOR THE RECORD]. For an analysis of social use of this data as representing a limitation on two-party negotiations, see Schwartz, *Personal Health Care Economics*, *supra* note 29, at 57-59.

48. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2709, 3121-3126 (1994 & Supp. IV 1998)).

49. *Id.* § 2703(c)(1)(B).

to structure the flow of personal information in either the health care setting or on the Internet. In both settings, the autonomy trap forms a smoke screen that disguises information processing practices and leads to choices that are bad for individuals and for society.

B. *The Data Seclusion Deception*

Like the autonomy trap, the data seclusion deception occurs in both online and offline contexts. This aspect of privacy-control views information privacy as an interest in keeping data isolated. The data seclusion deception conceives of privacy as a trump that keeps information confidential. Yet, privacy-control which rests on information seclusion is quickly swept aside because of two collective demands that weigh against it. First, *public accountability* often requires outside access to personal information as part of democratic governance. Second, *bureaucratic rationality* often demands outside access to allow administrative structures to function.

For examples of public accountability and bureaucratic rationality, we need look no further than the Supreme Court's decision in *Whalen v. Roe*[50] and the lower court decisions that follow it.[51] *Whalen v. Roe* concerned a New York statute that created a centralized state computer listing of names and addresses of all persons who obtained certain drugs pursuant to a physician's prescription. In response, the Supreme Court identified a constitutional right of information privacy grounded in substantive due process. It was divided into two branches: one concerning nondisclosure of personal information; and the other concerning "independence in decision-making."[52] In the more than two decades since the *Whalen* Court first articulated the right of information privacy, this decision's legacy has been at best mixed.

1. *Public Accountability*

As concerns public accountability, *Whalen*'s nondisclosure interest sounds in privacy-control, but the degree of personal information removed from collective decisions under it has not been great. For example, in a leading case following *Whalen*, the Sixth Circuit in *Kallstrom v. City of Columbus*,[53] while finding a violation of the nondisclosure interest, set the bar so high as to isolate only a limited variety of personal data.[54] In *Kallstrom*, the City of Columbus was poised to release information from the

50. 429 U.S. 589 (1977).

51. For an introduction to this case and lower court decisions under it, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 76-88 (1996) [hereinafter SCHWARTZ & REIDENBERG, DATA PRIVACY]; PAUL M. SCHWARTZ & JOEL R. REIDENBERG, 1998 SUPPLEMENT 7-14 (1998) [hereinafter SCHWARTZ & REIDENBERG, 1998 SUPPLEMENT].

52. *Whalen*, 429 U.S. at 599-600.

53. 136 F.3d 1055 (6th Cir. 1988).

54. *See id*. at 1067.

personnel files of undercover police officers under Ohio's Freedom of Information Act. Using *Whalen*, the Sixth Circuit placed some limits on this disclosure because it would "create a serious risk to the personal safety of the plaintiffs and those relatives named in the files."[55] This danger was present in this case because the data was sought by a criminal organization with a "propensity for violence and intimidation."[56]

Kallstrom indicates the strength of the value of public accountability. Only the threat of life-threatening harm to officers and their families and the City of Columbus' plan for automatic disclosure of this information allowed the triumph of a restricted nondisclosure interest. Moreover, the Sixth Circuit granted merely a limited injunction to the undercover officers that allowed them a chance to object when someone requested their personal data.[57] In other words, the *Kallstrom* court left the door open for release of this information under other circumstances.[58] This modest conception of the non-disclosure interest removes most personal data in the government's control from the protection of the constitutional right of information privacy.

2. *Bureaucratic Rationality*

Whalen v. Roe and its progeny also demonstrate how a belief in bureaucratic rationality limits the paradigm of data seclusion. Our interest here shifts to the second *Whalen* interest, which concerns independence in decision-making. The *Whalen* right in independent decision-making ideally seeks to extend constitutional safeguards to personal information to prevent a chilling effect on choice.[59] As the *Whalen* Court observed of the State of New York's data collection scheme, "some patients [were] reluctant to use, and some doctors reluctant to prescribe," drugs that were medically indicated because of a fear that information would become "publicly known" and "adversely affect" their reputation.[60]

At the same time that the *Whalen* court noted this threat, it sealed the fate of the interest in independent decision-making. Despite the evidence of coercion through data gathering, the Supreme Court found that New

55. *Id*. at 1063.

56. *Id*.

57. *See id*. at 1067-70.

58. As the *Kallstrom* court states:

> [T]he constitutional violation arises when the release of private information about the officers places their personal security, and that of their families, at substantial risk without narrowly serving a compelling state interest. Thus, the officers are entitled to notice and an opportunity to be heard prior to the release of private information contained in their personnel files only where the disclosure of the requested information could potentially threaten the officers' and their families' personal security.

Id. at 1069.

59. For an elaboration of this point, see Paul M. Schwartz, *Privacy and Participation*, 80 IOWA L. REV. 553, 581-82 (1995).

60. Whalen v. Roe, 429 U.S. 589, 600 (1977).

York's planned data processing did not violate the second *Whalen* interest.[61] This finding largely rested on the logic of bureaucratic rationality; as the Court noted, "disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient."[62] This quotation from *Whalen* appears time and time again in lower courts' summary rejection of the interest in independent decision-making.[63] Modern administrative systems must receive the personal information needed for their operations.

The independent decision-making strand of *Whalen* has never been developed into an effective tool for scrutiny of state data processing practices.[64] Indeed, the faith in bureaucratic rationality is so strong that courts have been unable to develop even a rudimentary syntax for discussing the second *Whalen* interest. In contrast, the first *Whalen* interest, that of nondisclosure of personal interest, is generally compatible with the concept of data seclusion and has met at least a mixed history in lower court opinions.[65]

C. *The Commodification Illusion*

Privacy-control's third flaw is the fashion in which it contributes to the commodification illusion. The idea that one has a right to control her data leads inexorably to the concept of a trade in personal information. Instead of protecting privacy through the privacy tort, we are to safeguard it through a property regime and recourse to a privacy market. Indeed, to the

---

61. *See id.*

62. *Id*. at 602.

63. A sample of cases draw on this language. *See In re* Grand Jury Proceedings, 867 F.2d 562, 565 (9th Cir. 1989); Borucki v. Ryan, 827 F.2d 836, 840-41 (1st Cir. 1987); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); Schachter v. Whalen, 581 F.2d 35, 37 (2d Cir. 1978); *In re* The August, 1993 Regular Grand Jury, 854 F. Supp. 1380, 1388 (S.D. Ind. 1994); Thompson v. City of Arlington, Texas, 838 F. Supp. 1137, 1146 (N.D. Tex. 1993); Borzillieri v. American Nat'l Red Cross, 139 F.R.D. 284, 288 (W.D.N.Y. 1991); Plowman v. U.S. Dep't of Army, 698 F. Supp. 627, 635 (E.D. Va. 1988); McKenna v. Fargo, 451 F. Supp. 1355, 1380 (D.N.J. 1978).

Several cases entirely reject or strongly narrow the *Whalen* interest. *See* Cutshall v. Sundquist, 193 F.3d 466, 480-81 (6th Cir. 1999); J.P. v. DeSanti, 653 F.2d 1080, 1089-91 (6th Cir. 1981); Adams v. Drew, 906 F. Supp. 1050, 1056-58 (E.D. Va. 1995); Hansen v. LaMontagne, 808 F. Supp. 89, 94-95 (D.N.H. 1992).

64. *See, e.g*., Fadjo v. Coon, 633 F.2d 1172, 1174-76 (5th Cir. 1981); Faison v. Parker, 823 F. Supp. 1198, 1201-02 (E.D. Pa. 1993); Mann v. University of Cincinnati, 824 F. Supp. 1190, 1198-99 (S.D. Ohio 1993); Hodge v. Carroll County Dep't of Soc. Servs., 812 F. Supp. 593, 599-600 (D. Md. 1992); Soucie v. County of Monroe, 736 F. Supp. 33, 35-36 (W.D.N.Y. 1990).

65. *See, e.g*., Russell v. Gregoire, 124 F.3d 1079, 1093-94 (9th Cir. 1997); Doe v. Southeastern Pa. Transp. Auth. (SEPTA), 72 F.3d 1133, 1141-43 (3d Cir. 1995); Doe v. Attorney General, 941 F.2d 780, 795-97 (9th Cir. 1991); Thorne v. City of El Segundo, 726 F.2d 459, 468-69 (9th Cir. 1983); Fadjo v. Coon, 633 F.2d 1172, 1175-76 (5th Cir. 1981); *Westinghouse Elec. Corp*., 638 F.2d at 575-78; Hodge v. Carroll County Dep't of Soc. Servs., 812 F. Supp. 593, 600 (D. Md. 1992); *Soucie*, 736 F. Supp. at 35-37.

extent that the privacy tort itself is receiving renewed attention in the Information Age, it is largely due to its "appropriation" branch, which is the most property-like aspect of this tort.[66]

This view of privacy-property has been advocated, for example, by Lawrence Lessig, one of the most astute legal thinkers regarding cyberspace.[67] Lessig calls on government to change the current legal entitlements regarding personal information. In his view, bottom-up choice regarding the use of personal information is currently blocked by "code," which is his term for technology's regulatory force.[68] At present, the default for Internet code favors the collection of personal information without customer consent.[69] Lessig's solution is as follows: "The trick would be to change the legal entitlements in a way sufficient to change the incentives of those who architect the technologies of consent."[70] His solution has two steps: "The state could (1) give individuals a property right to data about themselves, and thus (2) create an incentive for architectures that facilitate consent before turning that data over."[71]

Lessig's insight is genuine; it concerns the State's important role in using law to shape the form of technology. As Joel Reidenberg has also argued, technological configurations and system design choices constitute a powerful baseline structure of information policy.[72] Reidenberg describes these technical norms as the new "Lex Informatica," or information law, and calls for increased involvement by government and different policy communities in the process of standard-setting for technology.[73] Software and other technical elements of the Internet's infrastructure help create the conditions for personal data use in cyberspace, but these conditions are malleable.

Because technology is not fate, cyberspace can be constructed in any

---

66. For an attempt, albeit unsuccessful, to use such a tort to protect privacy from alleged misappropriation on an electronic bulletin board, see *Stern v. Delphi Internet Services Corp.*, 626 N.Y.S. 694 (N.Y. Sup. Ct. 1995). For an introduction to the appropriation branch, see DAN B. DOBBS, THE LAW OF TORTS 1198-1200 (2000).

67. *See* Lessig, *Law of the Horse*, *supra* note 20; *see also* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. 1998) [hereinafter R. POSNER, ECONOMIC ANALYSIS OF LAW] ("Secrecy figures in privacy law, which is conventionally treated as a branch of tort law but which is, in part, functionally a branch of property law.").

68. *See* Lessig, *Law of the Horse*, *supra* note 20, at 506, 509.

69. Lessig describes the invisibility of cyberspace monitoring: "Data is collected but without your knowledge. Thus you cannot . . . choose whether you will participate in or consent to this surveillance. . . . Nothing reveals whether you are being watched, so there is no real basis upon which to consent." *Id.* at 505.

70. *Id.* at 520.

71. *Id.*

72. *See* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 556 (1998) [hereinafter Reidenberg, *Lex Informatica*]. For an analysis of the impact of technological configurations within the context of choice-of-law in cyberspace, see Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1213-15 (1998).

73. *See* Reidenberg, *Lex Informatica*, *supra* note 72, at 587.

number of ways. In particular, the law can be used to shape incentives for construction of cyberspace code so less rather than more personal data are collected. Yet, the failure in the privacy market at present is so extensive that a mere declaration of a property right in personal information is likely to make matters worse rather than better. As I have noted above, privacy-control ignores the constraints on choice found in the movement to take-it-or-leave it processing of personal data.[74] Due to information asymmetries, collective action problems, bounded rationality, and limits on "exit," privacy is effectively being defined down on the Internet. As a result, legal identification of a property right will not alone create a functioning market.

Other conditions are necessary beyond an unembellished move to a property regime. A fully functioning "privacy market" requires incentives for companies to engage in behavior that I term "privacy price discrimination."[75] The standard definition by economists of price discrimination is that under it a seller sets "different prices to different purchasers depending not on the costs of selling to them, . . . but on the elasticity of their demands for his product."[76] In contrast, privacy price discrimination involves

74. As a final example, we can leave cyberspace and consider the processing of health care data in real space. Consumers of health care are invariably asked to sign two sets of "informed consent" documents. The first document must be signed to indicate consent to medical treatment; the second, to express consent with the processing of personal information that is generated by the treatment and associated events, such as third party payment. Here, again, we see a liberal conception of privacy. Just as it would violate physical self-determination under a liberal concept of privacy to have a physician touch or treat one's body without permission, it would violate information self-determination to have one's data processed without informed agreement.

With informed consent to medical treatment, the obtainment of agreement is supposed to help shape a process of communication about alternatives between physician and patient. In contrast, the second version of informed consent, in actual practice, merely involves signing a form that agrees to virtually all processing of personal data as a precondition to obtaining medical treatment. These broadly drafted disclosures of medical data serve to obscure physician and companies' practices rather than open a discussion about them. These informed consent forms are part of a smokescreen about information practices and not the basis for negotiations about them. *See supra* notes 42-45 and accompanying text. As Joel Reidenberg has observed of commercial data practices in general, "[c]ompanies control the disclosure of their practices and suffer no penalties for refusing to disclose. In fact, companies may suffer harm if they do disclose their inappropriate practices as a result of negative backlashes." Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 533 (1995).

75. For previous discussions, see Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1687.

Privacy price discrimination has a close analogy in the law of intellectual property. In the context of computer software, in particular, the law has been highly attentive to price discrimination and the kinds of behavior that should be permitted among buyers and sellers of information goods. *See, e.g.*, ProCD Inc. v. Zeidenberg, 86 F.3d 1447, 1448-49 (7th Cir. 1996); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 328 (1989); Robert Merges, *Comment: Of Property Rules, Coase, and Intellectual Property*, 94 COLUM. L. REV. 2655, 2666-67 (1994).

76. R. POSNER, ECONOMIC ANALYSIS OF LAW, *supra* note 67, at 305. For a pathbreaking discussion of the benefits of price discrimination, see Harold Demsetz, *The Private Production of Public Goods*, 13 J.L. & ECON. 293 (1970).

An illustration of the extent to which companies will seek to engage in price discrimination is Coca-Cola's current testing of "a vending machine that can automatically raise prices for its drinks in

a differentiation by data processing companies among individuals with varying preferences about the use of their personal data.

To illustrate this point, we can imagine two consumers: Marc and Katie. Marc cares deeply about the use of his personal information; Katie does not.[77] A surplus from cooperation under a property regime is only created, however, if Marc and others with similar preferences receive more than their "threat value" before disclosure.[78] The term "threat value" refers to the "price" that Marc would place on *not* disclosing his personal information, that is, on keeping it private. Under the current regime, companies have no need to offer Marc greater services or more money for his personal data than they do Katie. And Marc has little ability for either "voice" or "exit." In many instances, Marc may not even know that his data are being collected.[79] Indeed, Marc also has scant ability to *reduce* the supply of his personal information or to *increase* its price.[80] The consequences of this situation resound far beyond Marc and Katie.

Due to the pervasive failure in the privacy market in the United States, a subsidy is given to those data processing companies that exploit personal data. Commercial entities obtain Marc and Katie's personal data for the same low price. As a result, the true cost of personal data is not charged to these organizations. Such potentially privacy-enhancing developments, as I discuss in Part III.B, as Trusted Third Parties and privacy filters have yet to change this equation and appear unlikely to overcome the existing market equilibrium. The resulting subsidy to commercial entities in personal information, like other subsidies, is likely to encourage wasteful behavior.

The result of subsidized personal information is that companies over-invest in reaching consumers who do not wish to hear from them. Personal information at below-market costs also leads companies to under-invest in technology that will enhance the expression of privacy preferences. To build on Lessig's argument, the code of the Internet will not be altered until data processors are forced to internalize the cost of Marc's privacy preferences.

As a final observation regarding commodification, I wish to note that

---

hot weather." Constance L. Hays, *Variable-Price Coke Machine Being Test*ed, N.Y. TIMES, Oct. 28, 1999, at C1.

77. For a discussion of different consumer preferences about privacy, see Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1, *available at* <http://www.nytimes.com/library/tech/99/11/circuits/articles/11priv.html>.

78. For a concise introduction, see ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 73-74 (2d ed. 1997).

79. Imagine a prisoner's game with one party not only locked into repeat "plays," but with this same party unable in many circumstances to even know that the game is underway.

80. The ability to engage in price discrimination would permit Marc to limit the market power of the data processors. As such, my suggestion differs from proposals to give producers of intellectual property both market power and the power to engage in price discrimination. For analysis of the flaws of combining strong market power and price discrimination, see Wendy J. Gordon, *Intellectual Property as Price Discrimination: Implications for Contract*, 73 CHI.-KENT L. REV. 1367, 1384 (1998).

the present fashion in which personal information is consumed also causes non-economic spillover effects. Most importantly, the current regime of personal data use on the Internet leads to an opaque process involving: (1) widespread storage of personal data on networked computers; (2) tracking of one's visits to Web sites; (3) the creation of detailed marketing lists with personal data culled from cyberspace; and (4) introduction of pervasive technology for Web snooping. In this Article's next section, I turn to the issue of these non-economic spillover effects. I argue that the current privacy regime has a negative effect on the Internet's ability to contribute to democratic community in the United States.

II. THE PROMISE OF CONSTITUTIVE PRIVACY

Information privacy, whether on or off the Internet, should not be considered a right of control. Instead, it should be conceptualized as a constitutive value. Put simply, access to personal information and limits on it help form the society in which we live in and shape our individual identities. For example, the structure of access to personal information can have a decisive impact on the extent to which certain actions or expressions of identity are encouraged or discouraged. The importance of information privacy for both individuals and the community necessitates attention to boundaries about personal information.

Constitutive privacy is, therefore, a matter of line-drawing along different coordinates to shape permitted levels of scrutiny. Standards of information privacy should be considered as normatively defining "information territories."[81] These territories create patterns of knowledge and ignorance of personal data to stimulate or discourage different kinds of social expression and action.

An additional point must be made about constitutive privacy. An information privacy territory should not be expected to function as a data fortress that isolates personal information in some absolute sense. Personal data often involve a social reality that is external to the individual. As a result, the optimal utilization of this information is unlikely to exist at either end of the continuum that ranges from absolute privacy to complete disclosure.[82] The proper social response to information privacy issues cannot be to maximize secrecy about individuals and their pursuits. Rather, information privacy norms should create shifting, multidimensional data preserves that insulate personal data from different kinds of observation by different parties. Different kinds of "outing," that is, revelation of otherwise fully or partially hidden aspects of one's life, should be prevented

81. *See* Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1664-67.

82. For a similar conclusion regarding the use of personal medical information, see Schwartz, *Personal Health Care Economics*, *supra* note 29, at 41.

before different audiences.

As a concrete example of constitutive privacy, consider the Supreme Court's plurality opinion in *Planned Parenthood v. Casey*.[83] In *Casey*, five justices affirmed *Roe v. Wade*'s recognition of a woman's constitutional right to choose an abortion before fetal viability.[84] Beyond this aspect of *Casey*, the Supreme Court invalidated aspects of a Pennsylvania law mandating disclosure and record keeping requirements for abortions.[85] This statute required that physicians provide the state with a signed statement indicating either spousal notification by the woman seeking an abortion or existence of a significant reason for allowing bypass of such notification.[86] Through this law, Pennsylvania sought to employ physicians as government agents to ensure that husbands were informed of their wives' reproductive choices.[87]

In invalidating this aspect of the statute, the *Casey* Court created an information preserve for wives who seek independence in making reproductive decisions. This information territory was required, as Justice O'Connor's plurality opinion noted, due to the high level of domestic violence in the United States and the "[s]ecrecy [that] typically shrouds abusive families."[88] A spousal notification requirement, even one with a bypass provision, would devastate a woman's ability to engage in autonomous decision-making about reproductive choice.[89] At the same time, however, the Supreme Court upheld various provisions of the Pennsylvania statute that required limited release to the state of personal data about women who obtained abortions.[90] This disclosure was for public health reporting purposes and would be used only to generate statistical data.[91]

The result of *Casey* is to combine disclosure and non-disclosure rules for the same piece of information. It creates a multidimensional information preserve for personal information concerning women who seek and obtain abortions.[92] This Article will now further develop the nature and

---

83. 505 U.S. 833 (1992).

84. *See id.* at 846.

85. *See id*. at 887-94, 900-01.

86. *See id*. at 887-88, 901.

87. *See id*.

88. *Id*. at 889.

89. *See id*. at 898. As Justice O'Connor writes in her opinion for the plurality, the Pennsylvania law would empower a husband "with this troubling degree of authority over his wife." *Id*. Spousal notification would lead to men preventing "a significant number of women from obtaining an abortion." *Id*. at 893.

90. *See id.* at 900, 994. In an earlier case, *Thornburgh v. American College of Obstetricians & Gynecologists*, 476 U.S. 747 (1986), however, the Supreme Court voided a more detailed public health reporting requirement that was likely to reveal information to the public about specific individuals who had chosen to have an abortion. *See id.* at 764-70.

91. *See Casey*, 505 U.S. at 900.

92. It is important to stress that *Casey* created only two aspects of the necessary multidimensional rules. The Supreme Court found that an informational preserve: (1) was constitutionally mandated for

importance of constitutive privacy through an excursion into communitarian scholarship, and a response to the communitarians that draws on theorists of social norms.

A. *Constitutive Privacy and Communitarian Theory*

We begin with the communitarians, and I start with a caveat: I will include some civic republicans in this camp. Whether taken in this broader sense or a more narrow one, communitarians are a disparate group who, nevertheless, are bound by certain shared beliefs. In their view, the good society is a self-governing one based on deliberative democracy.[93] In place of liberalism's emphasis on the individual, communitarians seek an ongoing social project of authorship of a country's political values by its people. In searching for ways to construct this strong democracy, these thinkers emphasize common participatory activities, reciprocal respect among political equals, and the development of consensus about political issues.[94]

From this perspective, the promise of the Internet is not as a place for electronic commerce, but as a forum for deliberative democracy. Cyberspace answers the communitarians' search for a new hospitable place. It is an ideal locus for "civic forums," where to cite Frank Michelman's general formulation, "the critical and corrective rigors of actual democratic discourses" can occur.[95] As Benjamin Barber expresses a similar desire, our society requires shared areas "where we can govern ourselves in common without surrendering our plural natures."[96]

Areas for self-governance already exist and will continue to emerge on the Internet.[97] For example, Rutgers' Walt Whitman Center for the Culture

---

wives who seek to make reproductive decisions, and (2) did not extend to the state's public health reporting requirement. *See id*. at 897-98, 900. Many information privacy issues are not constitutionally cognizable, however, and additional dimensions of this particular data preserve are needed to map the conditions under which this information is to be shared with other entities, such as health insurance companies. This task will largely draw not on constitutional law, but on such means as health care privacy statutes. *See* NRC, FOR THE RECORD, *supra* note 47, at 39-46. For a view similar to my concept of constitutive privacy, see PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 44 (1995). This important work of Professor Regan also offers insightful historical analysis of the dynamics of privacy policy formulation within Congress. *See id*. at 174-211.

93. *See* MICHAEL J. SANDEL, DEMOCRACY'S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY 117 (1996) ("[T]he republican tradition emphasizes the need to cultivate citizenship through particular ties and attachments.").

94. *See id*. at 117-18; Joshua Cohen, *Deliberation and Democratic Legitimacy*, *in* DELIBERATIVE DEMOCRACY: ESSAYS ON REASON AND POLITICS 67 (James Bohman & William Rehg eds., 1997) [hereinafter DELIBERATIVE DEMOCRACY]; Frank Michelman, *How Can the People Ever Make the Laws? A Critique of Deliberative Democracy*, *in* DELIBERATIVE DEMOCRACY *supra* at 145, 147-48 [hereinafter Michelman, *How Can the People?*].

95. Michelman, *How Can the People?*, *supra* note 94, at 165.

96. BENJAMIN R. BARBER, A PLACE FOR US: HOW TO MAKE SOCIETY CIVIL AND DEMOCRACY STRONG 3 (1998).

97. For general discussions, see STEPHEN DOHENY-FARINA, THE WIRED NEIGHBORHOOD 45 (1996); LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE 8 (1997). The Usenet has al-

and Politics of Democracy, which Barber leads, in collaboration with Yale Law School's Information Society Project, is developing a model Web site, "Civic Exchange."[98] To facilitate self-governing political discourse on the Internet, Civic Exchange seeks to elaborate a "best practices" model.[99] Its Web site is to be "crafted in the hope that other users and institutions will develop kindred sites for culture, politics and education—sites that will make the Internet, not only a place for electronic commerce, but a place for us."[100] One of Civic Exchange's specific goals is to increase the interactivity of Web sites, which means, of course, that even more personal information will be generated by visitors to it and the sites that follow its approach.[101]

It remains to be seen how Civic Exchange and its cyber-progeny will collect and transmit personal information. Yet, its vision of deliberative democracy will be undercut by an absence of strong privacy rules. Deliberative democracy requires more than shoppers; it calls for speakers and listeners in a "space in which democratic attitudes are cultivated and democratic behavior is conditioned."[102] But when widespread and sometimes secret surveillance becomes the norm, the goal of democratic dialogue will be elusive.[103]

As I have observed in this Article's Part I, the Internet's current technical architecture causes individuals on simultaneously to collect and transmit information. While this architecture can be shaped to increase data privacy, the danger of sites such as Civic Exchange is the creation of ever greater amounts of finely grained personal data. When behavior leaves trails of personal information in a fashion that is difficult to understand or anticipate, speaking or listening will require a level of civic courage that cannot be required on a daily basis.

---

ready functioned as an important area for self-governance on the Internet. For an analysis, see Paul K. Ohm, *On Regulating the Internet: Usenet, A Case Study*, 46 UCLA L. REV. 1941 (1999).

98. *See Civic Exchange–Strong Democracy in Cyberspace* (visited Nov. 14, 1999) <http://www.law.yale.edu/infosociety/projects.html#civic>.

99. *See id*.

100. *Id*.

101. *See id*.

102. BARBER, *supra* note 96, at 6; *see also* Frank Michelman, *Law's Republic*, 97 YALE L.J. 1493, 1533-34 (1988) [hereinafter, Michelman, *Law's Republic*] (arguing for a "constitutional principle of privacy" suitable to "modern republican constitutionalism . . . [that protects] admission to full and effective participation in the various arenas of public life").

103. An opposite situation with harmful consequences is also possible. A society of only anonymous speech will not be supportive of democracy. The lack of accountability in such a world will encourage racist "flaming" and other kinds of abusive behavior. *See* Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1131 (2000).

B. *Responding to the Communitarians: Of Groups, Norms, and Preference Falsification*

The challenge for communitarians is to incorporate a concept of information privacy in their idea of civic dialogue. Yet, the immediate prognosis for the success of this endeavor is not good. For example, in one of the contemporary classics of civic republicanism, *Democracy's Discontent*, Michael Sandel does prefer information privacy to the freedom to engage in certain activities free of governmental restrictions. Apart from this preference, however, Sandel does not have much to say about data privacy in the Information Age.[104] Amitai Etzioni, a distinguished sociologist and leading communitarian, offers an even clearer indication of this movement's difficulty with information privacy, and I wish now to examine Etzioni's provocative views.

In *The Limits of Privacy*, Etzioni seeks to depict "the other side of the privacy equation."[105] In a series of case studies, he examines HIV testing of infants; data banks that list sexual offenders; restrictions on encryption products; the societal use of ID cards; and the processing of personal medical data.[106] Almost without exception, his conclusion is that "the common good is being systematically neglected out of excessive deference to privacy."[107] In Etzioni's judgment, the common good must now be shored up by greater public access to personal information. His call is for "a new communitarian conception of privacy."[108]

Instead of the State, Etzioni looks to the community and seeks to redraw the privacy balance by heightening communal scrutiny of individuals. For Etzioni, the present difficulty is that "the more privacy is granted from informal social controls in a given period, the *more* State controls will be necessary in following years to sustain the same level of social order."[109] The community should be given greater access to personal data and allowed to rely on its "subtle social fostering of prosocial conduct by such means as communal recognition, approbation, and censure."[110] In short, Etzioni wants to strengthen community by diminishing information privacy, which, in turn, is to have the further benefit of reducing the State's influence. In his judgment, "the best way to curtail the need for governmental control and intrusion is to have somewhat less privacy."[111]

My response to Etzioni's privacy agenda begins with some general comments about community decision-making and continues with more

104. *See* SANDEL, *supra* note 93, at 97; *see also* Michelman, *Law's Republic*, *supra* note 102.
105. ETZIONI, *supra* note 2, at 2.
106. *See id*. at 17-42, 43-74, 75-102, 139-82.
107. *Id*. at 4.
108. *Id*. at 15.
109. *Id*. at 215.
110. *Id*. at 213.
111. *Id*. (emphasis omitted).

specific analysis of his proposal's informational aspects. To begin then, Etzioni's idea of the community applying only a "subtle social fostering of prosocial conduct," while a worthwhile hope, has not been a historical reality.[112] Groups that act as intermediaries between the individual and the State have often proved oppressive of their members, and this intolerance as well as other problematic behavior undercut Etzioni's dream that strengthening the community and its institutions will further democratic goals. Alone due to this oppression and the sometimes high costs of exit for group members, the permissible scope of self-governance by different communities within the United States remains highly contested.[113]

In addition, communities, as norm theorists have pointed out, often generate inefficient rules.[114] By this observation, norm scholars indicate the frequent failure of self-governing groups to enable their members to exploit the full surplus of collective action. As Eric Posner warns, the demand for efficient norms "does not effortless[ly] call forth [their] supply."[115] Indeed, inefficient group norms may endure over decades in some instances. An example of suboptimality, much beloved in the legal literature of norms, is dueling, which long persisted as a means of resolving disputes in the antebellum South.[116] Another example of inefficient norms is over-fishing by New England whalers, which ultimately destroyed this industry.[117] Finally, groups not only have a potential for oppression and to be otherwise inefficient for their members, but also to create significant externalities for non-group members.[118] Such spillover costs can be pervasive.

This analysis helps demonstrate how imperfect a group definition of self-benefit can be. It also indicates that, in the abstract, no way exists to decide whether favoring a given community's development and enforcement of norms will lead to a positive result, whether for group members or society itself. These are general criticisms of strengthening groups. As for information privacy, Etzioni's policy of increasing the supply of personal information to the community appears no more convincing than his general

---

112. *Id.*

113. Among the entities whose behavior sometimes raises these controversial issues are the Amish, Church of Latter Day Saints, and Rajneesh. For a sample of differing voices in the debate about group autonomy, compare Netanel, *supra* note 27 (manuscript at 44-45), with Mark D. Rosen, *The Outer Limits of Community Self-Governance in Residential Associations, Municipalities, and Indian Country: A Liberal Theory*, 84 VA. L. REV. 1053, 1055-60 (1998).

114. *See generally* McAdams, *supra* note 6, at 418-20 (discussing conditions under which inefficient norms emerge).

115. Eric A. Posner, *Law, Economics, and Inefficient Norms*, 144 U. PA. L. REV. 1697, 1708 (1996) [hereinafter E. Posner, *Inefficient Norms*].

116. For explanations of the suboptimality of dueling, see Lawrence Lessig, *The Regulation of Social Meaning*, 62 CHI. L. REV. 943, 968-972 (1995); E. Posner, *Inefficient Norms*, *supra* note 115, at 1737-39.

117. *See* ELLICKSON, *supra* note 5, at 195-206.

118. *See* Netanel, *supra* note 27 (manuscript at 42).

plea for increasing community power.[119]

To be sure, democratic community requires access to personal data. As this Article's discussion of public accountability has already suggested, democratic community relies on an ongoing critical examination of persons and events, and, in many circumstances, this assessment depends on access to personal data.[120] At the same time, however, democratic community is *not* invariably furthered by heightening the access of groups to personal data. An increase in such flow of data can heighten oppression of group members, improve the longevity of inefficient group norms, and create externalities for others. Moreover, giving groups more personal information about oneself reveals nothing about whether or not the State's regulation will be displaced, or whether meddlesome behavior by community *and* government will be increased.[121]

To explain these negative implications of greater community access to personal data, I wish to draw on social norm theory and, in particular, the concept of "preference falsification." Social norm theorists have explored the phenomenon of modification of personal beliefs in response to social pressures under circumstances large and small. Such tailoring frequently leads people for a short or long period to join a perceived majority position.[122] One aspect of this process, preference falsification, provides special help in indicating the importance of access to personal information.[123]

As Timur Kuran has developed this concept, preference falsification is "the act of misrepresenting one's genuine wants under perceived social pressures."[124] People engage in such behavior because their public preferences affect how they are valued and treated. This act is widespread and has social implications that are sometimes positive, sometimes of no great

---

119. *See generally* ETZIONI, *supra* note 2.

120. For further analysis, see Thomas I. Emerson, *The Right of Privacy and Freedom of the Press*, 14 HARV. C.R.-C.L. L. REV. 329, 356-60 (1979) (analyzing the balance between "the right to know" and "personal privacy"); Robert C. Post, *The Social Foundations of Privacy*: *Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 999-1000 (1989) (analyzing further the assumption that the public has a right to inquire into the significance of public persons and acts).

121. As a historical example of this last possibility, the notorious Mississippi Sovereignty Commission in the 1950s and 1960s sought to assist white racist groups' opposition to the civil rights movement by collecting personal data, storing this information, and finding ways of drawing on it to harass disfavored individuals and groups. *See* American Civil Liberties Union of Miss. v. Mississippi, 911 F.2d 1066, 1068 (5th Cir. 1990); Calvin Trillin, *A Reporter at Large: State Secrets*, NEW YORKER, May 29, 1995, at 54.

122. As I will argue below, both the "Starr Report" and material released by the House Republicans sought to disclose endless amounts of humiliating details about President Clinton to discredit him and create an anti-Clinton bandwagon. *See infra* notes 128-133 and accompanying text.

123. *See* KURAN, *supra* note 6, at 3-5.

124. *Id.* at 3. For a study of negative effects flowing from the informational advantage enjoyed by a national leader, see Vai-Lam Mui, *Information, Civil Liberties, and the Political Economy of Witch-Hunts*, 15 J.L. ECON. & ORG. 503 (1999). Professor Mui argues that the incidence of witch-hunts increases when a nation's leader enjoys "an informational advantage" irrespective of the level of civil liberties in a country. *Id.* at 520.

import, and sometimes negative. To be adequately nuanced, I seek only to suggest that beyond a certain point of intensity, this herd behavior distorts public discourse and then alters both private knowledge ("the understandings that individuals carry in their own heads")[125] and private preferences (the preference that one "would express in the absence of social pressures").[126] At the extreme, a withdrawal of "beliefs from the realm of the thinkable to that of the unthinkable" occurs.[127]

Building on Kuran's work, I wish to argue that access to personal data is of critical importance due to its impact on the rate of preference falsification. Specifically, access to personal data can be used by norm entrepreneurs to gain knowledge of private preferences that may have been falsified under social pressure. Norm entrepreneurs are individuals who seek to bring about social change by identifying and acting on existing norms. Such knowledge of private preferences allows the revelation of beliefs and desires that one would rather hide, the placing of pressure on private knowledge, and the shifting of that which is and is not discussed in public discourse.

The path of norm entrepreneurs towards these goals can involve either *release* or *suppression* of personal data. Once a norm entrepreneur has superior knowledge regarding a group member's private knowledge or private preferences, she might choose exposure of personal information to embarrass the group member, discredit her, and/or create a groundswell of opinion against her. Indeed, individuals may also strategically reveal their own personal information to shape public discourse. In Bill Clinton's immortal words during his first campaign for the Presidency: "I did not inhale."[128] The goal for the norm entrepreneur and the individual revealing his information is the same: it is to manipulate the process by which people learn from the information that is publicly available. As I have already noted, this process is complex. Preference falsification can serve to support good or bad norms. My initial point is merely that the release and suppression of personal data play a powerful though not inevitably salubrious role in formation of social beliefs.

Once elected President, Clinton would continue to offer useful examples for students of privacy and norms. Consider the publication of intimate details of Clinton's life in the Starr Report and in evidence released by the House Judiciary Committee. In *An Affair of State*, Richard Posner offers a vivid characterization of the collection and disclosure of this per-

125. KURAN, *supra* note 6, at 157.

126. *Id.* at 17.

127. *Id.* at 177.

128. DAVID MARANISS, FIRST IN HIS CLASS: A BIOGRAPHY OF BILL CLINTON 154 (1995). According to witnesses of Clinton's Oxford years, the President did, in fact, have trouble in this regard. One contemporaneous witness told Maraniss, "[w]e spent enormous amounts of time trying to teach him to inhale. . . . He absolutely could not inhale." *Id.*

sonal information.[129] In his account, Judge Posner is particularly scathing concerning the House Judiciary Committee's publication of its "mass of evidence."[130] Posner terms this material "an astonishing farrago of scandal, hearsay, innuendo, libel, trivia, irrelevance, mindless repetition, catty comments about people's looks, and embarrassing details of private life."[131]

Judge Posner's characterization is correct: the House Judiciary Committee's report is all this and more. This publication is also an excellent example of norm entrepreneurs at work; its release marks an attempt by Republicans in Congress to shape the terms of public discourse by shifting that which is and is not discussed. Their immediate goal was to create a focal point around the personal and sexual life of the President as well as his artful and not so artful prevarications about his behavior ("It all depends on what the meaning of the word 'is' is.").[132] The hope of the anti-Clinton norm entrepreneurs was that citizens would react with venom against the President's behavior and lies about it. Their plan was to present the awaited public disgust as signaling agreement with the forces for impeachment and to use this groundswell of anti-Clinton opinion to cast the President out of office. The result, as we know, was different. Of particular interest, however, is that competing norm entrepreneurs sought to neutralize this strategy by creating a mirror focal point through their release of humiliating information about the personal life of leading Republicans.[133]

Norm entrepreneurs do not always seek to *reveal* personal information to the public. Private and public opinion also can be altered through the collection and then *suppression* of personal data about private knowledge and private preferences. Sometimes a group represses personal information because it would indicate widespread deviance from group norms. Such suppression can be combined with a suggestion to targeted individuals of the future possibility of release of information about them, with or without separate forms of punishment, if their obedience to group norms does not follow. During the Cold War, the East German secret police, the

---

129. *See generally* RICHARD A. POSNER, AN AFFAIR OF STATE: THE INVESTIGATION, IMPEACHMENT, AND TRIAL OF PRESIDENT CLINTON (1999). As Judge Posner writes regarding the frequent recourse to demagoguery of Republicans and Democrats in the public debate over impeachment:

> Democrats called for an end to the "politics of personal destruction," but did not retract their own attempts to destroy Starr (sex-obsessed sickie), Jones (trailer trash), and Lewinsky (stalker). Few of them criticized Larry Flynt, the publisher of the feminists' nightmare, the pornographic magazine *Hustler*, when he "outed" Speaker-designate Robert Livingston in an effort to derail the impeachment train, or when he tried to out Congressman Bob Barr, one of the House prosecutors in the impeachment trial.

Id. at 115.

130. *Id*. at 82.

131. *Id*. at 88.

132. *Id*. at 57 n.75. Posner provides an account of President Clinton's statement and the maneuvers of the President's lawyers that provoked it. *See id.* at 57.

133. *See id*.

Stasi, perfected this technique of collection, repression, and selective disclosure of personal information.[134] The Stasi sought to suppress any social or political change that did not occur on its own terms. In the United States, in contrast, the law sometimes forbids the extraction of a reward for not carrying out threats to reveal information. It terms such threats "blackmail."[135]

Let us return to information privacy as a constitutive value. This excursion through communitarianism and social norm theory suggests that privacy provides an essential way of policing the community and the State. Constitutive privacy is a way to limit the rate of preference falsification; it places restrictions on an "outing" of knowledge and preferences that would be destructive to democratic community.[136] Properly devised, therefore, information privacy does not impede norm formation; rather, it prevents mission-creep by over-zealous norm entrepreneurs. In contrast to a blanket default that would increase the community's access to personal information, constitutive privacy views limits on access by the State and community to personal information as a necessary means of restricting these entities' sovereignty.[137] These limits shape information territories to allow the necessary independence of social expression and action. Witch hunts are only more effective when those in control know more about those that they seek to persecute.[138]

III. THE STATE'S ROLE

This Article has now presented a substantive theory of information privacy. In this Part, it shifts from ends to means. I begin with a criticism of the dominant rhetoric of cyber-talk concerning means and conclude by exploring the proper role for the State in the process of creating and maintaining constitutive privacy.

A. *The Dominant Rhetoric*

In this Article's introduction, I briefly set out the dominant rhetoric concerning cyberspace governance. As I noted, this rhetoric is built around

---

134. For two popular accounts in English, see TIMOTHY GARTON ASH, THE FILE: A PERSONAL HISTORY (1997); TINA ROSENBERG, THE HAUNTED LAND: FACING EUROPE'S GHOSTS AFTER COMMUNISM 261-394 (1995).

135. *See* Ronald H. Coase, *The 1987 McCorkle Lecture: Blackmail*, 74 VA. L. REV. 655, 657-58 (1988); *see also* James Lindgren, *Unraveling the Paradox of Blackmail*, 84 COLUM. L. REV. 670 (1984) (attempting to discover a theory that explains the illegality of blackmail).

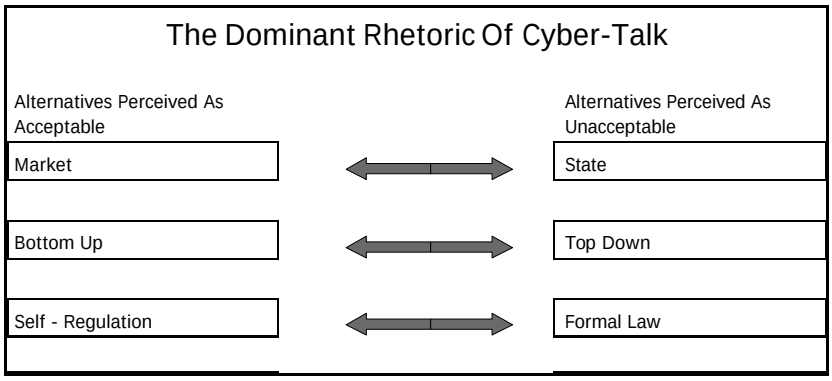
136. For a pathbreaking discussion from a similar perspective, see McAdams, *supra* note 6, at 425-32.

137. Kuran merely points to the necessary "domain in which we are free to do as we please" as being embodied in "our own homes [where] we are generally free to make our own decisions, guided by our own knowledge, expectations, and priorities." KURAN, *supra* note 6, at 40.

138. *See generally* Mui, *supra* note 124, at 510-18.

three pairs with only one choice from each set deemed as acceptable. The structure of this cyber-talk can be represented in graphic form, and I have done so in Table A.

TABLE A



The preferred discourse begins with a choice between letting either the market or the State have the upper hand in shaping decision-making on the Internet. Here is how Microsoft expressed its own public preference for the market and not the State: "The growth and success of [the information technology sector], this dynamic and flourishing industry, has been driven almost exclusively by action taken in the private sector."[139] As part of its discourse in favor of the market, Microsoft has started a major public relations offensive dedicated to its "freedom to innovate" and compete in the marketplace.[140] In its view, the State now stands in the way of its freedom and the market. In the view of the Justice Department and Judge Thomas Penfield Jackson, the federal district judge now hearing the Microsoft antitrust case, Microsoft's own predatory behavior interfered with the work-

139. *Microsoft, Technology and Our Economy*, N.Y. TIMES, Sept. 21, 1999, at A18 (advertisement).

140. Information on the public relations campaign can be found at Microsoft, *Freedom to Innovate Network* (visited Jan. 28, 2000) <http://www.microsoft.com/freedomtoinnovate/>. For media coverage on the "Freedom to Innovate Network," see Joel Brinkley, *Awaiting Verdict, Microsoft Starts Lobbying Campaign*, N.Y. TIMES, Nov. 1, 1999, at C6; John R. Wilke, *Microsoft Seeks Help of Holders*, WALL ST. J., Nov. 1, 1999, at A56.

ings of the market.[141]

The argument in favor of the market instead of the State has also been made specifically in the context of privacy. Solveig Singleton is a leading academic proponent of an exclusive reliance on the market. In her view, "entrepreneurs must be permitted to take care of their cues from the results of engaging in the marketplace, not from top-down commands."[142] She believes that the market will infallibly supply as much privacy as people desire.[143]

The second alternative is bottom-up versus top-down. Bottom-up relates to the ideas both of spontaneous order and of self-rule. The idea of spontaneous order, which is closely associated with bottom-up governance, is an integral part of the Internet's own construction as a network of networks. The Internet is engineered to have the redundancy that is typical of spontaneous arrangements.[144] Bottom-up also relates to a belief in governance of the Internet through self-rule. Cyberspace appears to rewrite *Federalist 14*, where James Madison deemed representative government necessary for the United States because of "the great extent of country which the union embraces."[145] In Madison's words, a sad limitation on direct democracy was its necessary restriction to "a small number of people, living within a small compass of territory."[146] On the Internet, however, distance under many circumstances no longer matters, and self-rule appears possible for cyberspace.

In this Article, however, I have scrutinized this belief in cyberpopularism in the specific context of privacy-control and found that considerable limits exist on individual decision-making. In the broader context of self-governance of the Internet, Mark Lemley, Neil Netanel and

---

141. *See* United States v. Microsoft Corp., 65 F. Supp.2d 1 (D.D.C. 1999) (providing findings of fact).

142. *Electronic Commerce, Testimony Before the House Subcomm. on Telecomms., Trade and Consumer Protection Electronic Commerce: The Current Status of Privacy Protections for Online Consumers*, July 13, 1999 (statement of Soveig Singleton), *available in* 1999 WL 20009951. In her words, "the view that business would not respond to privacy preferences is an extraordinary bizarre view." *Id*. at 3.

143. *See id*. For a similar view, see Thomas G. Donlan, *Freedom of Information: The Right to Privacy Must Be Maintained by Private Effort*, BARRON'S, June 21, 1999, at 62, *available in* 1999 WL-BARRONS 19353447.

144. As Nathan J. Muller writes:

> The fundamental operational characteristics of the Internet are that it is a distributed, interoperable, packet-switched network. A distributed network has no one central repository of information or control, but is comprised of an interconnected web of host computers, each of which can be accessed from virtually any point on the network.

NATHAN J. MULLER, DESKTOP ENCYCLOPEDIA OF THE INTERNET 172 (1999); Reidenberg, *Lex Informatica*, *supra* note 72, at 566-568.

145. James Madison, *"Publius," The Federalist XIV, in* DEBATE ON THE CONSTITUTION 431 (Bernard Bailyn ed., 1993).

146. *Id*. at 432.

others have criticized the ideology of cyber-popularism writ large.[147] Others, including David Post, who is otherwise a strong believer in Internet self-governance, have expressed their disenchantment with the emerging reality of domain name management by the Internet Corporation for Assigned Names and Numbers (ICANN).[148]

As to the third alternative, industry self-regulation versus formal law, it would be difficult to exaggerate the influence in the privacy policy debate of either this dichotomy or the current preference for self-regulation. In particular, the online industry is ceaseless in lobbying for this policy alternative. In the words of the Online Privacy Alliance, for example, online industry is engaged in development and use of self-regulation to create "an environment of trust and foster the protection of individuals' privacy online and in electronic commerce."[149] According to the *New York Times*, the Online Privacy Alliance's campaign for self-regulation "has strengthened the standing of those who believe that a hands-off approach is the wisest Internet policy."[150] In Part I.A above, moreover, I have described how this notion of self-regulation already has captured a majority of the FTC.

This Article has criticized such standard setting, however, as a defining down of privacy in a fashion intended to favor the interests of online industry. Yet, a complete theory of self-regulation must look beyond this current reality and the limited rhetoric of "industry" self-regulation. Public choice theory has allowed us to see that much legislation is created through a negotiated process that involves the government brokering arrangements among interest groups.[151] In the field of information privacy, however, scholars still need to develop a model of self-regulation's normative possibilities.

Self-regulation possesses the great potential to involve not only industry, but government and watchdog groups in negotiating standards, such as codes of conduct, that shape industry behavior. Already, good and bad news exists in this area. First, the good news. As one positive sign, the watchdog groups that might be involved in such a process of negotiation already exist, and include the Center for Democracy and Technology,[152] the

147. *See* Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1266-92 (1999); Netanel, *supra* note 27.

148. *See* David Post, *ICANN and the Consensus of the Internet Community* (Aug. 20, 1999) <http://www.icannwatch.org/archives/essays/935183341.shtml>.

149. Online Privacy Alliance, *Mission* (visited Feb. 2, 2000) <http://www.privacyalliance.org/mission>. Or, as a final example, Peter P. Swire and Robert Litan, in a study of privacy for the Brookings Institute, emphasized the promise of "self-regulatory measures" to protect "important privacy values while reducing the compliance burden on organizations." SWIRE & LITAN, *supra* note 2, at 159.

150. Steve Lohr, *Seizing the Initiative on Privacy*, N.Y. TIMES, Oct. 11, 1999, at C1.

151. *See* DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION 17-21 (1991); KENNETH A. SHEPSLE & MARK S. BONCHEK, ANALYZING POLITICS: RATIONALITY, BEHAVIOR, AND INSTITUTIONS 222-226 (1997).

152. *See* <http://www.cdt.org>.

Electronic Privacy Information Center,[153] and the Electronic Frontier Foundation.[154] In addition, privacy seal organizations, such as TrustE[155] and BBBOnline,[156] also have a potentially important role as organizations capable of: (1) certifying that bargains once struck are upheld, and (2) streamlining the presentation of information to the public through representations in the form of a simple "seal."

The bad news is that most privacy self-regulation thus far has led to online industry drafting weak standards that ratify the current status quo or even weaken it.[157] Moreover, privacy watchdogs have not yet had significant impact on industry behavior.[158] Finally, privacy seal organizations are still at a nascent stage and moving only slowly to present the kinds of standardized terms that consumers might be able to understand with limited investment of time.[159]

As for the Clinton Administration, it has expressed a strong preference for the market, bottom-up, and self-regulation. In *The Framework for Global Electronic Commerce*, the White House states, "[t]he private sector should lead."[160] As the adage on Wall Street has it: let the winners run. *The Framework for Global Electronic Commerce* goes on to attribute at least part of the "genius and explosive success of the Internet . . . to its decentralized nature and to its tradition of bottom-up governance."[161] More specifically regarding privacy in cyberspace, the White House's reliance on the dominant rhetoric has encouraged its deference to the private sector's self-regulation. For example, the U.S. Government Working Group on Electronic Commerce's *First Annual Report* finds "privately enforced codes of conduct should be a central instrument for protection of online privacy . . . ."[162]

---

153. *See* <http://www.eff.org>.

154. *See* <http://www.epic.org>.

155. *See* <http://www.truste.org>.

156. *See* <http://www.bbbonline.org>.

157. *See* Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1687-96.

158. The latest example of industry attempts to ignore privacy watchdog organizations comes from DoubleClick, an online advertising agency, which initially offered a weak response to external criticisms of its plan to link its online and offline databases. *See* Lukenbill & Magill, *supra* note 15, at 1 (quoting Michigan Attorney General Jennifer Granholm). Criticisms from these organizations, lawsuits, government investigation and media coverage have, however, led DoubleClick to at least temporarily modify this plan. *See supra* note 15 and accompanying text.

159. On the nascent current state of the privacy seal organizations, see Center for Democracy and Technology, *Behind the Numbers: Privacy Practices on the Web* 12-13 (July 27, 1999) <http://www.cdt.org/previousheads/dataprivacy.shtml>.

160. THE WHITE HOUSE, THE FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, at Principles § 1 (1997) <http://www.whitehouse.gov/WH/New/Commerce/read.html>. The Framework adds: "Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention." *Id.* § 2, ¶ 1.

161. *Id.* § 4, ¶ 1.

162. U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT 8 (1998).

Despite the dominant rhetoric's pervasiveness, it fails in two significant ways. I will set out these shortcomings in a nutshell and then elaborate in more detail with examples drawn from the Digital Millennium Copyright Act's privacy provisions.[163] The first shortcoming of the dominant rhetoric is that, on a descriptive level, this model neglects the complex reality of the Internet in the year 2000. An outsider observing Internet development might report back that people in the United States were talking about one thing and doing another. This visitor would find no shortage in cyberspace of recourse to modes of regulation other than those favored in the dominant rhetoric. In some circumstances, moreover, this flight from the dominant rhetoric appears highly desirable.

Second, the structure of the current policy debate provides little help for voyagers in the realm of the normative. When we go beyond "is" to discuss the means for attaining what cyberspace "ought" to be, the rhetoric's stark contrasts leave no possibility for adequately nuanced solutions. The market, bottom-up, and industry self-regulation are to be the essential elements of any solution. The result is systematic, yet supple: the right answer is never the State, top-down, or the law. In fact, the best responses to many issues regarding Internet privacy in particular and Internet governance in general exist beyond the dominant rhetoric.[164]

To illustrate these two points about the dominant discourse's shortcomings, I wish to examine one aspect of the Digital Millennium Copyright Act of 1998. Among its other goals, this statute uses law to regulate copyright management systems (CMS). These systems put secure digital envelopes around works in order to permit copyright owners to regulate access to their works reliably and to charge automatically for different kinds of access.[165] The Digital Millennium Copyright Act's response to CMS attempts not to command behavior directly, but to shape technology, market forces, and norms.

These trusted systems, as Julie Cohen has pointed out, provide a form of private copyright governance.[166] Using these devices, copyright owners can precisely control the exploitation made of their intellectual property.

---

163. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, § 1201, 112 Stat. 2863 (1998) (codified at 17 U.S.C. § 1201 (Supp. IV 1998)) [hereinafter DMCA].

164. *See* Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1297-98 (1998) ("The bottom-up 'versus' top-down distinction tends to be obfuscatory in cyberspace, as it is elsewhere" and, therefore, the critical question regards the "details of a good mixture.").

165. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 983-84 (1996); Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. § I, ¶ 1 (1997) <http://www.law.berkeley.edu/journals/btlj/articles/12-1/cohen.html> [hereinafter Cohen, *Some Reflections*].

166. *See* Cohen, *Some Reflections*, *supra* note 165, § IV.A. For an industry-wide step to build the technology to allow CMS into online products, see Trusted Computing Platform Alliance, *Background* (visited Nov. 14, 1999) <http://www.trustedpc.org/home/home.htm>.

Yet, the implications of CMS for privacy can be highly negative; these systems enable copyrighted works themselves to carry out a pervasive monitoring of individual activity. As Pamela Samuelson has written, copyright material with CMS permits works to "rat" on readers.[167]

In contrast to the restricted actions envisioned by the dominant rhetoric, the Digital Millennium Copyright Act will shape technology and the market to reach privacy norms. It thereby demonstrates the validity of the insight of social norm theorists regarding the law's ability to reach behavior indirectly by an impact on other regulatory forces.[168] Its path to a certain kind of privacy norm is worth tracing with some care.

The Digital Millennium Copyright Act's general prohibition on circumvention of CMS seeks to overcome these systems' greatest weakness, which is their potential to stimulate a digital arms race. In other words, individual hackers and enterprising companies might develop software that allows CMS to be bypassed or, in the law's language, "circumvented."[169] To limit this possibility, the Digital Millennium Copyright Act generally forbids circumvention of these devices and even includes criminal penalties for certain violations of its ban.[170] Yet, the Act also permits exceptions to its general restrictions on anti-circumvention devices. For our purposes, the most interesting of these is the one for privacy.[171]

Here, the Digital Millennium Copyright Act reveals its intention to shape technology, the market and, ultimately, privacy norms. To quote from the Act, privacy circumvention is permissible only "if the technological measure . . . collects or disseminates personally identifiable information about the person without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capacity to prevent or restrict such collection or dissemination."[172] Thus, the Digital Millennium Copyright Act seeks to stimulate a privacy norm that includes: (1) notice and (2) an opportunity to opt out of collection of personal data by CMS technology. It does so by offering a "carrot" to a copyright owner: the privacy anti-circumvention loophole will be closed if the copyright owner sets CMS technology to provide "conspicuous notice" and provides users of copyrighted products with "the capacity

---

167. *See* Pamela Samuelson, *Will the Copyright Office Be Obsolete in the Twenty-First Century?*, 13 CARDOZO ARTS & ENT. L.J. 58 n.18 (1994).

168. *See* Lessig, *Law of the Horse*, *supra* note 20, at 512-13. For a second norms theorist who has made this point, see Richard H. McAdams, *Comment, Accounting for Norms*, 1997 WISC. L. REV. 625, 635-36.

169. *See* DMCA, *supra* note 163, § 1201.

170. For the DMCA's criminal penalties, see *id.* § 1204.

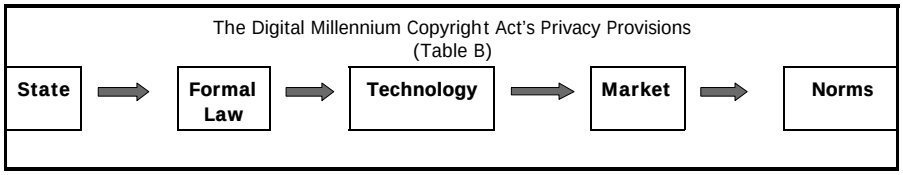
171. *See id.* § 1201(i)(1)(B). David Nimmer colorfully refers to the privacy exception to the general rule of anti-circumvention as being one of the "public interest quasi-exceptions" of the DMCA. David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPYRIGHT SOC. USA 401, 407 (1999).

172. DMCA, *supra* note 163, § 1201(i)(B).

to prevent or restrict such collection or dissemination."[173]

If this norm does not emerge, the Act takes a different tack and turns to the market. Its goal is to stimulate a market for privacy-enhancing devices by explicitly allowing CMS technology to be weakened. These regulatory moves can be represented graphically, and I have done so in Table B.

TABLE B



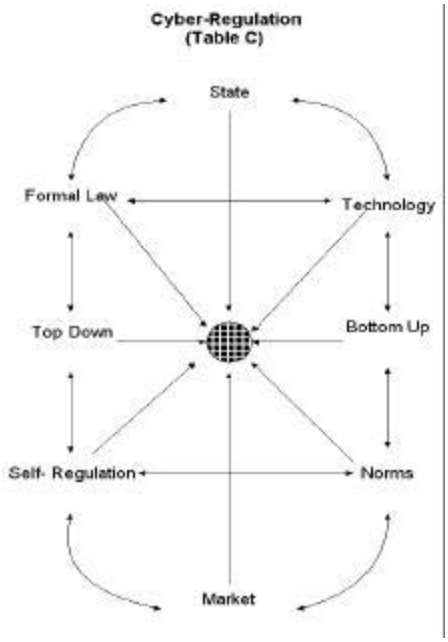
As this graph indicates, the Digital Millennium Copyright Act acts on technology first. It does so by anti-circumvention measures that forbid tampering with or bypassing CMS devices.[174] If the CMS installer allows too much snooping, however, the Digital Millennium Copyright Act permits the technology to be weakened by those who will be spied upon. Its permission may stimulate a market for privacy-enhancing technology that will, thereby, shape norms. Thus, the choice between the carrot or stick is left to the copyright owner; it all depends on how she plans to use CMS. The Act's shaping of norms takes a different approach depending on the level of snooping or privacy that the copyright owner provides through CMS.

The news is therefore both good and bad. The bad news is that the dominant rhetoric fails; the good news is that the world of cyberspace is a far more interesting place than the dominant rhetoric envisions. In place of the paired opposites of the accepted rhetoric, more complex choices are available in the creation of public, quasi-public, and private spaces in cyberspace. Although I have represented a subset of these possibilities in linear fashion in Table B, the regulatory universe is not one-dimensional. A more accurate depiction of the possibilities of direct and indirect regulatory effects is a Copernican model, and I have created such a representa-

173. *Id.*

174. *See id.* § 1201(a).

tion in Table C.[175] The object in the center, the radius of the regulatory system, is cyberspace.



This Table, the "Lessig Chart," represents the world of cyber-regulation.

Table C corrects the dominant rhetoric and its flaws (Table A) and builds on two-dimensional representation of regulation in cyberspace (Table B). It demonstrates illustrative regulatory possibilities for privacy in cyberspace. By stating that these are illustrative possibilities, I wish to indicate that arrows can be drawn from any one entity in Table C to any other, and that I have limited the depiction of lines to keep the chart from becoming hopelessly crowded.

A simple example of this chart in use might indicate that self-regulation (represented in the lower left hand of this chart) can begin with an industry code of conduct. If effective within industry, this code of conduct will have an impact on norms (bottom right hand of the chart) and then effect the object in the center, which represents cyberspace, or more precisely, a given application of it, such as Web sites on the Internet.[176] This story is, in fact, the one that online industry would have us believe its

175. This depiction builds on that of Lessig, whose influence on this section is great. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 164-82 (1999) [hereinafter LESSIG, CODE]; Lessig, *Law of the Horse*, *supra* note 20, at 506-10.

176. *See generally* Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1164 (1999) (arguing against "old talk of the Internet as a whole" in favor of analysis that focuses on the application layer "above the basic Internet protocols").

posting of privacy policies presents. Codes of conduct might also go beyond norms to an impact on technology (upper right hand of the chart), as, for example, in stimulating the use of privacy-enhancing technologies.

As a final point, I wish to place a label on Table C, which I propose to term a "Lessig Chart." The eponymous label follows from Lawrence Lessig's path-breaking demonstration of the variability of cyberspace regulation in his *Code and Other Laws of Cyberspace*.[177] For different areas of cyberspace, customized "Lessig Charts" should be drawn to indicate the risks and promises of different kinds of regulatory strategies. Different individuals or organizations may even reach various conclusions about these outcomes and present different charts to represent the likely path of a cyber-regulatory strategy. Yet, the benefit of using "Lessig Charts" will remain. This new model replaces today's preferred rhetoric of constricted cyber-talk with a vision that opens up, rather than limits, our vision of regulatory possibilities in cyberspace.

B. *Correcting Market Failure and Limiting Preference Falsification*

The State may seem like the most unlikely source of anything positive for Internet privacy. To begin with, many consider the State, whether the federal government or any government, as Orwell's Big Brother. For these critics, the State is and will always be Privacy Enemy Number One.[178]

In addition, the State's own behavior all too often seems intended to live up to its low reputation. In particular, the federal government has made heroic efforts to shape Internet technology to keep it at least as open for law enforcement spying as older telecommunication systems. Thus, the Federal Bureau of Investigation advocated its ill-fated Clipper Chip, the Clinton Administration sought to restrict encryption software, and Congress enacted the Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunication companies to make the next generation of digital switchers and routers as "tappable" as the past generation of analogue devices.[179]

Yet, the private sector is as much the potential enemy of privacy as the State and, as a result, we must fear the government's inaction as much as its action. To illustrate this point, I wish to discuss Jamie Boyle's critique of the State's role on the Internet.[180] For Boyle, writing in 1997, the danger is that the State will "privatiz[e] the Panopticon."[181] Boyle's work draws

177. LESSIG, CODE, *supra* note 175, at 85-108.

178. *See* PETER HUBER, LAW AND DISORDER IN CYBERSPACE 189 (1997).

179. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. §§ 2518, 2522, 3124; 47 U.S.C. §§ 229, 1001-1010) (1994 & Supp. IV 1998)).

180. *See* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 177-78 (1997).

181. *Id*. at 198.

on Michel Foucault's study of the Panopticon, a proposal for a progressive prison made by Jeremy Bentham in 1787.[182] Bentham's plan was to construct a prison as a wheel around an observing warden. Unsure when those in authority might be spying on him, the prisoner would conform his behavior to their presumed desires. In Foucault's view, however, power in the modern age is not merely exercised by the State, but also by "multidinous non-state sources."[183] Foucault's view depicts private entities' discipline of individuals by their forcing of an internalization of authority.

Boyle situates Foucault's analysis in cyberspace and finds that the State is working to create an Internet Panopticon. In Boyle's view, the State is building its surveillance into the "architecture of transactions" while shifting responsibility for actual enforcement to ISPs and other large-scale commercial entities.[184] In this turning to the private sector, the State enlists "nimbler, technologically savvy players as [its] private police."[185] As a consequence, as Boyle writes, "[i]ntrusion into privacy, automatic scrutiny of electronic mail, and curtailment of fair use rights . . . would occur in the private realm, far from the scrutiny of public law."[186]

Some of the State's past and current actions fit Boyle's prescient analysis. The government's herculean efforts to make Internet technology open for snooping resemble such an attempt to install the Panopticon. Moreover, many fear that the intense, ongoing attempts to develop rating devices for content on the Internet will permit upstream filtering by the government.[187] As the Global Internet Liberty Campaign has stated, "[t]he existence of a standardized rating for Internet content—with the accompanying technical changes to facilitate blocking—would allow governments to mandate the use of such a regime."[188] Yet, the government's privatized Panopticon is only one danger. Beyond it, private entities are happily and busily creating their own independent Panopticons.

The private sector is eager to spy on us to create its marketing lists and profiles while, at the same time, seeking to keep this process opaque and refusing to grant basic fair information practices. Solutions to the problem

---

182. *See* JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., 1995) (original published in 1787); MICHEL FOUCAULT, DISCIPLINE AND PUNISH (Alan Sheridan trans., Vintage Books 2d ed. 1995).

183. FOUCAULT, *supra* note 182, at 104-05.

184. Boyle, *supra* note 180, at 197-98.

185. *Id*. at 197.

186. *Id*. at 197-98. For a further discussion of the Panopticon, Foucault, and how bureacracy gains from use of personal information, see OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 53-94 (1993).

187. For an excellent collection of essays with this viewpoint, see ELECTRONIC PRIVACY INFORMATION CENTER, FILTERS AND FREEDOM: FREE SPEECH PERSPECTIVES ON INTERNET CONTENT CONTROLS (1999)

188. Electronic Frontier Foundation, *Global Internet Liberty Campaign Member Statement* ¶ 4 (last modified Sept. 7, 1999) <http://www.eff.org/pub/Censorship/Rating...9990907_gilc_intl_rating_statement.html>.

of the private Panopticon will require some recourse to the State. In light of the known danger of answered prayers, however, the critical question regards the State's proper role in Internet privacy. In my view, the State should concentrate its activities on two areas: (1) assisting in the creation and maintenance of the conditions for a functioning privacy market, and (2) supporting development of privacy norms that protect against too great a rate of preference falsification. Success in both areas is essential to creation and maintenance of constitutive privacy's information territories. In other words, I am not retreating to an autonomy-perfecting approach. In my view, both a functioning privacy market and certain kinds of privacy norms are necessary. I wish now to address the two areas of cyberspace privacy in which the State should play an important role.

First, in considering the creation of a functioning privacy market, we should return to the idea of privacy price discrimination and to Marc and Katie. The market can play an important role in creating information territories in cyberspace. For example, Trusted Third Parties (TTPs), sometimes termed "infomediaries," are already emerging.[189] These companies seek to act on behalf of individuals in creating a new information supply chain. TTPs assist Marc and those with similar privacy preferences by locating firms that agree to respect these wishes. TTPs can also reach out to Katie by offering an alternative to those firms that currently benefit from her failing to bargain before surrendering her personal data. Under their influence, her privacy preferences may even shift. Other market solutions include filtering technologies, such as P3P, which is a transmission protocol for allowing an individual to check whether a Web site's privacy practices match her wishes.[190]

At present, however, a personal information subsidy stifles the market for these privacy-enhancing approaches. Moreover, the current approach to self-regulation encourages online industry to use collaborative standard-setting to lock-in a poor level of privacy. Industry consensus can easily form around norms that do not benefit society as a whole.

To build a functioning privacy market, the State's first two steps should be to: (1) discourage a default of maximum information disclosure, and (2) encourage a market for privacy enhancing technology. To overcome more general failings in privacy market efficiency, the State's next steps should be to: (3) reduce information asymmetries, and (4) seek ways to overcome collective action problems. In one small area of cyberspace, which concerns commercial Web sites' gathering of personal data from

189. *See* Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1685. John Hagel III and Jeffrey F. Rayport first predicted the development of these organizations and coined the eponymous, if not euphomous, term, "infomediaries." *See* John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, HARV. BUS. REV. 53, 54 (1997).

190. *See* Philip DesAutels, *W3C Platform for Privacy Preferences (P3) Project* (visited Mar. 29, 1999) <http://www.w3.org/P3P/Update.html>.

children, the State has made efforts regarding almost all of these steps.[191]

The Children's Online Privacy Protection Act of 1998 (COPPA)[192] attempts to end the previous default of maximum collection and use of children's personal data on the Internet. Its attack on this default occurs in a number of ways. First, it seeks to avoid the kind of notice and consent that this Article criticizes as presenting take-it-or-leave-it terms by, for example, spelling out the elements required for notice to be valid.[193] Second, COPPA includes fair information practices beyond notice, including a right of parents to have access to any information of their children that is collected.[194]

Third, in its rule-making under this statute, the FTC has interpreted COPPA in a fashion to prevent self-regulation around a default of maximum information disclosure.[195] The final element of its attempt to shift the existing default is to target one of the most egregious kinds of maximum information disclosure. It does so by restricting Web sites' "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such an activity."[196]

COPPA also takes incremental action to reduce information asymmetries and overcome collective action problems. A burgeoning academic literature on informational approaches to regulation has examined the problem of effective communication of information, in particular about health and safety risks, to consumers. As Wesley A. Magat and W. Kipp Viscusi summarize in their path-breaking empirical research in this area, "[t]o be effective, information programs must convey information in a form that can be easily processed, and in an accurate and meaningful way that will enable individuals to make informed decisions."[197] As I have

191. The exception concerns encouraging a market for privacy enhancing technology.

192. 15 U.S.C. § 6502 (Supp. IV 1998).

193. *See id.* § 6502(b).

194. *See id.* § 6502(b)(1)(B)(iii).

195. *See* Children's Online Privacy Protection Rule; Proposed Rule, 64 Fed. Reg. 22,750 (1999) (proposed Apr. 27, 1999) (to be codified at 16 C.F.R. pt. 312). In enacting this statute, Congress also provided an important role for the FTC in issuing rules under it. *See* 15 U.S.C § 6502(b)(1). The FTC has encouraged industry to develop norms by self-regulation while, at the same time, attempted to channel these norms towards certain substantive levels. *See* 64 Fed. Reg. at 22,750. COPPA permitted a "safe harbor" for commercial Web sites that followed "a set of self-regulatory guidelines, issues by representatives of the marketing or online industries" or other approved person. 15 U.S.C. § 6503(a). If these guidelines are approved by the FTC, the Web sites will be deemed in compliance with COPPA. In issuing its rule, the FTC required that the safe harbor regulations: (1) meet the substantive standards of COPPA, (2) require Web sites under it to submit to independent auditing, and (3) provide effective incentives for compliance with the guidelines, including, in the alternative, "voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines." 64 Fed. Reg. at 22,759.

196. 15 U.S.C. § 6502(b)(1)(C).

197. WESLEY A. MAGAT & W. KIP VISCUSI, INFORMATIONAL APPROACHES TO REGULATION 17 (1992).

noted, COPPA spells out the elements of notice to be provided parents. In doing so, it takes an initial step to overcome information asymmetries by indicating the skeletal elements of acceptable notice. It thereby makes a modest effort to encourage a standardized conveying of information about processing practices.

As to collective action problems, COPPA assigns a significant role to state attorneys general by granting them the power to bring civil actions under it.[198] American information privacy law has generally relied on lawsuits and other actions by individuals to shape data protection practices and principles. Colin Bennett, a Canadian political scientist, terms such recourse to individual action, the "subject control model."[199] Bennett and other scholars have found, however, that this dependence on individual action has been largely ineffectual in the United States due to statutory hurdles, ineffective remedies, and limited damages.[200] Through its involvement of state attorney generals, COPPA may overcome this failing. Specifically, the potential payoff in favorable publicity for attorney generals is likely to encourage them to devote resources to pursuing violations of COPPA.

Beyond helping to create conditions for a functioning privacy market, the State should seek to stimulate privacy norms capable of preventing too great a rate of preference falsification. Such norms would protect private knowledge and private preferences in order to preserve independence of social expression and action. The risk otherwise is that the State, groups, and norm entrepreneurs will be excessively meddlesome; that is, they will zealously expand the areas regulated by norms or induce excessive levels of compliance with norms.

The State's approach to stimulating norms that limit preference falsification should be through: (1) encouragement of norm circumvention by facilitating attempts to bargain around objectionable norms; (2) incentives to groups to modify their behavior; and (3) construction of positive bandwagon effects.[201] My discussion of COPPA has shown the State is making attempts to increase the ability of consumers to bargain around industry's norms and creating incentives for online industry to modify its behavior. I now wish to concentrate my remarks on the State's impact on bandwagon effects.

The tendency of individuals to imitate behavior encourages conformity based on the information available through public knowledge and public discourse. One way that the State can intervene in this process is through a positive example regarding its own data processing practices. Congress

198. *See* 15 U.S.C. § 6504 (Supp. IV 1998).

199. COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 156 (1992).

200. *See, e.g.*, SCHWARTZ & REIDENBERG, DATA PRIVACY, *supra* note 51, at 205-06.

201. *See* KURAN, *supra* note 6, at 71-73, 194; E. Posner, *Inefficient Norms*, *supra* note 115, at 1726.

has already taken decisive action in this regard concerning the sale and dissemination of personal information contained in records maintained by State Department of Motor Vehicles (DMV).

In 1994 and 1999, Congress passed laws to govern use of such databases. The first statute, the Driver's Privacy Protection Act (DPPA),[202] seeks to shape the behavior of both governmental officials and private parties by creating effective fair information practices for personal information about drivers.[203] The DPPA's creation of a positive bandwagon is demonstrated by the surprisingly large number of drivers who have exercised their statutory interests under it by refusing non-mandatory use of their information that involves disclosure to marketing firms.[204]

At the end of 1999, Congress responded to a challenge to the DPPA pending before the Supreme Court on federalism grounds by enacting the second law of interest, which is the "Shelby Amendment."[205] This statute safeguards a privacy bandwagon about DMV information in two ways. First, it responds to the federalism challenge to the DPPA by tying the safeguards of DPPA to the state's acceptance of transportation funding.[206] The Shelby Amendment's second path to strengthening the privacy bandwagon is by requiring that state DMV's obtain affirmative consent, or "opting in," before release of personal records for a wide range of disclosures.[207] In contrast, the DPPA had required affirmative action for, or opting out of, these disclosures.[208] As regards personal motor vehicle information, the federal government has now taken effective action to establish and protect positive feedback for a privacy norm.[209] Its adoption first of an "opting out" and now an "opting in" norm has led to governmental publicity for both of these options.[210] In time, these State activities may stimulate greater consumer sophistication in responding to these options in other contexts.

---

202. 18 U.S.C. § 2721 (1994).

203. *See id.*

204. *See* SCHWARTZ & REIDENBERG, 1998 SUPPLEMENT, *supra* note 51, at 28-29.

205. *See* H.R. 2084-40, 106th Cong. § 350 (1999). The Supreme Court has upheld the constitutionality of the DPPA against a federalism challenge under the Tenth Amendment. *See* Reno v. Condon, 120 S. Ct. 666, 671-72 (2000). Several cases show the split that had existed among lower federal courts regarding the DPPA. *See* Condon v. Reno, 155 F.3d 453 (4th Cir. 1998), *rev'd*, 120 S. Ct 666 (2000); Travis v. Reno, 12 F. Supp. 2d 921, 925-30 (W.D. Wis. 1998), *rev'd*, 163 F.3d 1000 (7th Cir. 1998); Pryor v. Reno, 998 F. Supp. 1317, 1324-31 (M.D. Ala. 1998), *vacated*, 120 S. Ct. 929 (2000); Oklahoma v. United States, 994 F. Supp. 1358, 1359-64 (W.D. Okla. 1997), *rev'd*, 161 F.3d 1266 (10th Cir. 1998); SCHWARTZ & REIDENBERG, 1998 SUPPLEMENT, *supra* note 51, at 32-34.

206. One element of the federalism objection to the DPPA is that under it the federal government is commandeering state officials. The Supreme Court discussed and then explicitly rejected this argument in *Reno v. Condon*, 120 S. Ct. at 672.

207. *See* H.R. 2084-40, § 350(d) (amending 18 U.S.C. § 2721(b)(12)).

208. *See* 18 U.S.C. § 2721(b)(12).

209. *See* KURAN, *supra* note 6, at 186-90.

210. For a discussion of the initial experience under the DPPA, *see* SCHWARTZ & REIDENBERG, 1998 SUPPLEMENT, *supra* note 51, at 28-29.

IV. CONCLUSION

Information privacy is not a mere right of control, but a matter of line-drawing along different coordinates to shape permitted levels of scrutiny. By stimulating or discouraging different kinds of social expression and action, information privacy serves a constitutive function in society. As a result, information privacy should not create data fortresses, but shifting multidimensional data preserves that insulate personal data from different kinds of observation by different parties.

This discussion of *ends* naturally leads to analysis of *means*. In the dominant rhetoric of policy discussions about the Internet, agreement exists about how regulation is to be carried out. The dominant rhetoric favors the market, bottom-up regulation, and industry self-regulation. In this Article, I have argued, however, that this rhetoric when applied to the question of privacy in cyberspace sets up the wrong alternatives and encourages the wrong conclusions. It ignores the State's important role in shaping both a privacy market and privacy norms for information in cyberspace.

In my view, the State should concentrate its activities on two areas: (1) assisting in the creation and maintenance of the conditions for a functioning privacy market, and (2) supporting development of privacy norms that protect against too great a rate of preference falsification. The government's attention to the privacy market is of importance because of the popularity of proposals to commodify personal information. Privacy law is moving from a tort regime to a property one, but considerable reasons exist to doubt that the current privacy market functions well. As for preference falsification, access to personal data can be used by norm entrepreneurs to gain knowledge of private preferences that have been falsified under social pressures. Information privacy provides an essential way to place limits on this process. It should restrict the kind of "outing" of knowledge and preferences that is destructive of democratic community. In this fashion, information privacy can limit mission-creep by over-zealous norm entrepreneurs.

In each of these two areas, the State has a critical part to play. Regarding the privacy market, the State's first two steps should be to: (1) discourage a default of maximum information disclosure, and (2) encourage a market for privacy enhancing technology. To overcome more general failings in privacy market efficiency, the State should also: (3) reduce information asymmetries, and (4) seek ways to overcome collective action problems. Regarding privacy norms, the State's approach to stimulating norms that limit preference falsification should be through: (1) encouragement of norm circumvention by facilitating attempts to bargain around objectionable norms; (2) incentives to groups to modify their behavior; and (3) construction of positive bandwagon effects.

To conclude, I wish to offer a final example of the dominant rhetoric.

Under attack from the Justice Department, Bill Gates has decided to rally the nation to his side by talking about personal empowerment.[211] He argues that just as the computer evolved into the personal computer, the Web will evolve into the "personal Web."[212] On the so-called personal Web, customers will obtain information, goods, and services from a variety of "interactive service centers."[213] For Gates, Microsoft is the champion of the "personal" and its detractors are advocating centralized control.[214] Once again, we are being told that bottom-up is the answer. From this Article's perspective, however, all these personal devices on a personalized Internet will cause one's information to be broadcast in new ways. As a result, empowerment sometimes requires recourse to the State, which has a positive role to play in shaping the privacy market and privacy norms.

211. *See* David Bank & John R. Wilke, *Gates Pushes People's Power as Rally Point*, WALL ST. J., Nov. 15, 1999, at A3.

212. *See id*. at A18.

213. *Id*.

214. *See id*.