Title

Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices

Author

Schwartz, Paul M

Publication Date

2022-12-16

Peer reviewed

1-1-2000

Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices

Paul M. Schwartz
Berkeley Law

ARTICLES

BEYOND LESSIG'S *CODE* FOR INTERNET PRIVACY: CYBERSPACE FILTERS, PRIVACY CONTROL, AND FAIR INFORMATION PRACTICES

PAUL M. SCHWARTZ*

INTRODUCTION

An ongoing series of Internet privacy scandals has demonstrated the centrality of personal data to social, political, and economic life. As a consequence of these scandals, federal and state agencies are currently investigating the information privacy practices of Amazon.com, DoubleClick, and Yahoo!, three blue-chip Internet firms.[1] Not surprisingly, Americans are highly concerned about who has access to their personal information in cyberspace and the kinds of decisions that are made about them with that

---

* Professor of Law, Brooklyn Law School. This Article is based on my presentation at the Kastenmeier Colloquium of the University of Wisconsin Law School on April 14, 2000. It was a great honor to meet and discuss privacy law that day in Madison with Bob Kastenmeier, former Member of the U.S. House of Representatives and distinguished public servant. I would like to thank Dean Peter Carstensen for the invitation to speak at the Colloquium and David Anstaett and Jerry DeMaio of the *Wisconsin Law Review* for their interest in this Article. A grant from the Dean's Scholarship Fund of the Brooklyn Law School supported this work. I would like to thank Dean Joan Wexler for this support and for her enthusiasm for this project.

Dean Carstensen, Robert Gellman, Gregory C. Shaffer, and David Saul Schwartz provided helpful comments on my presentation on the occasion of the Kastenmeier Colloquium. This Article also benefited from the comments of Josh Bauchner, Ted J. Janger, Joel R. Reidenberg, Laura J. Schwartz, Stefanic Schwartz, Peter J. Spiro, William M. Treanor, and Benjamin H. Warnke. Finally, Larry Lessig provided an insightful and gracious critique of a previous draft of this Article.

1. *See* Lynn Burke, *A DoubleClick Smokescreen?*, (May 23, 2000) <http://www.wired.com/news/business/0,1367,36404,00.html> (privacy woes of DoubleClick); Keith Perine, *The Privacy Police*, THE INDUSTRY STANDARD, Feb. 21, 2000, at 71 (privacy woes of Amazon.com); Matt Richtel, *Yahoo Says It is Discussing Internet Privacy with the F.T.C.*, N.Y. TIMES, Mar. 31, 2000, at C5 (privacy woes of Yahoo).

At the federal level, the Federal Trade Commission has been especially active in its privacy investigations and related activities. Federal Trade Commission, *Privacy Initiatives* (visited July 18, 2000) <http://www.ftc.gov/privacy/index.html>.

For a report on activities at the state level, see *States to Turn Focus to Privacy* (June 20, 2000) <http://news.cnet.com/news/0-1007-200-2115898.html>. Regarding the ongoing investigation of the privacy practices of selective Web sites by the Michigan Attorney General, see Chris Oakes, *Michigan Warns Sites on Privacy* (June 14, 2000) <http://www.wired.com/news/politics/0,1283,36967,00.html>.

information.[2] A vigorous policy debate is now underway about the merits of different mechanisms for establishing privacy standards on the Internet.[3] Despite the increasing involvement of government agencies and rising public concern, no easy solution is in sight because information privacy raises some of the most important and difficult regulatory issues for the Internet.

In *Code and Other Laws of Cyberspace*, the most influential book to date about law and cyberspace, Lawrence Lessig makes an intriguing attempt to structure privacy rules for the Internet.[4] His two-part scheme involves: (1) assigning every individual a property interest in her own personal information, and (2) employing software transmission protocols, such as the World Wide Web Consortium's (W3C) Platform for Privacy Preferences Project (P3P), to enable the individual to control her access to Web sites based on her privacy preferences and whether the practices at a given site meet them.[5] Lessig's approach contrasts dramatically with his strong opposition on First Amendment grounds to Internet filters that seek to block children's access to pornography.[6] However, his reliance on property-based and technological solutions to privacy on the Internet is as problematic as the speech filters that he rejects.

In this Article, I use Lessig's two-part proposal for Internet privacy as a starting point for exploring the promise and perils of establishing property

---

2. As an example of this concern, a *Wall Street Journal/NBC News* poll in late 1999 asked, "Which one or two [of the following] concerns you the most about the next century?" Threats to personal privacy came in at the top of the list—ahead of terrorism, the destruction of the environment, and overpopulation. Christy Harvey, *American Opinion (A Special Report)*, WALL ST. J., Sept. 16, 1999, at A10.

As a further example of public concern about personal privacy, a *Business Week*/Harris Poll found that 89% of Americans would be uncomfortable if a Web site "[m]erged . . . browsing habits and shopping patterns into a profile that was linked to your real name and identity." *A Growing Threat*, BUS. WK., Mar. 20, 2000, at 96. Ninety-five percent of Americans would be uncomfortable about a Web site creating a profile that included real name as well as "additional personal information such as your income, driver's license, credit data, and medical status." *Id.*

These practices are common. For a good overview, see Center for Democracy & Technology, *CDT's Guide to Online Privacy* (visited July 25, 2000) <http://www.cdt.org/privacy/guide/>. See also JULIAN S. MILLSTEIN ET AL., DOING BUSINESS ON THE INTERNET § 10.02 (2000) (describing some of the ways in which personal information about individuals is collected as they browse the Internet "without the knowledge—or consent—of Internet users, and with little or no governmental oversight").

3. A headline in the *Privacy & American Business Newsletter* summed up the policy interest in privacy in Washington, DC: "What a remarkable six month period for privacy!" PRIVACY & AM. BUS. 1 (May/June 2000).

4. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) [hereinafter LESSIG, CODE].

5. *Id.* at 143-63. In a recent op-ed article, Lessig confirmed his support for this solution, Lawrence Lessig, *Technology Will Solve Web Privacy Problems*, WALL ST. J., May 31, 2000, at A26.

6. LESSIG, CODE, *supra* note 4, at 164-85.

rights in personal information. In Part I, I develop two initial criticisms of Lessig's two-step solution. First, his approach is internally inconsistent because of his rejection of speech filters. Second, I fault the underlying privacy paradigm that Lessig adopts, which is based on an idea that I term "privacy-control." In its place, I develop a normative concept of information privacy based on its constitutive function. In Part II, I raise two further challenges to Lessig's *Code*. First, propertization à la Lessig will not necessarily promote privacy (the problem of privacy market failure). Second, the Calabresi-Melamed jurisprudential framework adopted by Lessig points not to the merits of a pure property solution, but to the benefits of a mixed property-liability regime.[7]

In Part III, I propose an approach to Internet privacy centered around fair information practices (FIPs), which are rules for the fair treatment of personal information. I argue that FIPs are best understood as liability rules embedded in a compulsory licensing system. Yet, FIPs bring with them peril as well as promise. In order to prevent FIPs from becoming excessively rigid, we must consider how they can mix mandatory rules and default rules.[8] Where private bargaining about data processing is unlikely to be successful, mandatory rules should set immutable standards to prevent failure in negotiations from producing social harm. Where more potential for private bargaining exists, FIPs should establish default rules that merely set a baseline. It is important to recognize, however, that individuals may also face problems in negotiating on their own behalf in these areas. Under such circumstances, the default rule generally should be an "opt-in" rule, to insure that consumer ignorance or inaction will result in non-disclosure of personal data rather than the opposite. This approach places the onus on Internet data processors to convince consumers to share personal information with them.

---

7. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

8. For previous use by privacy scholars of the concept of default and mandatory rules, see Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. LAW REV. 1609, 1671-72 (1999) [hereinafter Schwartz, *Privacy in Cyberspace*]; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246-65 (1998); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 53-56 (1997) [hereinafter Schwartz, *Privacy Economics*]; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2402 (1996).

For a general discussion of default and mandatory rules in the context of cyberspace, see Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1209-11 (1998). For analysis of the function of these rules in "Real Space," that is, the offline world, see Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 730-32 (1992) [hereinafter Ayres & Gertner, *Optimal Choice*]; Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989) [hereinafter Ayres & Gertner, *Default Rules*].

I. LESSIG ON PRIVACY

Lawrence Lessig is the renaissance man of cyberspace law. Beyond the wide range of his prolific scholarship in law reviews, he has served as an expert in two of the most important lawsuits yet to concern cyberspace, the Microsoft antitrust case and the Napster copyright case.[9] In all of these endeavors, Lessig has combined a computer scientist's awareness of software and silicon with a law professor's knowledge of legal theory and practice. Even beyond these achievements, Lessig has written *Code and Other Laws of Cyberspace* which, less than a year after its publication, is the most influential book published about law and cyberspace.[10] *Code* offers an impressive display of Lessig's insights on the open source movement, norm theory, constitutional law, and intellectual property. Yet, when it comes to information privacy, his proposals in *Code* are highly problematic.

This section sets out Lessig's analysis of information privacy on the Internet. It examines and contrasts his two-part plan for privacy with his ideas regarding limits on speech in cyberspace, concluding with a critique of Lessig's idea of privacy-control and the presentation of a contrasting proposal concerning the constitutive function of information privacy.

A. Prologue: Two Risks to Privacy

In *Code*, Lessig describes the widespread electronic surveillance of individuals and their personal data that takes place on the Internet as well as in the offline world. He points, for example, to the extent to which data collection has become "the dominant activity of commercial Web sites."[11] This behavior is different than surveillance in previous eras—at the time of the founding of the United States, for example—because "the technolog[y] of monitoring—their efficiency and their power—are different."[12] Lessig contrasts the fallibility of gossipy neighbors with the perfection of machines, whether "videotape, a toll booth's electronic records of when you entered and when you left, a credit card system's endless collection of data about your purchases, or the telephone system's records of who you called when and for how long."[13]

---

9. Lessig's Microsoft Brief is posted at: <http://cyber.law.harvard.edu/works/lessig/AB/abd9.doc.html> (visited July 16, 2000). Lessig's Napster Brief is posted at the UCLA's Institute for Online Studies, which maintains a Web site devoted to this litigation. <http://www.gseis.ucla.edu/iclp/napster.htm> (visited July 16, 2000).

10. *See, e.g.*, Henry H. Perritt Jr., *Lawrence Lessig, Code and Other Laws of Cyberspace*, 32 CONN. L. REV. 1061 (2000) (Lessig's *Code* will change "the way people think about the relationship between information technology and the law.").

11. LESSIG, CODE, *supra* note 4, at 153.

12. *Id.* at 151.

13. *Id.* at 150-51.

In Lessig's view, the modern transformation of data collection is problematic for two reasons. Drawing on the conventional concept of information privacy as protecting a right to control one's personal data, or "privacy-control," Lessig points to (1) the problem of manipulation, and (2) the threat to equality.[14] The first point is easily summarized; the second requires somewhat more effort.

The first risk, the manipulation of individuals, occurs because "profiles will begin to normalize the population from which the norm is drawn."[15] In other words, initial examples of our behavior will be used to press us into a mold. Lessig writes, "The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again."[16] As this Article will discuss in more detail, the risk is one to autonomy.

As to the second risk, profiling is said to be dangerous because it threatens an important American principle regarding a society without hierarchy. Here, Lessig draws on the work of historian Gordon Wood concerning the development of an American identity in the decades leading to and culminating in the revolutionary era.[17] An American was meant to be someone who was free from traditional hierarchies of social rank and the special privileges associated with these distinctions. Pressing his mental "fast forward" button and skipping forward two centuries, Lessig argues, "[p]rofiling changes all this."[18] According to Lessig, modern data collection decreases the amount of equality in a society. Lessig is worth quoting at some length on this point: "An efficient and effective system for monitoring makes it possible once again to make these subtle distinctions of rank. Collecting data cheaply and efficiently will take us back to the past."[19] Lessig's specific example is more than slightly anticlimactic, however, as he turns out to be worried about frequent flier miles and similar programs that allow companies to distinguish among classes of consumers.[20]

Lessig's analysis of the impact of profiling on equality concludes with a modest retreat and a slight, albeit useful, change of subject. Lessig first admits that the value of equality may now be "relatively weak in American life" (the modest retreat), but then stresses that "the emerging technology of

---

14. *See id.* at 154.
15. *Id.*
16. LESSIG, CODE, *supra* note 4, at 154.
17. *Id.* at 154-55. GORDON WOOD, THE RADICALISM OF THE AMERICAN REVOLUTION 4-6 (1992).
18. LESSIG, CODE, *supra* note 4, at 155.
19. *Id.* at 155. For a similar argument, namely, how the "commercial pressure to identify individuals by their demographic characteristics reinforces many of the schisms in society," see Jonathan GS Koppell, *On the Internet, There's No Place to Hide,* THE INDUSTRY STANDARD 124, 128 (June 19, 2000).
20. LESSIG, CODE, *supra* note 4, at 155.

profiling" reveals "a conflict of values" (the change in subject).[21] Technology, or in Lessig's terminology, "code," changes the relative costs and benefits of undermining equality of social status and recreating systems of status.[22] Lessig's great insight is that a central fashion in which regulation takes place in cyberspace is through code, that is, through technological configurations and system design choices.[23] Relating this insight to privacy, Lessig observes, "Whereas before there was relative equality because the information that enabled discrimination was too costly to acquire, now it pays to discriminate."[24] It pays to discriminate because code makes it possible and profitable to draw new distinctions among customers and other persons.

The question for Lessig then becomes how code can be altered in a "more effective way to control what we collectively do" about privacy.[25] Code is malleable, and Lessig's solution for privacy on the Internet centers on the shaping of technological configurations to reach the right results.

B. The Two-Step Solution: Of Code and Property Law

Lessig divides his two-part solution between its technological and legal elements. Returning to the idea of privacy-control, he proposes that we search for a way to give people more choice about how their personal data are used. As he writes, "The standard response to this question of data practices is choice—to give the individual the right to choose how her data will be used."[26] At this juncture, one might imagine protecting choice by enacting a law that requires Web sites to engage in a range of privacy-favoring behavior, a set of rules that legal scholars call "fair information practices."[27] As an initial part of this regulation, one might also imagine a requirement that Web sites provide notice to visitors by disclosing their planned use of data. Lessig discusses and rejects the notice requirement, however, and instead focuses on the negative consequences of a sole reliance on privacy statements.

---

21. *Id.* at 156.

22. *Id.*

23. For a related analysis, see Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 556 (1998). For an analysis of the impact of technological configurations within the context of choice-of-law in cyberspace, see Goldsmith, *supra* note 8, at 1213-15.

24. LESSIG, CODE, *supra* note 4, at 156.

25. *Id.* at 160.

26. *Id.*

27. The idea of fair information practices has been present in information privacy law and policy since the era of mainframe computers in the 1970s. For a description of early proposals regarding fair information practices, see THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 14-15, 500-02 (1977) [hereinafter PRIVACY STUDY COMM'N, GENERAL REPORT]; DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306-07 (1989). For a more recent governmental discussion of a somewhat different set of fair information practices, see FEDERAL TRADE

A major weakness with privacy statements, as Lessig wisely observes, is that "[n]o one has the time or patience to read through cumbersome documents describing obscure rules for controlling data."[28] Instead of text, Lessig argues that we should have "code" do the reading for us. He writes, "What is needed is a way for the machine to negotiate our privacy concerns for us, a way to delegate the negotiating process to a smart agent—an electronic butler . . . who knows what we . . . [do or] do not like."[29] Elsewhere in *Code*, however, Lessig rejects the electronic butler in a chapter concerning the First Amendment in cyberspace.[30] Regarding privacy, nevertheless, his preferred solution is to write software and make system design choices that establish and activate this butler who will then negotiate privacy protections on our behalf.[31]

Lessig views a machine-to-machine protocol as necessary to allow an individual's browser and a selected Web site to negotiate privacy standards in a seamless fashion. The electronic butler is a customized part of the individual's browser that is enabled to respond to the privacy protocol. Here is how Lessig envisions this device in operation:

> The user sets her preferences once—specifies how she would negotiate privacy and what she is willing to give up, and from that moment on, when she enters a site, the site and her machine negotiate. Only if the machines can agree will the site be able to obtain her personal data.[32]

The electronic butler will carry out this task in a fraction of a second. Although Lessig's proposal may strike some readers as futuristic, it does not belong to the world of science fiction. Indeed, the idea of the privacy protocol is influential not only among academics, but also among those who are shaping the Internet's evolving infrastructure. The World Wide Web Consortium's P3P Project is moving beyond its beta versions, and

---

COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7-12 (1998) [hereinafter FTC, PRIVACY ONLINE]. As I have argued elsewhere, fair information practices "are the building bloeks of modern information privacy law." Schwartz, *Privacy in Cyberspace, supra* note 8, at 1614.

For other analyses of fair information practices, see Schwartz, *Privacy Economics, supra* note 8, at 56-67 (1997); Paul M. Schwartz, *Privacy and Participation*, 80 IOWA L. REV. 553-64 (1995) [hereinafter Schwartz, *Participation*]; Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 195-202 (Philip E. Agre & Marc Rotenberg, eds., 1997).

28. LESSIG, CODE, *supra* note 4, at 160.
29. *Id.*
30. *See id.* at 138-40, 176-85.
31. *See id.* at 160-61.
32. *Id.* at 160.

Microsoft's Internet Explorer and Netscape's Communicator are either already enabled for this application or soon will be.[33]

At this point, only one step remains in Lessig's two-part solution for privacy: What, if anything, can we do as a society to ensure that "privacy code" is actually utilized? In Lessig's judgment, the task is to create a privacy default. In the absence of such a pro-privacy tilt, people may lose their personal information without realizing it is being taken. In other words, individuals must have not only the ability to negotiate easily over privacy rights, but also an entitlement to privacy if they fail to take any action.[34] At this moment, Lessig discloses the second part of his plan: to create a legal property right in personal information. An architecture like P3P will facilitate the necessary negotiations, but the purpose of the law should be to create a rule that says negotiations must occur. Lessig argues that this is property's purpose: "it says to those who want, you must negotiate before you take."[35]

In reaching this conclusion, Lessig relies upon the foundational work of Guido Calabresi and Douglas Melamed regarding property and liability rules. In their seminal article, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, Calabresi and Melamed explored a wide range of differences in the protection of legal rights through these different regimes.[36] Lessig draws on only one of these distinctions, however, which is that a property regime sets the cost of violation *ex ante* while a liability regime sets it *ex post*.[37] For example, the sale of one's automobile generally triggers a property regime; an automobile owner can decide whether or not to sell *before* any exchange of property takes place and set her own price. In contrast, an automobile accident triggers reliance on liability rules by leading a jury to assess the loss to the harmed individual *after* the fact.

Compared to an automobile accident, any alternative is likely to seem attractive. Yet, Lessig reveals his underlying goal when he hints at the Pareto-optimal result of a recourse to privacy-through-property: "Such a regime gives us confidence that if a trade occurs, it will be at a price that makes neither party worse off."[38] By assigning the individual a property interest in her personal information, Lessig protects "both those who value

33. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Working Draft* (Sept. 15, 2000) <http://www.w3.org/TR/2000/WD-P3P-20000915/>. A W3C-sponsored demonstration of the P3P protocol in New York led to criticism from privacy activists, who denounced it as "Pretty Poor Privacy" as well as some praise from the Clinton administration. Glenn R. Simpson, *Clinton Supports Move to Protect Consumer Privacy on the Internet*, WALL ST. J., June 22, 2000, at B14; Chris Oakes, *Privacy Protocol Lauded, Sort Of* (June 22, 2000) <http://www.wired.com/news/politics/0,1283,37145,00.html>.

34. LESSIG, CODE, *supra* note 4, at 160.

35. *Id.* at 160-61.

36. *See* Calabresi & Melamed, *supra* note 7, at 1092-99.

37. *See id.* at 1105; LESSIG, CODE, *supra* note 4, at 160-61.

38. *Id.*

their privacy more than others and those who value it less, by requiring that someone who wants to take a given resource must ask."[39] The obligation to reach a market-clearing price in personal data will stimulate investment in privacy software and the use of electronic butlers. Thus, property in personal information is intended to block courts, juries, and even legislatures from deciding the value of privacy interests, and, best of all, to stimulate trade in information in general and use of privacy protocols in particular.

C. An Internal Critique: The First Amendment in Cyberspace

Having set out Lessig's privacy proposal, we next examine the extent to which his dependency on property rules for privacy contradicts his opposition on First Amendment grounds to Internet filters for speech. A reliance on technological and property-based solutions to privacy on the Internet is as problematic as the speech filters that Lessig rejects. The problematic aspects of privacy filters are revealed once we put them in a social context. One example, the so-called "blinking twelve" problem of user interfaces, will help shed light on Lessig's construct and its meaning for personal privacy on the Internet.

1. PICS VERSUS P3P

When speech and the values protected by the First Amendment are at stake, Lessig objects in strong terms to the use of filters. Specifically, he opposes the Platform for Internet Content Selection (PICS) which, like P3P, is a proposed protocol for rating and filtering content on the Internet.[40] In the context of privacy, however, Lessig's electronic butler reacts to coded assertions about privacy practices. The idea behind PICS and more recent and competing proposals to rate speech on the Web is much the same. In the words of Yale Law School's Information Society Project, a technological solution is "to place choice in end users about what and whether to filter."[41] As R. Polk Wagner observes of this technology, "The objective is to prevent certain materials or content from arriving in places where they are not wanted."[42]

PICS divides the process of filtering into two parts—first, PICS labels, or rates content; second, PICS sorts the content according to those labels.[43]

---

39. *Id.*

40. *Id.* at 177.

41. J.M. Balkin, Beth Simone Noveck & Kermit Roosevelt, *Filtering the Internet: A Best Practices Model* (Sept. 15, 1999) <http://www.law.yale.edu/infosociety/filtering_report.html>.

42. R. Polk Wagner, *Filters and the First Amendment*, 83 MINN. L. REV. 755, 760 (1998).

43. *See* LESSIG, CODE, *supra* note 4, at 177.

Lessig considers the technology that carries out the sorting as viewpoint neutral. He declares that users can pick the ratings they want—those of the Christian right or the Atheist left.[44] Lessig's objection lies elsewhere; for filtering protocols to work, speech on the Net must first be rated, and it is this practice that disturbs him deeply. Despite his favorable reaction to P3P, Lessig is strongly against PICS, which he memorably described in *Wired* magazine as "the devil."[45]

In *Code*, Lessig explains his distaste for PICS, this second software protocol, by returning to the idea of the cyber-assistant. "What happens," Lessig writes, "if everyone can, in effect, have a butler?"[46] For purposes of our discussion, we can call this butler the "Cyber-Jeeves."[47] When used to filter speech, the "Cyber-Jeeves" will have disastrous social consequences for two reasons: (1) its perfection allows *self-censorship*, and (2) its perfection allows *outside censorship*. The self-censorship danger arises because rating speech allows people to cut themselves off from what they do not want to read or see.[48] They can refuse to become aware of social issues that disturb them, such as homelessness, or political ideas with which they might disagree. Underlying this argument, of course, is the view, perhaps best articulated by Owen Fiss, of the centrality of the First Amendment to furthering a robust public debate on important issues.[49]

As for the danger of outside censorship, there are two primary ways that PICS makes it easier for organizations in both the private and public sectors to keep track of our online behavior. First, the PICS protocol allows filters to be imposed at any point in the distributional chain, including far upstream from intended recipients. As Lessig writes:

> Nothing in the design of PICS prevents organizations that provide access to the Net from filtering content as well. Filtering can occur at any level in the distributional chain—the user, the company through which the user gains access, the ISP, or even the jurisdiction within which the user lives.[50]

---

44. *See id.*

45. Lawrence Lessig, *Tyranny in the Infrastructure*, WIRED 5.07 (July 1997) <http://www.wired.com/wired/5.07/cyber_rights.html>.

46. LESSIG, CODE, *supra* note 4, at 180.

47. This term is my own, not Lessig's. For an introduction to the original Jeeves, see P.G. WODEHOUSE, THE CODE OF THE WOOSTERS (Penguin Books 1999) (1937). Wodehouse first invented this character in the 1920s; as for the Internet search company, "askjeeves.com," it came along later. *See* askjeeves.com (visited July 19, 2000) <http://www.askjeeves.com/docs/about/>. By the term "Cyber-Jeeves," I allude only to the original Jeeves.

48. LESSIG, CODE, *supra* note 4, at 180.

49. *See* OWEN M. FISS, THE IRONY OF FREE SPEECH 3 (1996) (free speech is important "because it is essential for collective self-determination").

50. LESSIG, CODE, *supra* note 4, at 178.

Second, and more dangerously, such filtering can be invisible. With nothing in the design of PICS requiring that such filters announce themselves, some outside party, whether in the private or public sector, may secretly use PICS to track an individual's cyber-activities.[51]

To his credit, Lessig admits the contradiction between his opposition to PICS and his support for P3P. Yet, he addresses this tension only briefly and is incapable of resolving it. Lessig begins with a rhetorical flourish by noting that "an annoying skeptic" would wonder how he can "oppose one yet favor the other."[52] Lessig answers that "the values of speech are different from the values of privacy; the control we want to vest over speech is less than the control we want to vest over privacy."[53] With respect to speech, he believes that it is desirable to disable some of the possible controls over content. In his words, "A little bit of messiness, or friction, is a value, not a cost."[54] In other words, Lessig views both PICS and P3P as potentially powerful technologies for controlling speech or privacy, respectively. Lessig endorses different regimes: one in which speech will not be very well controlled, a world of "messiness, or friction"; and another in which privacy will be very well controlled (i.e., protected) by the concerned individual.

Lessig's acceptance of different levels of control for privacy and speech on the Internet is a consequence of his fundamentally different approaches to these two topics. Lessig anchors his analysis of filtering speech in a social context, but makes his comments about privacy in a social vacuum.[55] In Lessig's analysis of speech values, some people will use filters to prevent themselves from encountering unpleasant topics. They will structure their time on the Internet to avoid random encounters with anything or anyone that might change their existing views. In his analysis of speech in cyberspace, privacy even emerges as a concern. Once PICS is in place and speech is rated, people will have to fear the prying eyes of others observing the ratings

51. *See id.* Rather than the filtering of speech on the Internet, Lessig would prefer a "zoning" of cyberspace through browsers enabled for "kids-mode browsing." *Id.* at 176. This approach would permit access to everyone "except those who identify themselves as children." *Id.* For more on how such "zoning" would function, see Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model,* 98 MICH. L. REV. 395 (1999).

52. LESSIG, CODE, *supra* note 4, at 181.

53. *Id.* at 182.

54. *Id.*

55. Marc Rotenberg has made a similar criticism of *Code* in noting how this book's discussion of privacy ignores much of the *history* of privacy law in the United States. Marc Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy*, STAN. TECH. L. REV. ¶ 26-39 (fortheoming 2000).

of what they look at and read.[56] Lessig's analysis astutely captures problems of speech in our world.

In Lessig's analysis of privacy and its value, in contrast, a move to a property regime will only make things better. According to Lessig, propertization will stimulate investment in and use of technology and thereby generate an optimal amount of privacy. This investment will take place because property will require negotiations before personal data are taken. The underlying motto of this part of *Code* can be simply stated: "Better Living through Technology." This credo is undercut, however, as soon as privacy, like speech, is put in a more concrete context. At this juncture, we will look at one component of this setting: the "blinking twelve" problem of user interfaces.

2. THE "BLINKING TWELVE" PROBLEM

In our digital world, user interfaces are ubiquitous and the design of good ones a complex art. As Neal Stephenson writes, "every little thing—wristwatches, VCRs, stoves—is jammed with features, and every feature is useless without an interface."[57] Yet, consumers frequently do not know certain features exist, and, for those who do, the bother of learning about them may appear greater than any potential benefit. This ignorance, intentional or not, leads to the "famous blinking 12:00 that appears on so many VCRs."[58] The "blinking twelve" occurs on the VCR because the owner of the device never bothered to set the correct time. Some households have chosen a low-tech solution to this difficulty of the "blinking twelve": use of black tape to cover the readout of the VCR's clock function.

The "blinking twelve" problem of personal data on the Internet has two facets. The first is the extreme difficulty of designing user interfaces.[59] The danger is that the P3P interface—like the wristwatches, VCRs, and stoves that Stephenson discusses—will become another device that we never master or even use. Many or even most people will never comprehend the nature of the different graphical computer interfaces that are all that stand between them and the surrender of their personal data.

---

56. *See* LESSIG, CODE, *supra* note 4, at 179 ("If content is labeled, then it is possible to monitor who gets what without even blocking access.").

57. NEAL STEPHENSON, IN THE BEGINNING WAS THE COMMAND LINE 67 (1999).

58. *Id.* at 68 (emphasis removed). Stephenson observes that the "blinking 12:00 itself is slowly disappearing from America's living room" as interfaces with the VCR improve through the advent of onscreen programming. *Id.* Yet, "[t]he blinking twelve problem has moved on to plague other technologies." *Id.* As a result, when "[c]omputer people" discuss "the blinking twelve," they usually aren't talking about VCRs." *Id.* The problem of interface design appears and reappears as we try to do more ambitious things with technology.

59. For a meditation on the meaning and difficulties of interface design, see STEVEN JOHNSON, INTERFACE CULTURE: HOW NEW TECHNOLOGY TRANSFORMS THE WAY WE CREATE AND COMMUNICATE 223-30 (1997).

The second aspect of the "blinking twelve" problem is that the design of P3P, or any other filtering option for privacy, requires simplifications and glosses to be made. We seek interfaces for exactly these kinds of assistance; this highly understandable desire need not have sinister consequences. As Stephenson writes, "the desire to have one's interactions with complex technologies simplified through the interface . . . is natural and pervasive—presumably a reaction against the complexity and abstraction of the computer world."[60] To return to our electronic butler, the Cyber-Jeeves will negotiate with sites regarding their privacy policies based on simplified instructions created by someone other than his putative master. As a result, code plus property may not only facilitate trading personal information on bad terms, but, more broadly, will shift power to those who decide how important shortcuts are to be taken.[61] Property plus code may turn into a powerful means for generating an unsatisfactory level of privacy.

Rather than thinking merely about individuals trading their personal information wisely or foolishly, however, we must consider the larger implications of these exchanges. For better or worse, the trade in personal data will shape the society in which we live. Evaluating the social costs of personal data use, however, requires a normative vision of privacy, to which we now turn.

D. Privacy is Not *Control*

Lessig considers the lack of privacy on the Internet to threaten autonomy and equality.[62] Although some of his analyses of these dangers are correct, it is not the case with his locating the solution in a right of control. In Lessig's view, we must search for a way to give people more choice about the use of their personal data. As he writes, "The standard response to this question of data practices is choice—to give the individual the right to choose how her data will be used."[63] This section first challenges Lessig's concern with equality—our real worry should be about democratic opportunity. Although Lessig presents a credible analysis regarding the Internet's threat to autonomy, his idea that privacy protects a right of individual control falls short; in its place, this section outlines a concept of constitutive privacy.

---

60. STEPHENSON, *supra* note 57, at 131. He adds, "Computers give us more choices than we really want. We prefer to make those choices once, or accept the defaults handed to us by software companies, and let sleeping dogs lie." *Id.*

61. In fact, Lessig's central concept of "code" points to the malleability of the Internet and the importance of the shaping of technology. LESSIG, CODE, *supra* note 4, at 5-13. Yet, Lessig also seems to neglect the critical role of democratic institutions in shaping Internet privacy. *See* discussion *infra*, Part III.B.

62. *See supra* text accompanying notes 14-24.

63. LESSIG, CODE, *supra* note 4, at 160.

1. FROM EQUALITY TO DEMOCRATIC OPPORTUNITY

Lessig worries about customer programs, such as those involving frequent flier miles, which he uses to demonstrate how data processing on the Internet will destroy an American identity based on a society without hierarchy.[64] This example is unconvincing; such consumer programs are socially and economically useful attempts by companies to differentiate their products and services from those of their competitors by rewarding their loyal customers.[65] Lessig's mistrust of these programs is as unmerited as opposition to them in Germany, where the law prohibits discounts, rebates, and similar incentives as creating unfair competitive advantages for firms.[66] In fairness to Lessig, however, the frequent flyer example may only be intended by him as a general example of the increased capacity to discriminate and no more.

Beyond its possible market-enhancing function, commercial data use can promote a specific and significant kind of equality in the United States by furthering equal access to commercial and professional opportunities. Where Lessig sees only evil hierarchy, there exists the potential for heightening economic opportunity. As Fred Cate notes, the financial industry's ability to market individualized products and services "democratizes" opportunity in the United States.[67] Cate writes, "In the United States, you get credit, insurance, investment opportunities, in fact, a wide range of financial services, based on your record, not your name or how long you have known your banker or broker."[68] This sounds, if anything, like Gordon Wood's account of Nineteenth Century America—a society of "many scrambling, ordinary, and insignificant people" in equal competition with each other.[69] Secured credit offers a specific example of how information use has been part

---

64. *Id.* at 155.

65. One best-selling marketing guide explains these programs as carrying out "loyalization." DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE: BUILDING RELATIONSHIPS ONE CUSTOMER AT A TIME 108 (1993). The idea is "to make loyal customers more loyal, increasing an airline's share of customer on an individual basis." *Id.*

66. Lufthansa even faces legal action in Germany due to its introduction of a credit card that rewarded eonsumers with frequent flier miles for their purchases. *See Lufthansa Card wird abgemahnt*, DER TAGESSPIEGEL, June 17, 2000, at 21. For that matter, German law also forbids discounts below three percent of the original price. *See* Rabattgesetz, §2, Gesetz über Preisnachlässe (Rabattgesetz), v. 25.11.1933 (RGBl. I S. 1011) in der Fassung der Änderungen, v. 25.7.1994 (BGBl. I S. 1688); Zugabeverordnung, § 1, Zugabeverordnung in Deutschland, v. 9.3.1932 (RGBl. I S. 121) in dcr Fassung der Änderung, v. 25.7.1994 (BGBl. I S. 1688). For a report on a poll that found many retailers in Germany were violating these restrictions by offering deeper discounts and rebates to their customers, see *Preiskreig am Verkaufstresen*, FOCUS 25/2000, at 252.

67. FRED H. CATE, PERSONAL INFORMATION IN FINANCIAL SERVICES 5 (2000).

68. *Id.* For similar arguments by Professor Cate, see FRED H. CATE, PRIVACY IN THE INFORMATION AGE 28-31 (1997); Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 886-88 (2000).

69. WOOD, *supra* note 17, at 359.

of this process; it has played an important role in opening up financial opportunity in America.[70] Secured credit relies on public filings of liens in the relevant jurisdiction to inform lenders about risk regarding borrowers.[71] In the Information Age, democratic opportunity now more generally relies on broader access to information by a wider range of institutions and individuals than ever before.

Although frequent flier programs are market-enhancing and the private sector's data use can heighten access to economic opportunity, information processing can also, if used improperly, squelch democratic opportunity. As an example, consider the emerging practice of "Weblining," which is similar to "red-lining" in the real world. Weblining, as *Business Week* tells us, is the "Information Age version of that nasty old practice of redlining, where lenders and other businesses mark whole neighborhoods off-limits."[72] By combining far-flung threads of personal data, including data about one's ethnic background or religion, into profiles that are used to sort people into categories, Weblining segments our data profiles, and determines the price that we pay, the services we obtain, and our access to new products and information.[73] Weblining sometimes even relies on so-called "neural networks," which are digital systems that evolve over time in a fashion both independent of their developers and impossible to predict.[74]

The danger is that Weblining will hinder or even reverse the democratization of opportunity that Cate advocates. It goes far beyond the existing model for secured credit; it can be used to restrict economic and informational possibilities for different groups and for individuals in a fashion that reflects and reinforces existing prejudices and mistaken beliefs. It may be possible, in fact, to assimilate to this analysis Lessig's own point about equality and the ability of commercial entities to discriminate; I do not wish to overstate our possible differences on this point. As *Business Week* warns,

---

70. If anything, as scholars have asked in the "ubiquity puzzle," the question is why secured credit is not even more prevalent. Barry Adler, *Secured Credit Contracts*, 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 405, 407 (Peter Newman, ed. 1998) [hereinafter DICTIONARY OF ECONOMICS & LAW].

71. *Id.* at 405. For an empirical study of secured credit that finds that it not only lowers the cost of lending "by increasing the strength of the lender's legal right to force the borrower to pay, but also by enhancing the borrower's ability to give a credible commitment to refrain from excessive future borrowing and by limiting the borrower's ability to engage in conduct that lessens the likelihood of repayment," see Ronald J. Mann, *Explaining the Pattern of Secured Credit*, 110 HARV. L. REV. 625, 683 (1997).

73. LESSIG, CODE, *supra* note 4, at 3-4.

74. *Id.* at 4.72. On redlining, see Peter P. Swire, *The Persistent Problem of Lending Discrimination: A Law and Economics Analysis*, 73 TEX. L. REV. 787, 816-18 (1995). On Weblining, see Marcia Stepanek, *Weblining*, BUS. WK. at 2 (Apr. 3, 2000) <http://www.businessweek.com/2000/00_14/b3675017.htm>.

73. *See id.*

74. *Id.*

"Weblining may permanently close doors to you or your business."[75] Moreover, at a certain point, Weblining and similar activities will call into question autonomous decision-making.

2. AUTONOMY

As Lessig notes, there is a risk when "[t]he system watches what you do" and "fits you into a pattern."[76] This risk is particularly acute in the online world where a person can only "move" about by means of a series of digital commands that her computer sends to HTTP servers.[77] Put more generally, the Internet is an interactive telecommunications system, which means that any computer attached to it does not merely receive information but also transmits it. These digital transmissions, whether sent through e-mails, file attachments, or the clickstreams of our mice, all generate personal information about us. Social life on the Internet creates a finely grained data map of our interests, our beliefs, and our interpersonal relationships. Yet, the ability to participate in social life, whether in cyberspace or elsewhere, depends on the underlying communicative capacity of individuals.[78]

Where George Orwell in his dystopian fantasy *1984* feared the "Thought Police," we face the rise of a "Cyber-Thought Police."[79] Whether located

---

75. *Id. Business Week* does not explain, however, why economic self-interest will fail to correct this practice. One explanation is that such behavior will not be punished in the market. As Cass Sunstein has pointed out, market failure is promoted by the frequent inability of directly affected parties and concerned third parties to create countervailing pressures. CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 153-55 (1997).

76. LESSIG, CODE, *supra* note 4, at 154.

77. For a cogent description of the technical issues, see Kang, *supra* note 8, at 1223-29.

78. For Robert Post's eloquent expression of this view, see ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 51-88 (1995); Robert C. Post, *The Social Foundations of Privacy*, 77 CAL. L. REV. 957 (1989) [hereinafter Post, *Social Foundations*]. For a related explanation of the tie between privacy and "the practice of self-determination on the part of free and equal citizens," see JÜRGEN HABERMAS, FAKTIZITÄT UND GELTUNG 446-47 (1992) [hereinafter HABERMAS, FAKTIZITÄT]; JÜRGEN HABERMAS, BETWEEN FACTS AND NORMS 368-70 (William Rehg trans., MIT Press 1996) (English translation of FAKTIZITÄT UND GELTUNG) [hereinafter HABERMAS, FACTS & NORMS]. *See also* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 463-66 (1995); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734-36 (1987).

79. GEORGE ORWELL, 1984, at 2 (Penguin Books 1999) (1949). In this novel, Orwell imagined a machine called the "telescreen." This omnipresent device broadcasted propaganda on a nonstop basis and allowed the state officials, the "Thought Police," to observe the populace. *Id.* at 23. Orwell writes:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork . . . . You had to live—did live, from habit

within the public or private sector, the Cyber-Thought Police are potentially plugged into any wire at any time. The threat to autonomy is through a coercive influence that takes over, or subtly and persistently colonizes, a person's thinking process.[80] Protection of the capacity for self-determination requires a setting of limits on the collection of personal data, but it does not call for privacy-control as a central means of achieving these limits.

3. AGAINST PRIVACY-CONTROL AND TOWARDS CONSTITUTIVE PRIVACY

How are we best to counter the threats to equality of opportunity and to autonomy? Lessig asserts that it should be done through a right of personal control over information. There are two problems with privacy-control. First, this individualistic privacy paradigm ignores the critical harms to decision-making that can take place through data collection. To his credit, Lessig does notice that the widespread collection of data on the Web raises a "collective concern" about the impact "on a community."[81] His use of the principle of privacy-control, however, retreats to a belief in a narrower condition that Avery Wiener Katz has termed "normative individualism."[82] Lessig's own form of normative individualism is self-reliant data control; property plus code is intended to stimulate more choice about privacy on the Web. Yet, a person's control of her personal information may itself be hollowed out by the circumstances of data processing and other conditions that shape and restrict choice. Indeed, the meaning that we attribute to individual autonomy is itself strongly shaped by the actual means by which personal data are processed.[83]

---

that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinised.

Id. at 2.

80. For an elaboration of this argument, see Schwartz, *Privacy in Cyberspace, supra* note 8, at 1653-58.

81. LESSIG, CODE, *supra* note 4, at 154.

82. FOUNDATIONS OF THE ECONOMIC APPROACH TO LAW 36 (Avery Wiener Katz ed. 1998).

83. In this fashion, a dominant trend in personal use in cyberspace can slowly 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 habituation[s] or acculturation that is as subtle as it is profound." JERRY L. MASHAW, GREED, CHAOS, AND GOVERNANCE 3 (1997). In cyberspace, in time, a decision to go online and surf the Web may itself be considered as a decision to accept all use anywhere of one's personal data that this activity generates. Or, as Esther Dyson, a leading guru of information technology and Acting Chairperson of the Internet Corporation for Assigned Names and Numbers (ICANN), has observed, "It'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). With wishful thinking, Dyson adds, "we may all become tolerant if everyone's flaws are more visible." *Id.* at 217.

Privacy-control seeks to place the individual at the center of decision-making about personal information use, but it can instead help us to accept smoke screens that disguise information privacy practices and lead to choices that are bad for individuals and for society. Lessig's technological solution, privacy-code, which relies on measures such as P3P, is likely to form such a smoke screen. I have already pointed to the "blinking twelve" problem as a weakness in privacy-code, and I will discuss a further difficulty with P3P, namely, its creation of meta-data about privacy preferences.[84] My point is *not* that code for privacy is doomed to inevitable failure, but that Lessig's normative individualism relies on individual control of personal information to reach optimal levels of privacy, and significant reasons exist to consider this solution as unlikely in the current market for personal information.

The second problem with privacy-control is that society at times will wish for *less* control rather than *more*. In other words, the central response cannot be choice, a right to choose how one's data will be used, because relations with others require not only information privacy, but outside access to data.[85] The danger of choice as a central response is that it may lead us to view the shaping of rules for sharing information as unimportant details. Quite to the contrary, the terms on which personal information is transferred to and used by third parties are not mere exceptions to a regime of privacy-control, but a core task for information privacy law. Personal data often involve a social reality that is external to the individual; as a result, the optimal utilization of this information will not be reached by allowing maximum individual control or by the starting point of propertization.[86] Lessig skirts this important issue by failing to elaborate on the process by which he would differentiate between that personal information which should be treated as property and that which should not.[87] Without the proper limits on propertization and the proper process for deriving them, however, privacy-control would have at least three unfortunate results.

First, governmental access to personal information is required in many instances for administrative agencies to evaluate one's eligibility for different kinds of public benefits.[88] Second, public accountability and public order place limits on individual control because a democratic community requires

---

84. *See infra* Part II.A.

85. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 38-39 (1996).

86. For a similar conclusion regarding the use of personal medical information, see Schwartz, *Privacy Economics*, *supra* note 8, at 41.

87. LESSIG, CODE, *supra* note 4, at 162-63.

88. The State collects and processes personal data to create and maintain public services and public goods, to manage those who work for it, and to regulate human behavior. An administrative state now plays an essential role in safeguarding the conditions for the social, political, and physical environment in the United States. For a description of the transformation of the government's role, see generally Bruce Ackerman, *Constitutional Politics/Constitutional Law*, 99 YALE L.J. 453, 488-515 (1989).

a critical assessment of persons and events. This process frequently requires outside access to personal information to evaluate speakers at different kinds of public fora and town squares. The First Amendment plays an important role in safeguarding this kind of access to information.[89] Finally, economic efficiency requires outside access to certain kinds of records such as land ownership records.[90] Individuals have not traditionally been permitted control over these data, and such a solution would result in this information being removed from the public domain in a piecemeal fashion and with negative results.

What is information privacy then if not a right of control? Information privacy should be considered as a constitutive value that safeguards participation and association in a free society.[91] Decision-making in a democracy originates with individuals who are anchored in a variety of social settings. Democratic social systems therefore require information privacy because each of us, in one or more of our social roles, requires some insulation from observation and influence. As the sociologist Robert Merton states, "[p]rivacy is not only a personal predilection, though it may be that, too. It is a requirement of social systems."[92] Information privacy does not derive from the state of nature or an inborn capacity of autonomy, but depends on its essential relation to the health of a democratic society.[93] As

---

89. The First Amendment's precise limitations on personal data are, however, hotly contested at present. *Compare* Eugene Volokh, *Freedom of Speech and Information Privacy*, 52 STAN. L. REV. 1049 (2000) *with* Paul M. Schwartz, *Free Speech versus Information Privacy*, 52 STAN. L. REV. 1559 (2000).

90. *See* Thomas J. Miceli, *Land Title Systems*, *in* 2 DICTIONARY OF ECONOMICS & LAW, *supra* note 70, at 433, 434 ("[T]he United States has, since colonial days, relied for the most part on the recording system. This system . . . requires the maintenance of a public record of land transfer that can be inspected by prospective buyers to establish evidence of good title, thereby easing land transfer.").

91. I have made this argument more fully elsewhere. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 834-43 (2000) [hereinafter Schwartz, *Privacy and the State*]; Schwartz, *Privacy in Cyberspace*, *supra* note 8, at 1658-66. *See also* Post, *Social Foundations*, *supra* note 78, at 959 (describing how rather than upholding "the interests of individuals against the demands of community," information privacy creates rules "that in some significant measure constitute both individuals and community").

92. ROBERT K. MERTON, ON SOCIAL STRUCTURE AND SCIENCE 118 (Piotr Sztompka, ed. 1996). For an insightful discussion of the tie between information privacy and social practices, see Lloyd L. Weinreb, *The Right to Privacy*, 17 SOC. PHIL. & POL'Y 25, 42-44 (2000).

93. In this regard, a useful contrast can be drawn with totalitarian countries. In the analysis of Jürgen Habermas, totalitarian political systems seek to destroy "[c]ommunicative rationality . . . in both public and private contexts of communication" through "[a]dministrative intrusions and constant supervision." HABERMAS, FACTS & NORMS, *supra* note 78, at 369; HABERMAS, FAKTIZITÄT, *supra* note 78, at 446. As the spying of secret police in such countries makes clear, the structure of access to personal information has a decisive impact on the extent to which certain actions or expressions of identity are discouraged or encouraged. Information privacy is just as essential in non-totalitarian political systems. The

I have argued elsewhere, privacy helps to form the society in which we live and to shape our individual identities.[94] Its normative function is this constitutive role—and not the creation of individual control over personal data.

In particular, information privacy rules normatively define multidimensional information territories that insulate personal data from observation by outside parties. To do so, information privacy law should channel disclosure of certain information by restricting the receiving party's ability to share the data and by protecting the concerned individual's ability to shield this information from another audience.[95] As an example of such a multidimensional rule for information privacy, consider the Supreme Court's decision in *Planned Parenthood v. Casey*, which permitted the State of Pennsylvania to collect information about abortions for statistical purposes, but prevented it from sharing these data with the husbands of the women who sought this procedure.[96] As Justice O'Connor's plurality opinion for the Court indicates, protection of women's free decision-making about reproductive choice requires this restriction on data sharing due to the tragic history of spousal abuse in this country.[97] Autonomous decision-making and democratic opportunity require protection from various kinds of "outing," that is, revelation of otherwise fully or partially hidden aspects of one's life, before different audiences.

In the creation of multidimensional information territories, moreover, those who would shape legal and other rules must focus on the precise circumstances of the processing of personal information. As Guido Calabresi has urged, "I find the abstract discussion of when property rules are better than liability rules not all that helpful. I find the discussion instead very helpful when it takes place in a context, when it asks in a given situation why one rule is better than another."[98] In light of this admonition, I will now evaluate Lessig's property-based solutions to Internet privacy by setting his proposal into the existing context of information processing in cyberspace. Placing Internet privacy into context, I will identify significant failures in the privacy market in which Lessig's property regime is to function.

---

political systems. The Supreme Court's jurisprudence of associational rights and reproductive choice provides particularly striking examples concerning the link between autonomous decision-making and information privacy. SCHWARTZ & REIDENBERG, *supra* note 85, at 43-59.

94. For an elaboration of the concept of multidimensional privacy territories, see Schwartz, *Privacy in Cyberspace*, *supra* note 8, at 1667-80; Schwartz, *Privacy Economics*, *supra* note 8, at 55.

95. For a further discussion in the context of health care data, see Schwartz, *Privacy Economics, supra* note 8, at 69-74.

96. 505 U.S. 833 (1992).

97. *See id.* at 887-98.

98. Guido Calabresi, *Remarks: The Simple Virtues of the Cathedral*, 106 YALE L.J. 2201, 2205 (1997).

II. PRIVACY AS PROPERTY

Lessig's two-step solution for privacy on the Internet begins with the law declaring a property interest in personal information to promote trade in it. This Section makes a double response to this property regime for privacy. First, a market failure currently exists for information privacy and may well deepen following propertization à la Lessig. The consequences of this situation involve both deadweight losses and unfortunate distributional results. As a result, Lessig comes to the wrong conclusion regarding the Pareto-optimal result of a recourse to privacy-property: "Such a regime gives us confidence that if a trade occurs, it will be at a price that makes neither party worse off."[99] Finally, this section evaluates Lessig's reading of Calabresi-Melamed's work as supporting property rules for privacy.

A. Failure in the Privacy Market

Lessig's claim that propertization will lead to socially optimal data processing should be challenged on the grounds of failure in the privacy market. This failure can be traced to a bilateral monopoly in this market and the consequences of this phenomenon for "privacy price discrimination." There are structural reasons why the privacy market is unlikely to self-correct. While Lessig expects privacy-property to stimulate contract through code, property rights in personal data may systematically lead to bad bargains—and ones in areas of great social importance. The resulting cyber-agreements will be contracts of adhesion of a new kind. In other words, property plus code may lead to speedy ways to generate poor contracts or even no contracts, that is, the collection of data unbeknownst to the consumer and without her agreement.

1. PRIVACY PRICE DISCRIMINATION UNDER MARKET FAILURE

Price discrimination takes place when a seller sets "different prices to different purchasers depending not on the costs of selling to them, . . . but on the elasticity of the demand for his product."[100] A fully functioning "privacy market" requires sellers (i.e., consumers) to be able to bargain over the terms under which they will disclose their personal information, and buyers (i.e. data processors) to offer different packages and prices for this personal

99. LESSIG, CODE, *supra* note 4, at 161.

100. RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 305 (5th Ed. 1998) [hereinafter POSNER, ECONOMIC ANALYSIS]. 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).

information. In such a market, "privacy price discrimination" will emerge.[101] Privacy price discrimination involves a consumer seeking different packages of services, products, and money in exchange for her personal data, and a data processing company differentiating among consumers based on their varying preferences about the use of their personal data and the underlying value of the information.

To illustrate this point, imagine two hypothetical consumers: Marc and Katie. Marc cares deeply about how his personal information is used; Katie does not.[102] Marc also has especially valuable information to offer; he is rich and interested in high margin products such as sports cars and expensive watches.[103] In contrast, Katie is less affluent, takes the subway, and shops at thrift stores. Our intuition is that a privacy market should permit Marc to obtain greater services or more money for his personal information. Expressed more formally, a surplus from cooperation under a property regime requires at a minimum that Marc receive more than his "threat value" before disclosure.[104] The term "threat value" refers to the "price" that Marc would place on *not* disclosing his personal information. Beyond providing the threat value, privacy price discrimination also calls for further elasticity in meeting Marc's privacy preferences as his demand curve slopes upward.

Marc and the companies that process and exploit personal information are faced with a pervasive market failure, however, and the implications of this situation are significant. Under a property regime, the difficulties for Marc and the data processing companies are considerable due to a lack of information about how each party values Marc's personal data, potentially wide discrepancies in their respective valuations, and high transaction costs when they seek to bargain with each other.[106] The Internet privacy market is,

---

101. For a previous discussion, see Schwartz, *Privacy in Cyberspace, supra* note 8, 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 v. Zeidenberg, 86 F.3d 1447, 1448-49 (7th Cir. 1996); Robert Merges, *Of Property Rules, Coase, and Intellectual Property*, 94 COLUM. L. REV. 2655, 2666-67 (1994); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 328 (1989).

102. All names have been changed to protect the innocent. 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.

103. *See* Roger O. Crockett, *So the Rich Are Different: They Spend More Online*, BUS. WK., July 24, 2000, at EB 16 ("Rich cybernauts are . . . more likely than the rest of us to buy online" and "are far more likely to buy big-ticket items on the Web.").

104. For a concise introduction, see ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 92-94 (1988).

106. *See generally* Ian Ayres & Eric Talley, *Distinguishing Between Consensual and Nonconsensual Advantages of Liability Rules*, 105 YALE L.J. 235, 237-40 (1995); Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1098 (1995).

in fact, functioning poorly at present; as a consequence, it is not possible for the parties to look for a market valuation and rely simply on that. Indeed, the current market price for personal information is zero for many data processing companies because of a lack of knowledge for many consumers of how their personal information is collected in cyberspace.[107] Due to the resulting privacy market failure, a subsidy is given to those data processing companies that process and exploit personal data. Commercial entities generally obtain Marc's and Katie's personal data for the same low price or for free. As a consequence, the true cost of personal data is not imposed on these organizations.

This market failure both causes deadweight losses and has distributional consequences. The deadweight loss follows from the existence of consumers who would engage in more or different kinds of transactions on the Internet, but refuse to do so because of fears about how their personal data will be collected and used.[108] Polls have consistently shown that many Americans decline to engage in cyberspace transactions because of such fears.[109] In this fashion, the deadweight loss reduces the consumer surplus that would be created were privacy price discrimination in place. Such a loss, perhaps somewhat hidden during the Internet's early stages of rapid growth, will become more visible as e-commerce enters a slower stage. As a columnist in Silicon Valley's *Mercury News* warns, "almost all the online retailers hurriedly launched in 1998 and 1999 now appear doomed to disappear—not because e-commerce isn't going to be important, but because consumers aren't moving fast enough toward online shopping to sustain today's Web retailers."[110]

The failure in the privacy market also involves a distribution away from Marc and even Katie and towards data processing companies.[111] Companies

---

107. 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." Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 476 (2000).

108. For a general explanation of the deadweight loss under monopoly, see POSNER, ECONOMIC ANALYSIS, *supra* note 100, at 301-02.

109. For a recent summary and discussion of the poll data, see FEDERAL TRADE COMM'N, PRIVACY ONLINE 2 (May 2000) [hereinafter FTC, PRIVACY ONLINE]. As the FTC states, "surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce, and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction." *Id.*

110. Mike Langberg, *Info Appliances Aren't About to Push Aside the PC*, SAN JOSE MERCURY NEWS, July 14, 2000, at 6C.

111. Indeed, in a paper at a symposium devoted to the twenty-fifth anniversary of the seminal Calabresi-Melamed article, Calabresi emphasized the importance of examining distributional consequenees of legal rules, "[T]he article was a way of saying that we can look at a situation and consider whether one rule is more appropriate than another in terms that go

have no need to offer Marc greater services or more money for his personal data than they do Katie. In fact, they may not even meet Katie's more modest privacy threat value. The consequences of this situation resound far and wide. One 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.

2. STRUCTURAL PROBLEMS FOR A SELF-CORRECTING PRIVACY MARKET

The code for Internet information use will not be altered until data processors are forced to internalize the cost of different consumers' privacy preferences. Yet a move to a property regime under current and foreseeable future conditions is unlikely to lead to this result. In other words, a privacy self-correction will not happen under a property regime. The structural failure in the privacy market can be attributed to four causes: (1) information asymmetries, (2) collective action problems, (3) bounded rationality, and (4) limits on "exit" from certain practices. As a result of these weaknesses, an unadorned move to a property-based regime is unlikely to stimulate socially optimal levels of privacy. In fact, it is likely to make matters worse rather than better.

The first problem with a property regime for privacy is that most visitors to cyberspace lack essential knowledge of how their personal information will be processed. This idea has been discussed in the section regarding privacy price discrimination.[112] The knowledge needed for a functioning privacy market under a property regime begins with an understanding of the significance of the exchanges of personal information on the Internet. Yet, this understanding must extend not only to the primary use of consumer information, but also to the frequent secondary and tertiary uses. The existing system of data use is so complex, however, that even privacy experts can have difficulties in understanding the full range of data use. Beyond this knowledge, a property plus technology scheme requires that a critical mass of consumers understand and use Lessig's proposed electronic butler and comprehend the consequences of the shortcuts that are inevitably built into this system. As with the "blinking twelve" problem, however, considerable doubt must exist on this score.

---

beyond efficiency and allow decisionmakers to respond, for example, to distributional desires as well." Calabresi, *supra* note 98, at 2204.

112. *See supra* text accompanying notes 100-11.

The second difficulty in the Internet privacy market is a collective action problem—individual privacy wishes need to be felt collectively in the market.[113] The good news first: a group of privacy-promoting organizations is emerging that can promote effective collective action. Among these institutions are industry organizations that support self-regulation by drafting codes of conduct; privacy seal organizations, such as TrustE and BBBOnline; "infomediaries" that represent consumers by offering to exchange their data only with approved firms; privacy watchdog organizations that bring developing policy issues to public attention; and technical bodies, such as W3C, engaged in drafting Internet transmission standards, including P3P.[114] Lance Liebman has also tentatively proposed a role for private law-recommending institutions, such as the American Law Institute (ALI).[115]

Despite these promising developments, most of us are unable to free-ride successfully on the efforts of those who are more savvy about data privacy on the Internet. In particular, it is difficult to ride for free because of a lack of information about companies' compliance with their privacy policies. Detection costs remain high, and, as many experts have pointed out, current collective solutions, such as industry self-regulation and privacy seals, do not solve the problem.[116] As examples of the high cost of monitoring compliance with posted privacy policies, the FTC's 2000 Study, *Privacy Online*, points to the often confusing nature of privacy statements at Web sites and the lack of a significant Web presence for the privacy seal programs.[117] For that matter, the existence of competing privacy seal programs permits forum shopping by Web sites that hope for weaker enforcement from one seal service rather than the other.[118]

---

113. For a general discussion of collective action problems, see SUNSTEIN, *supra* note 75, at 59-61.

114. Part of the difficulty regarding collective action in cyberspace has been that groups on the Internet often lack the stability necessary for ongoing collective action. For discussion of this issue, see Netanel, *supra* note 107, at 405; Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1266-92 (1998). It remains to be seen whether any of the emerging privacy cyber-groups will prove more stable. For a further discussion, see Schwartz, *Privacy and the State, supra* note 91, at 854; Schwartz, *Privacy in Cyberspace, supra* note 8, at 1694-96.

115. Lance Liebman, *An Institutional Emphasis*, 32 CONN. L. REV. 923, 924-26 (2000). For Liebman, the work of bodies such as the ALI is to be integrated with the work of the other non-governmental organizations that promote privacy. *Id.*

116. Marc Rotenberg has stated, regarding the United States government's high level of deference to industry self-regulation, "One cannot escape the conclusion that privacy policy in the United States today reflects what industry is prepared to do rather than what the public wants done." Rotenberg, *supra* note 55, at ¶ 107.

117. FTC, PRIVACY ONLINE, *supra* note 109 at ii, 24.

118. For comparisons of the reported decisions of the two services, see TrustE, *Investigation Results*, (visited July 25, 2000) <http://www.truste.com/users/users_investigations.html>; BBOnline, *Public Postings of Dispute Resolution Case Decisions*, (visited July 25, 2000) <http://www.bbbonline.com/privacy/dr.asp>. For criticisms

The third difficulty with the propertization of personal information is bounded rationality.[119] Scholarship in behavioral economics has demonstrated that consumers' general inertia towards default terms is a strong and pervasive limitation on free choice.[120] This does not mean that consumers are all sheep, but it does mean that default rules and form terms can have great psychological force and are likely to reward those who otherwise have greater power. Lessig wishes to use law to turn personal information into property, but this act is likely to reward a limited set of market participants. Specifically, in the current privacy market, this move will benefit the parties who process and share our information and not those who help us place limits on this processing. As a result of this current power dynamic, individuals faced with standardized terms and expected to fend for themselves with privacy-property and available technology are likely to accept whatever data processors offer them.

In particular, P3P heightens the difficulties with bounded rationality by creating a new and potentially dangerous set of personal information, namely "privacy meta-data." This point is worth elaborating. In the context of his attack on PICS, Lessig notes how that software protocol's rating of speech provides useful information for any observer who wants a snapshot of our interests and activities.[121] Speech can be rated as Democratic or Republican, or to use existing PICS categories, as containing "extreme hate speech" or "non-explicit nudity." Although Lessig does not discuss it under the rubric of "meta-data," his example is, in fact, one concerning such "information about information."

It is significant that privacy meta-data are generated not only by PICS but by P3P as well. In other words, Lessig's kind of privacy filtering will

---

of TrustE as offering at best weak enforcement, see Chris Oakes, *TrustE Declines Real Probe* (last modified Nov. 9, 1999) <http://www.wired.com/news/technology/0,1282,32388,00.html>.

In fairness to TrustE, however, it has taken a more aggressive stance of late in the Toysmart bankruptcy case. Toysmart, a bankrupt Internet toy retailer, sought to sell its customer information although its Web site's privacy notice promised never to do so, and TrustE, objecting to the FTC's resolution of the case, has demanded additional privacy protections for these data. *See* Federal Trade Comm'n, *FTC Announces Settlement With Bankrupt Website* (last modified July 21, 2000) <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (hereinafter FTC, *Settlement*); Matt Richtel, *FTC Moves to Halt Sale of Database at Toysmart*, N.Y. TIMES, July 11, 2000, at C2; Matt Richtel, *Toysmart.com In Settlement With FTC: Deal Would Allow Sale of Customer Database*, N.Y. TIMES, July 22, 2000, at B1; Elinor Abreu, *TrustE to File Antiprivacy Brief Against Toysmart* (last modified June 30, 2000) <http://www.thestandard.com/article/display/1,1151,16577,00.html>.

119. For a concise introduction, see David M. Kreps, *Bounded Rationality*, in 1 DICTIONARY OF ECONOMICS & LAW, *supra* note 70, at 168-69.

120. 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).

121. Lessig, *supra* note 45, at 1; LESSIG, CODE, *supra* note 4, at 177-80.

create information about one's privacy preferences. All these data, whether created by PICS or by P3P, will be highly sought-after by marketers and other parties.[122] Filtering will thereby create the possibility of further privacy violations unless consumers are able not only to negotiate for their privacy but also for their privacy meta-data. Beyond privacy filters such as P3P, moreover, the increasing use of eXtensible Markup Language (XML) will also promote the creation of personal meta-data.[123] Like Hypertext Markup Language (HTML), XML is a document coding system used on the Web; the advantage of XML is that it permits the tagging of information elements in a more customized fashion than HTML. Specifically, XML defines a syntax that allows information elements on Web sites to be tagged according to their content (e.g., "article" or "privacy statement").[124] As a result, this programming format allows easier aggregation of information about consumer preferences, including those about privacy. The great danger, however, is that all this information about information, whether generated through PICS, P3P or XML, will lead to additional privacy invasions by providing new ways for data processors to benefit from consumer inertia. Bounded rationality points to the need to find ways to permit consumers to make informed decisions about use of their personal information as well as their meta-data at the least cost to them.

Finally, cyberspace, in certain of its applications, turns out to be far from friction-free. In particular, when limits exist on "exit" from certain practices, the danger is that online industry will "lock-in" a poor level of privacy on the Web. Cookies and data processing at work demonstrate the difficulty of exit and the danger of lock-in.

Cookies are alphanumerical numbers that Web sites place on the hard drives of their visitors.[125] Beyond the Web sites that one visits, cookies are also placed by ad banner services and advertisers.[126] A ready source of

---

122. For a battle over such "privacy meta-data" in the context of traditional telephony, see U.S. West, Inc. v. F.C.C., 182 F.3d 1224, 1228 (10th Cir. 1999), *cert. denied sub. nom.* Competition Policy Inst. v. U.S. West, Inc., 120 S. Ct. 2215 (2000). For differing views on the merits of this decision, compare Cate, *supra* note 68, at 893 with Paul M. Schwartz, *Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, 32 CONN. L. REV. 929, 935-36 (2000).

123. For a definition of meta-data, see MICROSOFT COMPUTER DICTIONARY (4th ed. 1999). For the official specifications of XML, see W3C, *XML Information Set* (last modified July 26, 2000) <http://www.w3.org/TR/2000/WD-xml-infoset-20000726>.

124. *XML Is . . . Technically Speaking* (visited Aug. 1, 2000) <http://architag.com/xmlu?XMLIs/Technieally.html>; MICHAEL J. YOUNG, STEP BY STEP XML 7-14 (2000).

125. For an introduction, see Brett Glass, *Cookies: The Good, the Bad, and the Sneaky*, PC MAG. (May 25, 2000) <http://www.zdnet.com/pcmag/stories/reviews/0,6755.2572521,00.html>; Junkbusters, *How Web Servers' Cookies Threaten Your Privacy* (visited July 20, 2000) <http://www.junkbusters.com/ht/en/cookies.html>.

126. As the Modern Humorist states tongue-in-cheek, "You may occasionally get cookies from our advertisers, which is standard in the Internet industry. Which makes it

detailed information about personal online habits and in widespread use, cookies are difficult to combat.[127] Mastery of advanced settings on one's Web browser, the downloading of "cookie-cutting" software, and some public protests about more egregious practices have helped, but not solved this problem. As a joint paper of the Electronic Privacy and Information Center and Junkbusters notes, "Those consumers, who have taken the time to configure their browsers to notify when receiving, or reject cookies, have found that web surfing becomes nearly impossible."[128] It is nearly impossible because so many sites set so many cookies. As a result, as the joint paper of the privacy advocates observes, "Many browsers . . . require the user to say 'no' to each cookie when a user asks to be informed when cookies are placed, which can be very burdensome when several attempts are made per page."[129] Moreover, beyond cookies, the next privacy melt-down is never far away. A possible source for the next crisis are so-called "Web bugs," also known as "clear GIF," which permit a Web page to snoop on visitors through tiny images, sometimes as small as one or two pixels in size, that log your access to the page and read previously set cookies on your computer.[130] These images are loaded from a different server than the rest of the Web page.

As a final example of the difficulties in exit and of the emerging "lock in" for informational privacy, the modern workplace demonstrates that many of us enter cyberspace anchored in real space settings that limit our ability to negotiate. Most participants in the American workplace leave their informational privacy at the door of work.[131] As the *New York Times* states,

---

okay." Modern Humorist, *Privacy Policy Statement* (visited July 20, 2000) <http://modernhumorist.com/house/policies.html>.

127. Both Microsoft's Internet Explorer and Netscape's Communicator offer some choices for managing cookies, and software can also be installed that limit some of the capacity for these devices to invade privacy. Yet, these solutions all have notable limits. Consider the Netscape Communicator warning that informs one when a cookie is set on one's hard drive. This screen will pop up so often when one surfs the Web that the most likely response is simply to disable it. If one refuses visits to Web sites that set cookies, most of the Web will be placed off-limits. Junkbusters & the Electronic Privacy Information Center, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (June 2000) <http://www.junkbusters.com/ht/en/p3p.html>.

128. *Id.* at 6.

129. *Id.* at 4.

130. See Richard M. Smith, *The Web Bug FAQ* (last modified Nov. 11, 1999) <http://www.tiac.net/users/smiths/privacy/wbfaq.htm>. Richard Smith is the computer consultant who coined the term, "Web Bug," and first brought these tracking images to the attention of the public. He has recently joined the Privacy Center, a joint effort of the Privacy Foundation and the University of Denver, which investigates the privacy implications of software activity on the Internet, Chris Oakes, *Privacy Sleuthing Goes Pro*, WIRED.COM, July 27, 2000, at 1 <http://www.wired.com/news/technology/0,1282,37812,00.html>. For this organization's Web site, see Privacy Foundation (visited July 31, 2000) <http://www.privacyfoundation.org/>.

131. As one sample "Corporate Internet Use Policy" warns, "Widget reserves the right to access and disclose, for any purpose, the contents of any Internet messages sent to and

"the debate over employee privacy is over."[132] It is over because "widespread, routine snooping on employees is no longer a threat but a fact."[133] Snooping takes place on employees not only at work, but, in our age of flexible and long hours, at home where more workers are now using computers for employment-related reasons.[134]

Propertization of personal data will reinforce the employer's ability to snoop; it will do so by strengthening the already popular argument that the employer owns all information generated by its employees.[135] Most workers also will never be permitted to use Lessig's electronic butler—and certainly not in daily privacy negotiations with their boss or outside Web sites. As for other kinds of self-help, such as encryption of one's email or use of Web sites that let one surf anonymously, *Business Week* warns workers that such behavior will "offer no legal protection—and can raise red flags with your employer."[136] In the workplace, an exit to privacy is frequently not possible—unless one wants to become self-employed.

B. Lessig's Nova, or the Limits of Property Rules

Lessig's recourse to property relies, of course, on Calabresi and Melamed's seminal work regarding the relative merits of property and liability regimes. It must be noted, however, that Lessig concentrates on only a single of the Calabresi-Melamed insights, which concerns the setting of one's price *ex ante* in a property regime.[137] In place of Lessig's abbreviated

---

from Widget's computer equipment, including e-mail. All users, including Widget employees, using the Internet waive any right to privacy in such messages, and consent to their being accessed and disclosed by Widget personnel." MILLSTEIN ET AL., *supra note* 2, AT § 6.12, 6-26. For two leading employee privacy cases, see McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App.-Dallas 1999); Smyth v. Pillsbury Corp., 914 F. Supp. 97 (E.D. Pa. 1996).

132. Jeffrey L. Seglin, *As Office Snooping Grows, Who Watches the Watchers?*, N.Y. TIMES, June 18, 2000, at Bus. Sec. 4.

133. *Id.* As *Business Week* concisely concludes, "When it comes to privacy in the workplace, you don't have any." Larry Armstrong, *Someone to Watch Over You*, BUS. WK., July 10, 2000, at 189.

134. See Michael J. McCarthy, *Data Raid: In Airline's Suit, PC Becomes Legal Pawn, Raising Privacy Issues*, WALL ST. J., May 24, 2000, at A1, (Northwest Airlines convinced court to issue order allowing it to search "20 or so hard drives at flight attendants' homes and union offices.").

135. For a report on the kind of ongoing observation of employees that typically takes place, see Michael J. McCarthy, *Snoop Dog: Web Surfers Beware: The Company Tech May Be a Secret Agent*, WALL ST. J., Jan. 10, 2000, at A1.

136. Armstrong, *supra* note 133, at 190.

137. LESSIG, CODE, *supra* note 4, at 160. Lessig's favoring of property rules for facilitating trade generally tracks the work of Richard Posner, who views privacy law, at least in part, as a functional branch of property law. *See* POSNER, ECONOMIC ANALYSIS, *supra* note 100, at 46 ("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."). For a more general plea

reading of Calabresi-Melamed, a fuller description of their framework is warranted.

These two authors propose that property rules are generally to be favored when there are few parties, difficult valuations, and otherwise low transaction costs.[138] Liability rules are preferable, in contrast, when there are many parties (and especially when one party has power to block an entire enterprise), a likelihood of strategic bargaining, and otherwise high transaction costs.[139] These distinctions have retained their fascination for a new generation of scholars.[140]

What then of liability versus property rules for Internet privacy? The Calabresi-Melamed framework does not point to an exclusive need for property rules, but, especially when read in light of later scholarship, suggests the benefits of a mixed regime. Moreover, Lessig's central example, which involves the sale of an automobile—to be precise, a Chevy Nova—also points to the necessity of going beyond property rules. We now examine each element in the Calabresi-Melamed framework albeit modifying the order of their elements by examining the valuation issue last.

Calabresi-Melamed's first criterion concerns the number of parties involved. If we consider Internet data processing through a focus on each discrete transfer of information, it may appear only to involve few parties. A weakness with this perspective, however, is the widespread downstream use of personal information. As noted above, beyond the primary use of consumer information, secondary and tertiary uses are frequent. For four quick examples of such downstream information use, consider: (1) the frequent mergers or affiliations between Internet companies that lead to sharing of databases;[141] (2) the corporations that demand personal data from

---

for favoring property rules, see Richard A. Epstein, *A Clear View of the Cathedral: The Dominance of Property Rules*, 106 YALE L.J. 2091 (1997).

138. Calabresi & Melamed, *supra* note 7, at 1106-08.

139. *Id.* at 1105-06.

140. On the enduring significance of the Calabresi-Melamed Article, see James E. Krier & Stewart J. Schwab, *The Cathedral at Twenty-Five: Citations and Impressions*, 106 YALE L.J. 2121 (1997). For examples of the influence of "The Cathedral," see Emily Sherwin, *Introduction: Property Rules as Remedies*, 106 YALE L.J. 2083 (1997); Epstein, supra note 137, at 2091; Carol M. Rose, *The Shadow of the Cathedral*, 106 YALE L.J. 2175 (1997); Ian Ayres & J.M. Balkin, *Legal Entitlements as Auctions: Property Rules, Liability Rules, and Beyond*, 106 YALE L. J. 703 (1997); Saul Levmore, *Unifying Remedies: Property Rules, Liability Rules, and Startling Rules*, 106 Yale L.J. 2149 (1997); Robert P. Merges, *Contracting into Liability Rules*, 84 CAL. L. REV. 1293 (1996); James E. Krier & Stewart J. Schwab, *Property Rules and Liability Rules: The Cathedral in Another Light*, 70 N.Y.U. L. REV. 440 (1995) [hereinafter Krier & Schwab, *Another Light*].

141. For an illustration of these mergers and affiliations, see for example, Jane Hodges, *In Good Company*, BUSINESS 2.0 (Aug. 8, 2000) <www.business2.com/context/magazine/marketing/2000/07/25/14815>; Paul Bonanos, *Deal Watch* (last modified June 19, 2000) <http://www.thestandard.com/research/metrics/display/0,2799,16068,00.html>.

chat rooms or from ISPs to identify parties that have criticized them;[142] (3) the sale at asset auctions of personal information collected by bankrupt e-commerce companies;[143] and (4) ad banner companies, such as DoubleClick and 24/7, that serve advertisements on Web sites and also track an individual's movements across different Web sites.[144] These examples of downstream data processing show that large numbers of parties are involved, often on a routine basis, in Internet data use. The first Calabresi-Melamed benchmark cannot be said unambiguously to support a property regime.

As to the second Calabresi-Melamed criteria, we are to prefer liability rules when high transaction costs are present and property rules when low transaction costs exist. Lessig views transaction costs under his property-technology regime as low.[145] Here, too, one cannot be as conclusive about the merits of propertization for privacy. First, transaction costs are often slippery to measure; Calabresi and Melamed, for example, have been criticized for failing to take into account the administrative costs associated with recourse to the legislature or judiciary under liability rules.[146] Second, as the above examples of downstream data processing indicate, Internet information use often involves parties who face high costs when starting the process of bargaining with each other. One property scholar, Carol Rose,

---

142. For a discussion, see Elinor Abreu, *Yahoo Postings Prompt More Lawsuits* (last modified July 14, 2000) <http://www.thestandard.com/article/display/0,1151,16828,00.html>.

143. For example, Toysmart, a bankrupt Internet toy retailer, has sought to sell its customer information although its Web site's privacy notice promised never to do so. *See* FTC, *Settlement*, *supra* note 119, at 1.

144. See Andrea Petersen, *DoubleClick Reverses Course After Privacy Outcry*, Wall St. J., Mar. 3, 2000, at B1; Chris Oakes, *DoubleClick Plan Falls Short* (last modified Feb 14, 2000) <http://www.wired.com/news/business/0,1367,34337,00.html>. The Michigan Attorney General has commented, "DoubleClick's privacy policy is a moving target, and consumers should be extremely cautious about relying on the company's vague promises." Grant Luckenbill & Ken Magill, *Michigan Latest to Open Fire on DoubleClick*, DM NEWS at 1, (Feb. 18, 2000) *available at* <http://www.dmnews.com/articles/2000-02-14/6549.html>.

The FTC, while calling for federal legislation to insure industry-wide coverage of Fair Information Practices by online advertising agencies, has recently negotiated an agreement with the Network Advertising Initiative (NAI) to put a self-regulatory proposal in place for online profiling. *See* FTC, *Federal Trade Commission Issues Report on Online Profiling, Commends Network Advertising Initiative's Self Regulatory Principles*, (July 27, 2000) <http://www.ftc.gov/opa/2000/07/onlineprofiling.htm>; Chris Oakes, *FTC Endorses Privacy Rules* (last modified July 27, 2000) <http://www.wired.com/news/politics/0,1283,37853,00.html>.

145. Lessig describes the move to the electronic butler as reducing an individual's "processing costs for text," which are said to be "wildly high." LESSIG, CODE, *supra* note 4, at 160.

146. *See* Krier & Schwab, *Another Light*, *supra* note 140, at 454-55. In response, Calabresi has stated: "[O]f course, the cost of costing is important . . . [b]ut we must equally take into account what it costs people to define the price at which they would sell, if we were to use property rules instead." Calabresi, *supra* note 98, at 2205. In his view, it is incorrect to assume that the costs of this assessment are always low. *See id.* at 2205-06.

describes such barriers to negotiations as "Type I" costs, that is, costs that occur *before* bargaining.[147] These "costs" are unlikely to be fully internalized—for the numerous reasons set out previously—because of failure in the privacy market. Lessig's point about low transaction costs under a property regime rests on a belief in the plasticity of these costs in the Internet privacy market. However, these "Type I" barriers to negotiation are unlikely to prove as easy to lower as Lessig believes. Without high adoption of the Cyber-Jeeves by Web sites and widespread adoption and mastery of this software protocol by the Internet masses, propertization of information will not have the sought-after affect.

The final Calabresi-Melamed criteria concern the likelihood of difficult valuation (which would favor property rules, if present) and strategic bargaining (which would favor liability rules, if present). The issue of difficult valuation is where Lessig's Nova emerges as a decisive example. To start with strategic bargaining, however, this issue generally points to impediments that occur *after* bargaining begins. Carol Rose terms these "Type II" costs.[148] One possible strategic bargaining difficulty is that of the holdout—the single intransigent person who stops a transaction involving multiple parties. The archetypical holdout is a landowner, perhaps one with a small estate, whose refusal to sell mini-Blackacre frustrates efforts to assemble a parcel of all property necessary for construction of a factory. This kind of holdout issue generally does not occur for Internet privacy. To return to Marc and Katie, whom we first encountered in our section on market failure, Marc, who cares deeply about privacy, will not be able to hold up transactions with others. To the contrary, the difficulty is that the privacy market is not yet elastic enough for him to have his preferences met at low costs. Marc cannot easily manage transactions involving his personal data. As previously noted, this situation leads to both deadweight losses and distributional results away from Marc and Katie.

As for the difficulty of valuation, Lessig correctly notes the idiosyncratic nature of many privacy preferences. He compares this situation to those who have a "sentimental attachment" to their automobile: "You cannot be forced to give up your Nova unless you get your minimum price."[149] Lessig adds, "A property regime thus protects both those who value their privacy more than others and those who value it less, by requiring that someone who wants to take a given resource must ask."[150] Even granting the idiosyncratic nature of many people's privacy preferences, propertization is at best a mechanism for setting the collective costs involved in *some* aspects of Internet privacy. The seminal work of Ian Ayres and Robert Gertner suggests, in fact, that

147. Rose, *supra* note 140, at 2184.
148. *Id.* at 2185.
149. LESSIG, CODE, *supra* note 4, at 161.
150. *Id.*

propertization in cases of asymmetric knowledge creates incentives for strategic behavior.[151] In contrast, a liability rule can be "information forcing"; it can lubricate consensual transactions by forcing disgorgement of private knowledge.[152] In other words, a liability rule forces parties to be more forthright. By indicating the cost of taking without permission, it causes those with superior knowledge to disclose it when bargaining around the settlement range.

We come now to Lessig's Nova, an example that inadvertently suggests the limits of property in shaping and maintaining privacy rules. In particular, Lessig's use of the Nova example is misleading because of his exclusive focus on the moment when the car is transferred;[153] the more important issue is the planned use of the car and the restrictions on what can be done with it. The use of an automobile is generally controlled through liability rather than property rules. In fact, something that may look only like property, an automobile, is actually actively formed, limited, and otherwise shaped through laws that compel obedience by setting the price of violation in advance rather than through market exchanges involving property rules.

Recall that, in the terminology of Calabresi and Melamed, liability rules seek to induce investment in obedience to standards through public setting of the cost of violations. Thus, a jury, court or legislature fixes damages for which the violator is "liable."[154] In contrast, property rules are enforced by injunctions for specific performance and contractual damages.[155] Now consider the most frequent use of a Chevy Nova: being driven on a road. Here, we see the first elements of the mixed-use system for automobiles. Accidents, as Lessig himself notes, are regulated through liability rules.[156] Moreover, in order to drive the Nova, we must license it, subject it to vehicle inspections on a regular basis, and obey all speed limits.[157] The design of Lessig's Nova was itself shaped by standards established through

---

151. Ayres & Gertner, *Default Rules, supra* note 8, at 99-100; Ayres & Gertner, *Optimal Choice*, supra note 8, at 732-35. For a concise summary, see Ian Ayres, *Default Rules for Incomplete Contracts*, 1 DICTIONARY OF ECONOMICS & LAW, *supra* note 70, at 585, 586-88.

152. Ayres & Gertner, *Default Rules*, *supra* note 8, at 128-30. In the health eare setting, I have argued in favor of such a use of liability rules for personal data. Schwartz, *Privacy Economics, supra* note 8, at 53-56.

153. LESSIG, CODE, *supra* note 4, at 161.

154. Calabresi & Melamed, *supra* note 7, at 1092.

155. *Id.*

156. LESSIG, CODE, *supra* note 4, at 160-61.

157. For examples from New York, see N.Y. VEH. & TRAF. § 301 (McKinney 1996 & Supp. 2000); N.Y. VEH. & TRAF. § 1180 (McKinney 1996); N.Y. VEH & TRAF. § 401 (McKinney 1996). A special category of registration even exists for "old timers," which can be driven only under limited conditions. *See* N.Y. VEH. & TRAF. § 401 (McKinney 1996).

governmental regulation and past litigation about product defects.[158] Finally, even at the moment of sale, "lemon laws" place strict restrictions on dealers of automobiles.[159] The real issue for automobiles—as well as for personal information—is what you can do with it. For personal information, once our concern becomes *the use* that one makes of data, and not the isolated moment of sale, necessary restrictions will require some recourse to liability rules as is the case for the use of automobiles.[160]

A restricted trade in heavily regulated automobiles is permissible—but property functions here against a thick background of liability rules.[161] Indeed, as Calabresi and Melamed conclude in their seminal article, "It should be clear that most entitlements to most goods are mixed."[162] The nature of the mix therefore becomes the critical issue, and the question that will now be discussed.

III. FAIR INFORMATION PRACTICES FOR INTERNET PRIVACY

Fair Information Practices (FIPs) are the leading policy tool for Internet privacy. When evaluated within the Calabresi-Melamed framework, these standards sound in liability rather than property. FIPs represent a kind of compulsory licensing scheme—they provide mandatory rules for all those who process personal information and force compliance by threatening damages should data not be handled as prescribed. Yet, FIPs can also include a property element. FIPs should provide limited room for *ex ante* negotiations by including default standards around which parties can contract. FIPs can be contrasted with the classic tort right of privacy, which suffers from numerous shortcomings as a tool for information privacy in cyberspace.

---

158. For the statutory framework, see the National Traffic and Motor Vehicle Safety Act, 49 U.S.C. § 30101 et seq. (1994). Jerry L. Mashaw & David L. Harfst offer a skeptical view of the extent to which automobile manufacturers gain useful information from the product liability docket about "how to alter the design of their automobiles." JERRY L. MASHAW & DAVID L. HARFST, THE STRUGGLE FOR AUTO SAFETY 241 (1990). Mashaw and Harfst contrast the weakness of product liability litigation with the importance, for better or worse, of National Highway Traffic Safety Agency (NHTSA) safety regulations and call for this ageney to "indicate the types of performance characteristics that it wants to see in automobiles in controlled tests." *Id.* at 252.

159. N.Y. GEN. BUS. § 198-b (McKinney 1988).

160. In real estate, the classic kind of property, there is evidence of this mixed regime. Violation of the deed covenant for title leads only to a damage remedy, a liability rule, rather than specific performance, a property rule. ROGER A. CUNNINGHAM ET AL., THE LAW OF PROPERTY 862 (1993).

161. For that matter, even modest use of an inalienability rule is made in this context. After all, while Lessig is generally permitted to transfer his Nova to the highest or lowest bidder as he chooses, he may not sell or otherwise alienate his driver's license. N.Y. VEH. & TRAF. § 509 (McKinney 1996).

162. Calabresi & Melamed, *supra* note 7, at 1093.

As a matter of some complexity, however, the critical issue for FIPs on the Internet will be their precise mixture of mandatory and default rules.

A. Out of the Shadows

The idea of the "shadow example" comes from Carol Rose, who has analyzed how a series of classic articles about property law rely on hidden, or "shadow" paradigms.[163] In Rose's assessment, for example, Calabresi and Melamed focus explicitly on the law of environmental nuisance, but, lurking as their secret model, is "the law of accidents, an example that barely makes an appearance in the article itself."[164] Rose argues for light on the shadows; she wishes to end this pattern of "rhetorical blurring" and urges that we "pay close attention to examples."[165] Through analysis of Lessig's Nova, this Article has begun this process of close attention to examples. It is only fair, however, to turn the tables and consider whether this Article has its own shadow examples. Two possibilities must be examined: first, the tort right of privacy, and second, fair information practices.

The tort right of privacy may appear to be the most likely example lurking in the shadows. Since Warren and Brandeis' identification of this right in 1890, it has emerged as one of the most important developments for the common law in the Twentieth Century.[166] The difficulty, however, is that the tort right of privacy is poorly suited to serve as a central tool for a privacy law for the Internet. If this right represents the best that liability has to offer, we may be better off with property rules after all. Let us briefly consider the privacy tort's weaknesses.

The common law has developed a set of tort rights that protect against four types of invasion of privacy. These are: (1) intrusion upon one's seclusion; (2) public disclosure of private facts; (3) publicity that places one in a false light before the public; and (4) appropriation of one's name or likeness without permission.[167] Various limitations that the common law

---

163. Rose, *supra* note 140, at 2176-77.

164. *Id.* at 2176.

165. *Id.* at 2199-200.

166. For the classic article, see Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

167. RESTATEMENT (SECOND) OF TORTS, § 652A-D (1977). Regarding the weaknesses of the privacy tort in the Information Age, see F. LAWRENCE STREET, LAW OF THE INTERNET 107-24 (1997); SCHWARTZ & REIDENBERG, *supra* note 85, at 180-82, 329; Joel R. Reidenberg, *Privacy in an Information Economy*, 44 FED. COMM. L.J. 195, 221-26 (1992); Gellman, *supra* note 27, at 210-11. For more general criticisms of the privacy tort in the offline world, see Murphy, *supra* note 8, at 2388; Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 292-93 (1983).

For a sampling of the applicable case law, see, e.g, Dwyer v. American Express, 652 N.E.2d 1351 (Ill. App. Ct. 1995); Miller v. Motorola, 560 N.E.2d 900, 903 (Ill. App. Ct.

places on each of these four branches eliminate their usefulness in responding to violations of privacy in cyberspace.[168]

To begin with the tort of intrusion on privacy, it prevents intentional interference with the private affairs or concerns of an individual. Yet, such intrusions must be "highly offensive."[169] The lesson from case law from the offline world is that most surreptitious collections of personal data are not likely to be found sufficiently "objectionable."[170] Second, as for the public disclosure tort, it requires both widespread disclosure to the public, which will not be present in most cases in which e-companies collect personal information, and a highly offensive matter that is publicized.[171] Third, the false light tort requires both a highly offensive revelation and that the information be false.[172] Internet privacy law must more typically be concerned, however, with the use of personal data that is true.

Finally, the misappropriation privacy tort, which is the branch most likely to have some impact in the Internet age, is also the most limited because it generally protects only those who wish to exploit their privacy. As Dan Dobbs notes in his treatise on torts, this form of the privacy tort is most frequently applied "to the case of public figures who do not seek privacy but on the contrary seek out opportunities for public exposure."[173] The misappropriation tort safeguards the monetary value of the kind of self-revelation that our culture associates with celebrity status. On the Internet, for example, this tort assists in the commodification of identity by lowering certain transaction costs for Elvis and Madonna wanna-be's. It helps Jenni, who has set up a Web-cam in her apartment and is Web-casting her own show, from any false Jenni using the term "Jennicam" and trying to steal her

---

1990); Porten v. University of San Francisco, 134 Cal. Rptr. 839, 841 (Ct. App. 1976); Shibley v. Time, 341 N.E.2d 337 (Ohio Ct. App. 1975).

168. See generally Schwartz, *Privacy in Cyberspace, supra* note 8, at 1634-35; Kang, *supra* note 8, at 1231.

169. RESTATEMENT (SECOND) OF TORTS, § 652B.

170. Kang, *supra* note 8, at 1231; SCHWARTZ & REIDENBERG, *supra* note 85, at 112.

171. RESTATEMENT (SECOND) OF TORTS, § 652D. As the Reporter's Comment to this section states, "'Publicity . . . means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.* at cmt. a.

172. *Id.* at § 652E.

173. DAN DOBBS, THE LAW OF TORTS 1198 (2000). For an introduction to publicity rights, see DONALD S. CHISUM & MICHAEL A. JACOBS, UNDERSTANDING INTELLECTUAL PROPERTY LAW § 6G, 6-66-6-78 (1992). For a discussion of the different tort interests in privacy, see Joel R. Reidenberg, *Setting Standards for Fair Information Practices*, 80 IOWA L. REV. 497, 504-06 (1995). For a sampling of case law, see Wendt v. Host Int'l, Inc. 125 F.3d 806 (9th Cir. 1997); White v. Samsung Elec. Am., Inc. 971 F.2d 1395, 1397 (9th Cir. 1992), *cert. denied* 508 U.S. 951 (1993); Eastwood v. Superior Ct. for Los Angeles County, 198 Cal. Rptr. 342, 347 (Ct. App. 1983). For further criticism of the right of publicity as a tool for information privacy, see Sehwartz, *Privacy and the State*, *supra* note 91, at 831-32.

audience.[174] States also increasingly permit the "publicity right" to be inheritable, which will be good news for Jenni's heirs.[175] But the misappropriation tort will not establish constitutive privacy's domains of access and non-access to information.

Having brought the privacy-tort and its four branches into the light, I have not found much promise here for cyberspace privacy. Fair Information Practices (FIPs) still remain to be considered as a shadow example. During the 1970s, some eighty years after Warren and Brandeis identified the privacy tort, the United States developed FIPs as a new tool for privacy protection.[176] By the start of the 1980s, FIPs had coalesced into their current form.[177] Currently expressed in statutes such as the Video Privacy Protection Act, the Privacy Act, and the Cable Communications Act, FIPs offer great promise for Internet privacy.[178] Although the expression of FIPs in different laws, regulations, and proposals varies in details, sometimes crucially, these standards generally require four things: (1) the creation of defined obligations, often statutory in nature, with respect to the use of personal information; (2) the maintenance of processing systems that are understandable to the concerned individual (transparency); (3) the assignment of limited procedural and substantive rights to the individual;[179] and (4) the establishment of effective oversight of data use, whether through individual

---

174. *See* Jennicam, (visited July 31, 2000) <http://www.jennicam.org>. Indeed, Jenni recently has discovered traditional intellectual property law, placed a copyright on her Web site, obtained a trademark on "Jennicam," and began streaming a Web-cast show about her life. *See id.* She is also selling bumper stickers that declare, "I'd rather be watching Jennicam." *Id.*

For the classic article about legal implications of the "cult of celebrity" in the United States, see Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CAL. L. REV. 125, 227-28 (1993).

175. On the inheritability of rights of publicity, see for example, Factors Etc., Inc. v. Pro Arts, Inc., 579 F.2d 215 (2d Cir. 1978) ("right of publicity" inheritable under New York State law); Peter L. Felcher & Edward L. Rubin, *Privacy, Publicity, and the Portrayal of Real People by the Media,* 88 Yale L.J. 1577, 1618-20 (1979). In California, the state legislature has resolved the question of commercial life after death through a statute that permits inheriting of the right of publicity. *See, e.g.*, CAL. CIVIL CODE § 3344.1.

176. Colin Bennett provides an excellent description of developments during this decade. COLIN J. BENNETT, REGULATING PRIVACY 96-101 (1992).

177. Perhaps the clearest evidence of this movement from the 1970s comes from the Privacy Act of 1974, which in its section (e) requires fair information practices for federal agencies. 5 U.S.C. § 552a(e) (1994). For a discussion, see SCHWARTZ & REIDENBERG, *supra* note 85, at 93-118. Concerning privacy law in the private sector, the Fair Credit Reporting Act of 1970 is the leading statutory embodiment of FIPs from this era. 15 U.S.C. § 1681 (1994).

178. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994); Privacy Act of 1974, 5 U.S.C. § 552a (1994); Cable Communications Act of 1984, 47 U.S.C. § 551 (1994).

179. For discussion of the standards, see Schwartz, *Participation*, *supra* note 27, at 557-64; *see also* BENNETT, *supra* note 176, at 101-11.

litigation (self-help), government and private scrutiny (external oversight), or some combination of these approaches.[180]

Within the Calabresi-Melamed framework, FIPs are best understood as liability rules. A good analogy to them is the kind of compulsory licensing system that American law provides for certain uses of music.[181] Similar to compulsory licensing of such intellectual property in the music industry, FIPs permit use of a protected interest only once pre-set conditions are fulfilled. Through their threat of damages should information not be handled in the prescribed fashion, FIPs will force data processors to invest in compliance and to engage in sought-after behavior. As Calabresi and Melamed note in general terms, "the choice of a liability rule is often made because it facilitates a combination of efficiency and distributive results which would be difficult to achieve under a property rule."[182]

To state this potential in this Article's terminology, FIPs can play a significant role in the construction of multidimensional information territories that insulate personal data from socially harmful kinds of observation and use by different parties. Laws such as the Video Privacy Protection Act, the Privacy Act, and the Cable Communications Act already create such multi-dimensional realms for certain kinds of personal information in the offline world. Yet, FIPs are also not without potential shortcomings. FIPs will fall short as an instrument of privacy policy if structured only as command-and-control rules, which mandate rigid outcomes and sometimes even specify the precise means, such as the kind of equipment, to be used by industry.[183] As scholars have argued concerning environmental regulation, command-and-control regulation tends to freeze development of technologies and discourage recourse to less costly alternatives.[184]

The form of FIPs becomes quite important, therefore, and even more so because of the positive, if slow, movement in favor of them for Internet privacy. Recently, for example, a majority of the Commissioners of the FTC as well as a few voices in the computer industry, including Andrew Grove of Intel, have called for enactment of a federal Internet privacy statute based on FIPs.[185] While many in government and industry remain unconvinced, this

---

180. A leading example is found in the Privacy Act of 1974, 5 U.S.C. §§ 552a(d), (e), (g) (1994). For analysis of these aspects of the law, see SCHWARTZ & REIDENBERG, *supra* note 85, at 91-128.

181. Merges, *supra* note 140, at 1310-20.

182. Calabresi & Melamed, *supra* note 7, at 1110.

183. *See* Robert N. Stavins, *Economic Incentives for Environmental Regulation*, in 2 DICTIONARY OF ECONOMICS & LAW, *supra* note 70, at 6, 7.

184. *See id.*; Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129, 164-79 (1998).

185. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000) <http://www.ftc.gov/> (calling by 3-2 vote of Commissioners for enactment of federal privacy legislation for the Internet); Ted Bridis, *Intel Chairman Says He Favors Sales Tax on Internet Purchases*, WALL ST. J., June

modest movement in favor of FIPs for the Internet is striking compared with the monolithic belief of only a few years ago in favor of the private sector's self-regulation.[186]

B. Getting the Mixture Right

How may FIPs best be shaped as a policy tool for Internet privacy? As standards for the fair treatment of personal data, FIPs are the most apt policy tool for information privacy on the Internet. However, FIPs should carefully mix mandatory rules and default rules. Briefly stated, where private bargaining about data processing is most likely to fail, mandatory rules should set immutable standards. Because the potential price of mandatory standards is regulatory rigidity, however, where potential exists for private negotiations, FIPs should only establish default rules that set a baseline for negotiations. Thus, where Lessig relies on property and unrestricted negotiations about personal data use, liability standards may be more appropriate. Only against this background is there room for bargaining around defaults, which, in the terminology of Calabresi-Melamed, should be seen as property standards.

To start our examination of these topics, mandatory and default standards must be described. *Mandatory rules* cannot be altered; in contrast, *default rules* are gap-filling terms that may be changed. For example, the UCC contains a mandatory requirement that all parties perform contracts in good faith, but permits parties to contract around most other rules of contract law.[187] In corporate law, parties are not free to negotiate around the detailed set of rules for corporate directors that "prevent fraud and opportunism."[188]

As for the second set of terms, they concern a further refinement of default rules, which can be set as either an "opt-out" or an "opt-in." The Gramm-Leach-Bliley (GLB) Act of 1999 and a proposed amendment to it demonstrate these two alternatives. The GLB Act repeals the Glass-Steagel Law, which was enacted during the Great Depression and placed a wide range of legal restrictions on financial institutions.[189] Crucial for our purposes

---

7, 2000, at B2 (stating Andrew Grove's belief that federal Internet privacy laws are "inevitable" as well as "preferable to a patchwork of privacy laws in 50 different states"); Keith Perine, *On Privacy, Ebay Prefers Feds Over States* (last modified May 18, 2000) <http://www.thestandard.com/article/display/1,1151,15274,00.html>.

186. *See* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT 8 (1998) (noting the President's proposals for private sector leadership and self-regulation of the Internet).

187. U.C.C. § 1-203 (1994).

188. John C. Coffee, Jr., *The Mandatory/Enabling Balance in Corporate Law: An Essay on the Judicial Role*, 89 COLUM. L. REV. 1618, 1624 (1989). *See* Jeffrey N. Gordon, *The Mandatory Structure of Corporate Law*, 89 COLUM. L. REV. 1549, 1555-85 (1989) (describing the role that mandatory rules play in a contractual system).

189. Gramm-Leach-Bliley, Pub. L. No.106-102, 113 Stat. 1338, (codified at 15 U.S.C. § 6801 (1999)).

is that GLB generally allows financial institutions to share personal financial data among their affiliates, but requires consumers to be informed of this practice and to be permitted to stop it as it concerns their own data.[190] Thus, GLB sets a privacy default as an opt-out—information will be shared unless consumers object to the practice. In contrast, the Clinton Administration backs a financial privacy bill that would reverse this aspect of GLB.[191] The Clinton proposal would prevent financial institutions from sharing information among affiliates unless consumers explicitly agreed to this practice. Here, the default is set as a privacy opt-in—information will not be shared unless consumers agree to the practice.

How should FIPs combine mandatory and default rules for cyberspace privacy? This question is important because private negotiations under current conditions are likely to have a range of problematic consequences. Due to the extent of the failure in the privacy market, the law at present should generally seek to minimize harms that flow from reliance on bargaining among consumers and data processors. In the formulation of Robert Cooter and Thomas Ulen, such an approach represents the "normative Hobbes theorem" of law: "Structure the law so as to minimize the harm caused by failures in private agreements."[192] Recourse to FIPs in this fashion will have another benefit. Lessig's great insight in *Code* is that a central fashion in which regulation takes place in cyberspace is through code, that is, through technological configurations and system design choices. The enactment of FIPs through statutory law and the judicial and administrative interpretation of these standards will have the crucial benefit of involving these institutions in the process of creating code for Internet privacy.

To begin then with the *mandatory* elements of FIPs, we should require them for the most significant procedural aspects of FIPs and the most sensitive substantive areas of data processing. For example, individuals should not be able to negotiate out of the notice requirement of FIPs. The harmful effect of information asymmetries is already significant enough so that notice should be mandatory. Moreover, an Internet privacy statute should seek to avoid the notice-and-consent approach that Web sites now frequently offer, which only present take-it-or-leave-it terms—and ones that

190. *Id.* at Title V, Subtitle A, § 502. For the regulations required under GLB, see FTC Privacy of Consumer Financial Information, 65 Fed. Reg. 11,188 (Mar. 1, 2000) (to be codified at 16 C.F.R. pt. 313); Dept. of Treasury, Office of the Comptroller of the Currency, Privacy of Consumer Financial Information, 65 Fed. Reg. 8,789 (Feb. 22, 2000) (to be codified at 12 C.F.R. pt. 40).

191. Consumer Financial Privacy Act, H.R. 4380, 106th Cong. (2000). For details on the Clinton Administration's views regarding financial privacy, see White House, *The Clinton-Gore Plan to Enhance Consumers' Financial Privacy: Protecting Core Values in the Information Age,* (last modified May 1, 2000) <http://www.whitehouse.gov/WH/New/html/20000501_4.html>.

192. COOTER & ULEN, *supra* note 104, at 99.

are frequently vague.[193] This statute should therefore include a mandatory rule that spells out the elements required for notice to be valid. Such specification of notice is already found in the Children's Online Privacy Protection Act (COPPA), the FTC's regulations under it, and the Department of Health and Human Services' proposed regulations for health care privacy.[194] Finally, beyond notice, an access interest should be mandatory. COPPA also reaches this judgment by granting parents a right to have access to any personal information of their children that is collected and stored online.[195]

As for the substantive areas for mandatory rules, we should require them in sensitive sectors where the potential harm to affected parties or parties external to the data use is so great that our society cannot rely on negotiations around default rules. Law enforcement provides perhaps the clearest example of a sector where mandatory rules are needed. Immutable rules are already used in this context in the off-line world where we have not depended on contracting around off-the-rack terms as the way to resolve issues about law enforcement agencies' access to personal data.[196] In cyberspace as well, three-party negotiations involving law enforcement agencies, ISPs, and consumers are unlikely to reach the proper level of disclosure of personal data generated on the Internet.[197] In this context, interestingly enough, we see that FIPs at times provide a *weaker* level of protection than in Lessig's property regime. Nevertheless, the most powerful limits on access to personal information are not always the best for society as a whole. In the law enforcement arena, for example, use of personal data often takes place when an individual would *not*

---

193. On the failure of notice-and-consent, see Schwartz, *Privacy and the State*, *supra* note 91, at 26-27.

194. *See* 15 U.S.C. § 6502(b)(1)(A)(i) (1994) (COPPA's requirement of notice); Dept. of Health and Human Services, 64 Fed. Reg. 59.918 (Nov. 3 1999), 16 C.F.R. § 312(c) (2000) (F.T.C. regulation under COPPA regarding notice to parents); Dept. of Health and Human Serviees, 64 Fed. Reg. 59,978 (Nov. 3, 1999) (to be codified at 45 C.F.R. pt. 164.512).

195. 15 U.S.C § 6502(b)(1)(B)(iii) (1994); 16 C.F.R. § 312.6 (2000) (health care regulations).

196. The law enforcement exception proved to be the single most difficult drafting issue in the failed attempt during the 105th Congress to enact a health information privacy bill. *See* Fair Health Information Practiees Aet of 1997, H.R. 52, 105th Cong. § 2(a)(5), §§ 119-120 (1997) (providing for disclosure of health information to a law enforcement agency in eertain limited circumstances). For a proposal concerning law enforcement access to cyberspace information, see Kang, *supra* note 8, at 1292-93.

197. To the extent that these rules are expressed through law, parties can, of course, seek to alter them through recourse to the legislative arena. The appropriate mandatory norm for cyberspace should make use of the judiciary and its power to issue subpoenas: a law enforcement agency should be permitted to obtain protected personal data only upon a showing of clear and convincing evidence of materiality to criminal activity. This kind of disclosure requirement is already required by law for the personal data that cable companies collect. 47 U.S.C. § 551(h) (1994).

otherwise want her personal information to be collected. American society has safeguards in place, including important constitutional ones, before wiretaps or other kinds of surveillance can be carried out. Yet, these protections do not generally require law enforcement officers to negotiate with the concerned party for permission to listen or watch. Law enforcement organizations do not have such an obligation, of course, because their surveillance requires a certain level of secrecy to be effective. This example stands as a more general indication, moreover, of circumstances where the optimal social utilization of personal information is reached neither through individual control nor through propertization of data.[198]

As a further example of this point about FIPs, consider the Federal Bureau of Investigation's deployment of a controversial system called "Carnivore" to covertly search e-mail traffic.[199] The Clinton administration has now introduced a bill that would set out explicit standards for such law enforcement eavesdropping on e-mails.[200] Leaving aside any merits or weaknesses of this particular proposal, Congressional enactment of a statute in this area, and one that requires judicial approval of any government interception of e-mails, would involve American democracy's essential institutions in the shaping of code for Internet privacy.

The consequence of the immutable rules is that the remaining realm for negotiated privacy in cyberspace is likely to be more restricted than in Lessig's *Code*. Yet, information privacy law for the Internet should not only consist of immutable rules. How should default rules be set for cyberspace? A *default rule* should permit private negotiations where parties have potential to reach agreements that internalize the kinds of privacy externalities that this Article has described. Our aim should be to encourage data processors to invest in privacy enhancing technologies and to compete with each other regarding information privacy. Furthermore, we should help private parties learn to negotiate for privacy terms.[201] Yet, here too, minimization of the harms caused by failures in private agreements must be sought. As a result, a default norm for cyberspace privacy should generally be set as an opt-in. The result of an opt-in default is that consumer inaction will lead to non-disclosure of personal data. This kind of default places the onus on data processors to convince consumers to agree to their terms by offering more products or services in exchange for data. Some existing privacy laws in the

198. *See supra* Part I.D.3.

199. Federal Bureau of Investigation, *Carnivore Diagnostic Tool* (visited July 24, 2000) <http://www.fbi.gov/programs/carnivore/carnivore2.htm>; Declan McCullagh, *FBI Gives a Little on Carnivore* (last modified July 25, 2000) <http://www.wired.com/news/politics/0,1283,37765,00.html>.

200. Stephen Labaton with Matt Richtel, *Proposal Offers Surveillance Rules for the Internet*, N.Y. TIMES, July 18, 2000, at 1.

201. *But see* Rose, *supra* note 140, at 2199 (moving to liability rules may prevent parties from learning to bargain for themselves).

United States, as well as internationally, have taken a similar approach to narrow use of a consent requirement by first spelling out statutory restrictions on the use of personal data. Because formal consent will be necessary only under circumstances when the processing of information occurs beyond the functionally necessary, consent will also be sought less frequently and subject to greater scrutiny by individuals.[202]

A default standard should require collection of only the minimum amount of personal data necessary and further transmission of this information only for purposes that are compatible with the original collection.[203] The idea of minimization requires the collection of the least amount of personal data necessary to accomplish the underlying purpose for which the information is sought.[204] The idea of compatibility calls for a significant degree of convergence between the purpose for which the personal information was gathered and any subsequent use.[205] A move beyond this default norm by data processors would require formal consent, that is, opt-in, from individuals.[206] This approach will lead to a higher quality of negotiations than those around either opt-out or the current informal standard of maximum information disclosure on the Internet.

The use of opt-in defaults will also encourage investment in privacy enhancing technological devices as well as help stimulate the necessary

---

202. To point to an American example, this model is followed by the Cable Communications Policy Act of 1984, 47 U.S.C. § 551(b) (1995). Moreover, in the Federal Republic of Germany, the Teleservices Data Protection Act of 1997 provides strong limitations on the use of personal information by providers of telecommunication services, including Internet Service Providers. An English text of this important statute is reprinted in THE PRIVACY LAW SOURCEBOOK 369 (Marc Rotenberg ed., 1999). For analysis of this law, see JOEL R. REIDENBERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES 22-115 (1998). This report, which was commissioned by the European Union's Directorate General on Internal Market and Finance Services, examines the emerging response to issues of online privacy in Belgium, France, Germany, and the United Kingdom. It is available at <http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.htm>.

203. For a health care privacy bill from the last Congress that attempted a similar approach, see Fair Health Information Practices Act of 1997, H.R. 52, 105th Cong. § 2(a)(5) (1997). For a discussion of this proposed approach for health care information, see Schwartz, *Privacy Economics, supra* note 8, at 59.

204. For an analogous recommendation, see Kang, *supra* note 8, at 1290. The Children's Online Privacy Protection Act (COPPA) targets one aspect of the existing Internet standard of maximum information disclosure by including a requirement of data minimization for Web contests and sweepstakes directed at children. COPPA states that Web sites may not "conditio[n] 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." 15 U.S.C. § 6502(b)(1)(C).

205. In the context of the Privacy Act, the Third Circuit has carried out an insightful discussion of "compatibility." *See* Britt v. Naval Investigative Serv., 886 F.2d 544, 550 (3rd Cir. 1989).

206. Ayres & Gertner, *Optimal Choice, supra* note 8, at 761.

adoption and use of these instruments. Once more effort is required to obtain personal information, these companies will have more interest in investment in privacy enhancing technologies, including technologies that provide anonymous interactions on the Internet. Put differently, opt-in may help to solve the "blinking twelve" problem by forcing companies to invest in good interface design. FIPs that set opt-in defaults will thereby help curtail a socially unproductive subsidy to online data processors.

As a final observation, the use of default rules introduces a modest recourse to property solutions against a thick background of liability rules. A privacy default requires agreement *ex ante* before any data use beyond the functionally necessary. Thus, only under careful circumstances, do we rely in this area on the property rule as set out under the Calabresi and Melamed framework: the transfer of the entitlement under an opt-in default rule takes place only with the holder's consent. FIPs are to begin with immutable standards based on liability rules, but interject negotiations and property rules through careful settings of defaults. Only at this point do we carefully move back to Lessig's starting point and permit a narrow space for trading personal information. It would be a mistake to assume, however, that Lessig's propertization and the FIPs advocated by this Article are merely two means that reach the same end. The results of the two different starting points are likely to be quite different. One merit of FIPs is that they guarantee, as I have argued above, the involvement of democratic institutions in the process of crafting rules for the use of personal information. These institutions furnish important fora for developing non-market perspectives on the increasingly market-driven process of trade in commodified personal information. A second benefit of FIPs as a starting point is that they allow us to draw on the history of information privacy law and to benefit from lessons learned. Issues regarding information privacy take place no more in a historical vacuum than they do in a social one.[207] Finally, FIPs have the potential to dislodge the bad privacy equilibrium that is now in place on the Internet. As I have noted above, a real danger is that sufficient use will not be made of P3P by privacy first-movers. If this result occurs, a propertization of personal data combined with Lessig's Cyber-Jeeves will have a negative social impact by helping to lock in the current low level of Internet privacy.

CONCLUSION

This Article has described and criticized the "Lessig two-step" for Internet privacy: (1) the legal assignment to every individual of a property

207. For a survey of some of the privacy battles won and lost and the lessons to be learned, see generally LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE 130-36 (1997); PRISCILLA REGAN, LEGISLATING PRIVACY (1995); FLAHERTY, supra note 27, at 371-407.

interest in her own personal information, and (2) the employment of software transmission protocols, such as P3P, to permit the individual to structure her access to Web sites. Lessig's proposal for privacy contradicts his stand against PICS, a software transmission protocol for filtering Internet content reminiscent of P3P. Once privacy is placed in a social context, as Lessig does for speech, P3P seems far less attractive an option. In particular, we must consider the difficulty of designing good user interfaces and the likelihood that most people will never master or even use P3P.

Beyond these initial criticisms of the Lessig prescription for Internet privacy, his underlying paradigm, which seeks to increase personal control of data, is questionable. In place of Lessig's idea that privacy protects a right of individual control, this Article has developed a concept of constitutive privacy. Information privacy is a constitutive value that safeguards participation and association in a free society. Rather than simply seeking to allow more and more individual control of personal data, we should view the normative function of information privacy as inhering in its relation to participatory democracy and individual self-determination. Information privacy rules should carry out a constitutive function by normatively defining multidimensional information territories that insulate personal data from the observation of different parties.

A privacy market can play a role in helping information privacy fulfill this constitutive function. Yet, Lessig's propertization of privacy raises a further set of difficulties. Propertization à la Lessig will only heighten flaws in the current market for personal data. This consequence follows from numerous shortcomings in this market and structural difficulties that indicate the unlikelihood of a self-correction in it. Moreover, in revisiting Calabresi and Melamed's work regarding the comparative merits of property and liability regimes, a mixed regime should be preferred for Internet privacy over Lessig's pure property regime.

Turning from criticism to prescription, this Article then developed the mixture of property and liability rules necessary for establishment of information privacy standards in cyberspace. Recourse to Fair Information Practices (FIPs) offers the best way to establish rules for the fair treatment of personal data on the Internet. Yet, FIPs are not without potential shortcomings if structured only as command-and-control rules. Therefore, an American Internet privacy law consisting of FIPs should include both mandatory and default elements.

This Article goes beyond Lessig's *Code* in its consideration of Internet privacy. Still, it must return to Lessig's great insight: that a central fashion in which regulation takes place in cyberspace is through "code," that is, through technological configurations and system design choices. The enactment of FIPs through statutory law and the judicial and administrative interpretation of these standards will have the crucial benefit of involving democratic institutions in the process of shaping the code of Internet privacy.

Where additional work must be done is in evaluating both the potential and the pathologies of democratic institutions in the specific context of information privacy. How can we draw on the promise of these institutions and correct for their shortcomings when using them to shape technological and market-based solutions for Internet privacy? The path of scholars should be in seeking to understand the existing and likely dynamics of different State actors in the promotion of information privacy on the Internet.