Stanford Technology Law Review

Fair Information Practices and the Architecture of Privacy

(What Larry Doesn't Get)*

MARC ROTENBERG†

CITE AS: 2001 Stan. Tech. L. Rev. 1
http://stlr.stanford.edu/STLR/Articles/01_STLR_1

I. INTRODUCTION

¶1 Larry Lessig's *Code and Other Laws of Cyberspace* has popularized the view that "code is law."[1] The observation, roughly stated, is that decisions regarding the architecture of the evolving communications infrastructure exercise control over individuals much like legal code, and therefore should be subject to democratic considerations such as accountability and public participation. The argument has attracted critics from the libertarian wing of the cyberintelligentsia[2] who see it as an invitation to government intervention and supporters on the liberal/communitarian/progressive (choose one) side who at last have a richly argued intellectual framework with which to explore the role of the public in the decisions made by large private entities.[3]

¶2 In my view, there is much in *Code* that is very useful. The book provides a reasoned, skeptical view of the benefits of technology and a broad-ranging exploration of the interaction of technology, norms, law and policy. However, a significant part of *Code* is deeply flawed, and that is the discussion of privacy.

---

* In offering this title, I am following the convention that is appropriate for this genre. Responses in the spirit of "What Marc Doesn't Get" are welcome and should be sent to rotenberg@epic.org.

† Executive Director, Electronic Privacy Information Center, Washington, DC; Adjunct Professor, Georgetown University Law Center, 1990-; Co-editor, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (1997); Editor, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (1999); Former counsel, Senate Judiciary Committee, Subcommittee on Law and Technology.

[1] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999). Although action figures and brightly colored lunch boxes have not yet appeared at Toys 'R Us, we can reasonably expect that law school bookstores will soon offer bumper stickers and T-shirts with the now famous slogan.

[2] Joseph Weizenbaum, distinguished professor of computer science at MIT and author of the ELIZA program, used the term "artificial intelligentsia" to critique popular punditry on artificial intelligence and its impact on social life. *See* Joseph Weizenbaum, *The Computer in Your Future*, N.Y. REV. OF BOOKS, Oct. 27, 1983, at 58-62 (reviewing FEIGENBAUM & MCCORDUCK, THE FIFTH GENERATION: ARTIFICIAL INTELLIGENCE AND JAPAN'S COMPUTER CHALLENGE TO THE WORLD (1983)).

[3] *See* David Post, *What Larry Doesn't Get: A Libertarian Response to* Code and Other Laws of Cyberspace, 52 STAN L. REV. 1439 (2000). Lessig was a special master in the government's case against Microsoft.

¶3 In this article, I look closely at Lessig's discussion of Internet privacy in *Code and Other Laws of Cyberspace*. In many areas, I find his argument without foundation and his characterization of key references, such as the European Union Data Directive, deeply flawed. I am particularly bothered by his failure to consider the relevant and very useful experience of courts and legislatures that have addressed the problem of how to protect privacy in an era of rapidly changing technology.

¶4 However, it is not only the purpose of this critique to argue that Lessig should consider much more carefully the recent political dimensions of the privacy issues. I am also interested in the conceptual problems with Lessig's analysis, and specifically why an argument that seems reasonably well-grounded in the relevant legal antecedents seems to veer so wildly and unpredictably to an undesirable and inconsistent outcome. In this venture, I am concerned not only about Lessig's proposed solutions to the far-reaching problems in the privacy arena, but more generally about what his argument may suggest about the invitation to promote discussions of code.[4] On one hand, he asks us to view the design of code as citizens and to look at the role of public institutions in shaping the architecture of cyberspace. Who could turn down such an invitation? On the other, he recommends that we forgo well known principles of privacy protection and adopt instead a technique that leaves individuals, confronted by a common problem, isolated in the marketplace. How could he reach such a conclusion?[5]

¶5 If the results produced in the areas outside of the privacy field are akin to those produced in the privacy field, then something is very much askew in Lessig's description of the relationship between code and law. If the code that results is so much at odds with the values that society wishes to protect, then code becomes a means by which to transfer decisions from the public realm to the privatized realm. In the use of the technique proposed by Lessig, it is a way to convert political rights into market commodities. I do not believe that this was Lessig's intent, but this is the conclusion that emerges from a close reading of his chapter on privacy in *Code and Other Laws of Cyberspace*.

A. "Code as Law:" No Kidding

¶6 To those who have followed and participated in the privacy debates over the past decade, the observation that code is law seems hardly remarkable.[6] When Lotus and Equifax proposed to join their credit record information and demographic data and make the resulting product available on inexpensive CD-ROMS to anyone who wished to purchase it, computer scientists identified various risks to privacy and advocates and the public joined in a campaign to stop the release of the product.[7] Decisions about the design of Lotus: Marketplace would

---

[4] In fairness to Lessig, he has at various times said things about privacy that were more in line with the view favored in this article than those originally set out in *Code*. But *Code* is an influential work, and it is important to consider the privacy argument put forward in its pages without regard to extra-textual material.

[5] *See* discussion *infra* Part II.

[6] Even before the recent public protests over architectures of surveillance, philosophers, journalists, sociologists and others have observed the relationship between design and methods of social control. *See generally* JEREMY BENTHAM, PANOPTICON (1791); JACQUES ELLUL, THE TECHNOLOGICAL SOCIETY (1964); DAVID BURNHAM, THE RISE OF THE COMPUTER STATE (1983); MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1995); OSCAR H. GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (1988).

[7] LAURA J. GURAK, PRIVACY AND PERSUASION IN CYBERSPACE: THE ONLINE PROTESTS OVER LOTUS MARKETPLACE AND THE CLIPPER CHIP 19-31 (1997); *see also* Langdon Winner, *A Victory for Computer Populism*, TECH. REV., May-June 1991, at 66.

obviously have an impact on individuals outside the realm of law and regardless of whether individuals exercised "choice" in the marketplace. The campaign was remarkable because it was not directed at a legislative body, but rather at the development of a new product that would make personal information available for sale and marketing use. Similar issues arose when Lexis-Nexis decided to make available the Social Security Numbers of individuals through its online news service, and when the Social Security Administration chose to make Personal Earning Benefits Estimate Statements (PEBES) available online.[8] More recently, questions about design and privacy were raised by Microsoft's plan to incorporate a global unique identifier into its product registration program, RealNetwork's secret collection of the email addresses of users who downloaded streaming audio and video, and the merger of Internet advertising giant Doubleclick with the catalog database firm Abacus direct.[9]

¶7 The power of code as law (or "architecture as policy") was also clear in the debates over encryption policy, in which law enforcement agencies sought to obtain by means of technical standards what they could not achieve through the legislative process.[10] For example, the U.S. government tried through a variety of means to enforce adoption of an escrow encryption standard that would enable law enforcement access to private encoded communications.[11] As there was no legal requirement that companies follow this standard, at least for the sale of products in the United States, and the likelihood of obtaining a political consensus in support of the goal was minimal, the government used export controls, federal contracting, funding and coercion to urge adoption of the key escrow standard.

¶8 Ultimately the Organization for Economic Cooperation and Development, a multi-national trade organization based in Paris, rejected this approach to the development of cryptographic standards. In 1997, the OECD issued the Cryptography Guidelines with the support of the 29 member nations, and the United States government gradually, albeit grudgingly, throttled back its attempt to require technical standards that would enable law enforcement access to private messages.[12] Critics of the Clipper proposal noted that the government had attempted to achieve through architecture and design what it could not obtain through the legislative process.

¶9 The battle over the Communications Assistance for Law Enforcement Act of 1994 is a particularly interesting example of how the "code as law" problem played out. Prior to 1994, it was generally understood that telephone companies had an obligation to comply with a lawful warrant, but there was no general requirement that communications providers alter the design of a network to enable the execution

---

[8] I will use the term "code" throughout this article to mean the design of information systems generally, although I recognize that Lessig probably has in mind the more limited application to the protocols and design choices currently associated with the Internet.

[9] *See Microsoft Will Alter Its Software In Response to Privacy Concerns*, N.Y. TIMES, Mar. 7, 1999, at A1; *Tracking Efforts to Halt, Firm Promises DoubleClick Will Await Guidelines on Web Privacy*, USA TODAY, Mar. 3, 2000, at 1B; *Net Privacy Concerns Mounting*, USA TODAY, Nov. 15, 1999, at 6E.

[10] *See generally* ELECTRONIC PRIVACY PAPERS (Bruce Schneier & David Banisar eds., 1997); WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE (1998).

[11] The technical standards were given various names: the Clipper proposal, the Escrowed Encryption Standard (FIPS 185), Mandatory Key Escrow, Commercial Key Escrow, Commercial Key Recovery, Message Recovery. Although the name frequently changed, the tune remained the same: all of these standards were intended to give government agents access, by means of code, to private messages that they might not otherwise obtain. Privacy advocates who grew tired of the repackaging of the proposal eventually adopted a more simplified nomenclature: Clipper, Clipper 2.0, Clipper 2.1, Clipper 3.0, etc..

[12] PRIVACY LAW SOURCEBOOK 305-13 (Marc Rotenberg ed., 1999) (OECD Cryptography Guidelines).

of a future warrant.[13] Indeed, it was fairly well understood that the purpose of the federal wiretap statute was to constrain the actions of government, not coerce the actions of private individuals.[14]

¶10 All of this changed when CALEA (the "digital telephony" proposal) became law.[15] The law gave the FBI the authority to set technical standards to enable access to private communications. The statute set out functional requirements that would enable this access, and all communication service providers were required to comply or face substantial penalties. The underlying purpose of the federal wiretap statute, and the two Supreme Court decisions from the 1967 term on which the Act was based, was turned upon its head: wiretap law no longer acted as a constraint on government, but instead became a means to coerce private behavior. Where once techniques were designed to minimize government surveillance and limit the risk of abuse, they would now be developed to enable greater government access to private messages and compel telephone service providers, equipment manufacturers and distributors to design devices to promote government surveillance. Law had transformed code.

¶11 Today, civil liberties organizations continue to fight the battle against CALEA, arguing in federal court that the FCC has ignored privacy considerations in its regulations.[16] However, the fundamental problem with CALEA goes far deeper than whether the FCC has complied with the requirement set out in the statute to consider privacy; it is that a law that was intended to encode restrictions upon government surveillance now compels public compliance in the design of techniques to enable government surveillance.

¶12 Even before the campaigns of the 1990s were those in the 1980s that concerned the emergence of the Caller ID service and a new architecture of the nation's telephone system, which would enable recipients to learn the phone number, though not necessarily the identity, of call originators. The Caller ID service represented a radical change, from a privacy viewpoint, in the architecture of the nation's telephone system.[17] The central claim of privacy, that individuals should have the right to determine when to disclose personal information to others, would effectively be transferred from telephone customers to telephone companies. These companies now found themselves in the enviable position of being able to sell to call recipients the right to know the telephone number of the calling party (the Caller ID service) as well as the right to sell to call originators the right to block disclosure of their telephone number (the Caller ID blocking service). This transfer

---

[13] In 1970 the federal law was amended to make clear that a communications carrier had to comply with a warrant. Pub. L. No. 91-358, tit. II, § 211(b), 84 Stat. 654 (1970). Until 1970, cooperation of the telephone company in the execution of a warrant was optional. The 1970 amendment came about after a telephone company in Nevada refused to comply with a warrant. EDITH J. LAPIDUS, EAVESDROPPING ON TRIAL 123 (1974).

[14] The federal wiretap statute includes elaborate restrictions on the use of wiretap authority. *See generally* JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE (Supp. 1999); CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING (1978); LAPIDUS, *supra* note 13.

[15] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010).

[16] *See* Brief of Electronic Privacy Information Center, et al., United States Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000) (Nos. 99-1442, 99-1466, 99-1475, 99-1523), *available at* http://www.epic.org/privacy/wiretap/calea/reply_brief.pdf.

[17] *See Telemarketing/Privacy Issues, Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce*, 102d Cong., 1st Sess. 43 (1991) (testimony of Marc Rotenberg) ("Caller ID is directly at odds with well established legal and ethical standards for privacy protection. . . . Telephone subscribers are entitled to decide when, to whom, and under what circumstances they should disclose their phone numbers."); *Investigation of New England Telephone and Telegraph Company's Phonesmart Call Management Services, Before the State of Vermont, Public Service Board*, Docket No. 5404 (Vt. 1991) (expert testimony of Marc Rotenberg).

of control over personal information, made possible by the transition from Signaling System 6 to Signaling System 7, raised a serious question about the role of code and the protection of privacy. The Caller ID service could be offered without any blocking of the call originators' phone number; it could be offered with per-call blocking or with per-line blocking. These were technical determinations within the control of the telephone company that would effectively allocate privacy rights among telephone customers.[18]

¶13 Fortunately, the Caller ID proposal arose in a regulatory environment that enabled public participation in the rule-making procedure. It would not simply be for the telephone companies to decide how they would collect and use information about customers: they would have to answer questions about the impact on customers. For example, should a woman calling her children from a shelter for battered women be forced to disclose the location of the shelter to her estranged spouse? Is it reasonable to ask telephone customers to select call blocking for each call if they would normally wish not to disclose their telephone number? Finally, what actual interest would a government agency or a private business have in knowing the telephone number of a calling party?[19]

¶14 Proceedings were brought before almost every public utility commission and public service commission in the United States and in several courts.[20] In many jurisdictions, free per-call blocking was mandated and in some, per-line blocking. As Mukherjee and Samarajiva have noted, as time progressed and state regulatory bodies learned more about the Caller ID service, they were more likely to adopt stronger privacy measures—that is to say, technical rules that would allow telephone customers to retain greater control over the decision of when to disclose their personal information to others.[21] In the end, these deliberations helped ensure that the final technical standards implemented by the telephone companies reflected, at least to some extent, the public's interest in the protection of privacy. Law controlling code.

¶15 Some or all of this history may have been useful for Lessig's consideration of the interplay of code, law, and privacy norms, as many of the issues that seem to interest him have, to some extent, already played out. The history of privacy protection is the history of the effort to regulate the design of technology ("code") by means of public institutions. This effort has always been predicated on the belief that architecture is not pre-determined, that it can be made subject to reason, public debate, and the rule of law.

¶16 There is also in this history a very useful literature that has helped shape public policy and enabled legal writers and technical experts to make a contribution to the enterprise of privacy protection in the information age.[22] As I will describe below, many of the key approaches to privacy protection are already well understood: for

---

[18] *See* Reshmi Mukherjee & Rohan Samarajiva, *Regulating "Caller ID": Emulation and Learning in the Policy Process*, 20 TELECOMMUNICATIONS POL'Y 531 (1996).

[19] Useful advice about the Caller ID service may be found in BETH GIVENS, THE PRIVACY RIGHTS HANDBOOK 45-50 (1997).

[20] *See* Barasch v. Pennsylvania Pub. Util. Comm'n, 576 A.2d 79 (Pa. Commw. Ct. 1992); Southern Bell Telephone v. Hamm, 409 S.E.2d 775 (S.C. 1991).

[21] Mukherjee & Samarajiva, *supra* note 18, at 537.

[22] *See generally* PHILIP AGRE & MARC ROTENBERG, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (1992); COLIN BENNETT, REGULATING PRIVACY (1992); ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS? (1997); Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96.

example, the enforcement of Fair Information Practices, the development of genuine privacy enhancing technologies, and the institutional importance of privacy agencies.

¶17 When, for example, the German government chose in a new communications bill to include a provision that will encourage the development of anonymous payment systems for electronic commerce, it was building upon a critical tradition that joins a legal concept which places anonymity at the core of privacy and a technical expectation that such interests can be designed and encouraged in the policy process.[23] This is "Code as Law," but in a more profound, more developed sense than the way Lessig uses the phrase. It is a result that draws upon an understanding of the relevant developments in law and technology, not one that simply announces the obvious intersection.

¶18 One need not accept this tradition uncritically.[24] But one must at least engage this history, assess it, review it, and reject it if appropriate. It simply can never be a sufficient answer to say that with the arrival of the Internet all that has come before is no longer relevant. That is hardly an invitation to reasoned discussion.

B. Lessig's Discussion of Privacy

¶19 At the outset, much of Lessig's discussion of privacy issues reflects the common understanding of the development of privacy law in America.[25] He notes with approval the Supreme Court's decision in *Katz v. United States* [26] to extend the reach of the Fourth Amendment to protect the new communications infrastructure, and perhaps more significantly embraces the interpretivist approach set out by Justice Brandeis in the *Olmstead* dissent, which calls on courts to extend the principles enshrined in the Constitution as new technologies evolve.[27] He says elsewhere that the Constitution as applied to "cyberspace" does not determine outcomes, a view somewhat at odds with Brandeis' analysis in the *Olmstead* dissent, but he also rejects the crabbed original intent view articulated by Chief Justice Taft in that case.[28] Thus, he has left the door open for a robust application of constitutional principles in the emerging communications realm.

¶20 Lessig also shows some sensitivity to and support for one of the hot topics in the privacy world—the protection of anonymity.[29] He recounts, for example, the experience of buying alcohol in a local store only to be questioned later by his school tutor about his purchase. He asks, quite reasonably, why one aspect of a person's private life should be made known to someone who occupies an unrelated position in that person's life. He considers issues of architecture and notes

---

[23] PRIVACY LAW SOURCEBOOK, *supra* note 12, at 371 (German multi-media law).

[24] *See, e.g.*, COLIN TAPPER, COMPUTER LAW 361-62 (4th ed. 1989) (arguing that the UK government was correct to reject the tort of privacy: "It is no accident that the concept of privacy has never been defined at all satisfactorily. It is no more than a name for an attitude towards a set of abuses, very weakly, if at all, associated with each other.").

[25] *See generally* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997); ROBERT B. GELMAN, PROTECTING YOURSELF ONLINE (1998); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971); PAUL M. SCHWARTZ, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996); RICHARD C.TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS (1999); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Reidenberg, *supra* note 22.

[26] 389 U.S. 347 (1967).

[27] LESSIG *supra* note 1, at 111-18; Olmstead v. United States, 277 U.S. 438, 475-76 (1928) (Brandeis, J., dissenting).

[28] LESSIG, *supra* note 1, at 115-16.

[29] *See, e.g.*, Peter Wayner, *A Tool for Anonymity on the Internet*, N.Y. TIMES, Dec. 16, 1999, at G17.

elsewhere that the controls over disclosure of identity may be determined in part by the requirements of a local network.[30] Lessig goes on to embrace the view put forward by Professor Julie Cohen and others that the right to receive information anonymously is so central to the First Amendment that there should be a general right to circumvent techniques that would otherwise block the ability of individuals to get access to information without disclosing their identity.[31] So far, so good.

¶21 But when Lessig tackles the topic of privacy in chapter 11 of his text, he careens from example to example, concept to concept, with little direction and ultimately settles for the coding of a market-based allocation of privacy interests that is remarkable in light of the skepticism toward market-based analyses that much of his book promotes.[32] The chapter is remarkable also in that not a single privacy code of the legal variety is actually considered. Specifically, there is no effort to assess whether laws that have traditionally regulated the protection of privacy interests in new communications settings, such as the subscriber privacy provisions in the Cable Act of 1984 or even the federal wiretap statute adopted in 1968, have been effective, would be appropriate for the Internet, or, as could possibly be argued after reviewing the history of these codes, stand in need of replacement.

1. Definition of Privacy

¶22 Lessig walks through a variety of privacy settings and privacy concepts. He puts some weight on the ideas of "monitoring" and "search," though neither term seems particularly tethered to common concepts of privacy.[33] Lessig describes a person's life as monitored as when "that part of one's daily existence that others see or notice and that others can respond to" and searchable as "the part of your life that leaves . . . a record." [34] It is hard to understand, however, in what sense people who walk down a city street or enters a shopping mall are "monitored." In the absence of a purposeful effort by some entity or device to actually track the actions of a particular individual, we would probably not consider social observation a form of monitoring.

¶23 Consider, by way of contrast, the use of anklets for parolees whose location is constantly monitored, a technique that Professor Gary Marx has aptly described as "electronic leashes."[35] Or the use of the pass card system in South Africa that

---

[30] LESSIG, *supra* note 1, at 26-27.

[31] *Id.* at 139-40. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 1003-38 (1996); *The WIPO Copyright Treaties Implementation Act, H.R. 2281, and Privacy Issues Before the Subcomm. on Telecomm., Trade, & Consumer Protection, House Comm. on Commerce*, 105th Cong., 2d Sess. (1998) (testimony of Marc Rotenberg).

[32] Most privacy literature can roughly be divided into those works that present a list of privacy threats brought about by new technologies (*see generally* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE (1983); SIMSON GARFINKEL, DATABASE NATION (2000); VANCE O. PACKARD, THE NAKED SOCIETY (1964); H. JEFF SMITH, MANAGING PRIVACY (1994)) and those that seek to articulate a robust conceptual framework for a right of privacy (*see generally* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); BENNETT, *supra* note 22; DAVID H. FLAHERTY, PROTECTING PRIVACY IN TWO-WAY ELECTRONIC SERVICES (1984); GANDY, *supra* note 6; MARX, *supra* note 6; WESTIN, *supra* note 25). Journalists typically author the first, scholars the second. Lessig, a scholar writing for a general audience, incorporates both traditions.

[33] LESSIG *supra* note 1, at 143. Such concepts generally turn on denying physical access to one's person or controlling personal information held by another. *See generally* TURKINGTON & ALLEN, *supra* note 25, at 72-74. I will argue below that privacy protection in information law is generally understood as the enforcement of Fair Information Practices.

[34] LESSIG, *supra* note 1, at 143.

[35] Gary T. Marx, *The New Surveillance*, TECH. REV., May- June 1985, at 43, 45-47.

enabled a minority government to exercise control over the larger populace.[36] Or the growing use of workplace surveillance techniques that count keystrokes, calls answered, shopping bags filled, and trips to the bathroom.

¶24 In characterizing "monitoring" as he has, Lessig has removed the essential characteristic—and the key to understanding much of privacy law—the concern that technology allows organizations to exercise control over the actions of individuals. It is this concept of monitoring, one described enthusiastically by Jeremy Bentham in his proposed architecture of the ideal prison—the Panoptican[37]—and more critically by Michel Foucault[38] and Oscar Gandy[39] in their critique of the Panoptican, that has influenced the development of much of privacy law.

¶25 Ultimately, Lessig rests his solution to the privacy problem on two key principles that follow from the search/monitor schema: "any burden [on privacy] must be minimal, and . . . any search must be disclosed."[40] This is not much material with which to build an architecture for privacy.

2. Characterization of Privacy Law

¶26 Lessig's characterization of the development of actual privacy law and specifically the EU Data Directive is simply not accurate. He first says the legal solution to the problem of monitoring is a European approach, presumably in contrast to a U.S. approach.[41] This is an odd conclusion since the historical claim of a legal right against nonconsensual monitoring (photography) is derived from the Brandeis and Warren article of 1890, which was even characterized by European scholars as the "American tort."[42] It is also an odd conclusion since most of the modern statutory law that addresses monitoring by hi-tech devices is of American origin. There is for example, the Federal Wiretap Act of 1968, the Act which followed from the *Katz* decision which Lessig describes earlier in the book, that limits the monitoring of private communications. There is also the Privacy Act of 1974 that established a legal framework for the records collected by the federal government and addressed the specific concern of Big Brother monitoring by means of automated databases. There are, for example, the privacy subscriber provisions of the Cable Act of 1984 (cable television), the Video Privacy Protection Act (video rental records), the Electronic Communications Privacy Act of 1998 (electronic mail), the Polygraph Protection Act of 1998 (lie detectors), and the Telephone Consumer Protection Act of 1991 (auto-dialers and junk faxes). In addition, many laws at the state level are designed to further limit the monitoring of private activities in the United States.[43] There is no comparable set of statutes in

---

[36] NARMIC, AMERICAN FRIENDS SERVICE COMMITTEE, AUTOMATING APARTHEID: U.S. COMPUTER EXPORTS TO SOUTH AFRICA AND THE ARMS EMBARGO (1982). For a most recent survey on the tools of monitoring, see PRIVACY INTERNATIONAL, BIG BROTHER INCORPORATED: A REPORT ON THE INTERNATIONAL TRADE IN SURVEILLANCE TECHNOLOGY AND ITS LINKS TO THE ARMS INDUSTRY (1995).

[37] BENTHAM, *supra* note 6.

[38] FOUCAULT, *supra* note 6.

[39] GANDY, *supra* note 6.

[40] LESSIG, *supra* note 1, at 158.

[41] *Id.* at 159.

[42] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960); John C. Scheller, *PC Peep Show: Computers, Privacy, and Child Pornography*, 27 J. MARSHALL L. REV. 989, n. 97 (1994). *See, e.g.*, John D. R. Craig, *Invasion of Privacy and Charter Values: The Common-Law Tort Awakens*, 42 MCGILL L.J. 355, 382 (1997) ("In fact, such an approach would be preferable to the simple importation of the American tort of invasion of privacy.").

[43] *See* ROBERT ELLIS SMITH, COMPILATION OF FEDERAL AND STATE PRIVACY LAWS (2000). A particularly interesting example of a state privacy law is the recently enacted California statute that attempts

Europe or elsewhere outside of the United States that specifically addresses the problem of monitoring by hi-tech devices.

¶27 While it is true that the EU Data Directive takes a more comprehensive approach to privacy protection in the private sector than does current U.S. law, it can easily be shown that the EU Data Directive came about in response to the economic requirements of the integration of the European national markets in the early 1990's. The harmonization of national law was necessary to promote the free flow of goods, services, labor and capital across the EU's internal borders. United States privacy law, in contrast, is derived from an effort to regulate intrusive monitoring practices made possible by new technologies. In other words, Lessig's characterization of EU privacy law is more aptly applied to the development of privacy law in the United States. This is critical because the argument against government regulation in the United States to protect privacy is oftentimes characterized as inconsistent with an American tradition. But this "American tradition" is a recent creation of lobbyists in Washington.[44] With the historical burden properly allocated, it becomes clear that the appropriate question is not whether the U.S. should suddenly adopt new legislation to protect privacy, but to ask why it should not.[45]

¶28 He next says that the basis of the EU Data Directive is "notice and choice," which is an odd reformulation of a comprehensive legal framework that addresses a wide range of privacy interests, from access and control to security and remedies.[46] The characterization is even more bizarre when one recognizes that the "notice and choice" formulation of privacy protection is a relatively recent creation of the U.S. marketing industry that, embraced by the Federal Trade Commission, almost purposefully attempts to negate the range of rights that are to be found in the EU Data Directive.[47] Prior to the recent efforts of industry to develop a self-regulatory alternative to the EU Directive, European privacy law would have been characterized as "omnibus," by way of contrast to U.S. privacy law, which was termed "sectional."[48] There was no general disagreement about the underlying interests that the law would protect, just differences in the scope of application. The term "sectoral" was used to emphasize that privacy law in the United States

---

to address the problem of the Paparazzi. The statute is noteworthy because it appears to indirectly address the conduct of the media, even though the strong First Amendment tradition of the United States has typically disfavored such legislation. At this time, there is no comparable law in either England or France, even though it was the death of Princess Diana, chased by journalists on the streets of Paris, that was the catalyst for the California legislation.

[44] JOHN B. JUDIS, THE PARADOX OF AMERICAN DEMOCRACY: ELITES, SPECIAL INTERESTS, AND THE BETRAYAL OF PUBLIC TRUST 231 (2000) (describing how the Clinton administration sided with business groups and opposed adoption of legislation to protect Internet privacy).

[45] *See* RICHARD E. NEUSTADT & ERNEST R. MAY, THINKING IN TIME: THE USES OF HISTORY FOR DECISION-MAKERS (1986) (explaining the use of history to establish policy arguments on contemporary matters).

[46] LESSIG, *supra* note 1, at 159.

[47] The concept of "notice and choice" was vigorously promoted by the Direct Marketing Association at a June 4, 1996 hearing held by the Federal Trade Commission. The DMA was seeking to avoid privacy legislation and recommended instead a self-regulatory model based on "notice and choice." Prior to the DMA's announcement hardly any references to this formulation of privacy can be found in the popular literature or legal scholarship. *But see* National Treasury Employees Union v. Von Raab, 489 U.S. 656, 672 n.2 (1989); Laura A. Lundquist, *Weighing the Factors of Drug Testing for Fourth Amendment Balancing*, 60 GEO. WASH. L. REV. 1151, 1207 (1992). The "notice and choice" formulation was adopted by the FTC following the 1996 hearing, though the Commission has since recognized that this phrase is at odds with traditional terminology--including all of United States privacy law--and has subsequently adopted the hybrid "notice and choice/consent."

[48] Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 438 (1995).

had come about on a sector specific basis. Commentators typically explained this development in regard to certain historical circumstances in the United States, such as the compromise that took place between Congress and the Ford White House to obtain passage of the Privacy Act or, the failure of the Privacy Protection Study Commission a few years later to recommend adoption of a comprehensive privacy regimes.[49] It was also understood that in some circumstances the First Amendment presumption against government restrictions on speech would not allow certain privacy laws that limited publication of personal information by news organizations.[50] Still, the structure, purpose and provisions of privacy law between the U.S. and the European countries revealed a high degree of similarity. [51]

¶29 The traditional complement to "notice" had long been "consent," and the problem that attracted privacy scholars and policymakers was to determine what would constitute adequate or meaningful consent. Under the EU privacy regime, meaningful consent typically required "opt-in," i.e., in the absence of affirmative action by the individual, the company simply could not make use of personal information for purposes unrelated to the transaction at hand. U.S. privacy law also followed an opt-in regime, particularly in the medical records field. However, industry groups and the Direct Marketing Association in particular urged the less burdensome "opt-out" regime, which allows businesses to go forward with various uses of personal data as long as there are some means (however burdensome or inefficient) for consumer objections. In the United States, the opt-out regime was typically viewed as what industry was prepared to do and not what the public wanted done.[52]

¶30 The "notice and choice" formulation put forward by the Direct Marketing Association in 1996 provided an opportunity for the marketing industry to avoid resolving the difficult problem of what would constitute meaningful consent. But it had this odd (and for business, highly advantageous) consequence: while both opt-in and opt-out presumed a limited, purpose-specific disclosure of personal information, albeit with differing allocations of burden, the "choice" formulation opened the policy world to the notion that there could be many diverse uses for personal information; instead of asking about a narrow and unrelated use of personal data, companies now were free to propose a wide range of uses for information that might otherwise be kept confidential. In the spirit of the age, one could almost ask, "where do you want your data to go today?"

¶31 This approach was clearly at odds with the general aim of privacy law in both the United States and Europe to limit the collection and use of personal data; it went against the specific European principle of "finality" that makes clear the need to limit data collection to a specific purpose.[53] Indeed, much of privacy law is premised on the idea of discrete transactions involving the transfer of personal

---

[49] JAMES B. RULE ET AL., THE POLITICS OF PRIVACY 63, 101-10 (1980); ROBERT ELLIS SMITH, PRIVACY: HOW TO PROTECT WHAT'S LEFT OF IT 86-87 (1979).

[50] *See* Florida Star v. B.J.F., 491 U.S. 524 (1989).

[51] *See* BENNETT, *supra* note 22; DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA AND THE UNITES STATES (1989). *See also* Colin Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99 (Philip E. Agre & Marc Rotenberg eds., 1997) (on "American exceptionalism").

[52] Public opinion polls have long shown support for opt-in. *See, e.g., Business Week / Harris Poll: A Growing Threat*, BUS. WK., March 20, 2000, at 96, *available at* http://www.businessweek.com/ 2000/00_12 /b3673010.htm. Editorials in papers both in the U.S. and Europe also argued for opt-in. *See, e.g., Virtual Privacy*, ECONOMIST, Feb. 10, 1996, at 16.

[53] Spiros Simitis, *Reviewing Privacy in an Informational Society*, 135 U. PA. L. REV. 707 (1987).

information from individual to institution where it is the individual's expectation—and the institution's responsibility—to ensure that the information will only be used for a well-defined, stated purpose. When you provide information to a state Department of Motor Vehicles, for example, what "choices" over the use of that data, other than to enable your receipt of a license, would you exercise?[54] Likewise, when you answer your doctor's question about the whether you have been sleeping well at night, what choice would you exercise other than to obtain appropriate care from the doctor?

¶32 The problems with the choice formulation also become apparent if one is willing to analogize privacy protection to other forms of health and safety protection. How much choice, for example, should consumers have in the quality of car brakes or airbags? The choice concept also imagines the creation of perfect market conditions where consumers are suddenly negotiating over a range of uses for personal information. Subtly, but powerfully and profoundly, the substitution of "notice and choice" for "notice and consent" transferred the protection of privacy from the legal realm, and from an emphasis on the articulation of rights and responsibilities, to the marketplace, where consumers would now be forced to pay for what the law could otherwise provide.

¶33 It is unfortunate that so much of Lessig's argument appears to be colored by the views of those who identify with the marketing association. He asserts that 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."[55] [Emphasis added]. What is the evidence that this is a "standard response?" Lessig provides a citation to a single web certification association established in 1997.[56] If this is a standard response to the problem of data protection, one might well ask what the exception looks like.

¶34 Lessig then quickly goes on to support a technique called Platform for Privacy Preferences.[57] This system facilitates the collection of personal information from individuals visiting commercial websites by enabling a "negotiation" over privacy "preferences." (The P3P standard was developed by a group of private companies, known as the World Wide Web Consortium, that attempt to control many of the technical standards for the Internet.) Lessig notes that P3P is not without faults; he says that the larger point is to "imagine an architecture, tied to the market, that protects privacy rights . . . ."[58] To make P3P viable, Lessig says that it would be necessary to establish property rights in personal information. "P3P is the architecture to facilitate that negotiation; the law is the rule that says negotiation must occur."[59]

---

[54] In Reno v. Condon, 528 U.S. 141 (2000), the Court rejected a challenge to the Drivers Privacy Protection Act of 1994, reversed decisions of two federal appeals courts, and upheld Congress's authority to regulate the sale of drivers record information held by state agencies.

[55] LESSIG, *supra* note 1, at 160. The use of the phrase "data practice" as opposed to the conventional "data protection" in this sentence is telling. It is quite possible that Lessig could not rationally link "protection" and "choice" because the two concepts are so often in tension. Thus the substitution of a term that offers less assurance to consumers, a term that more accurately reflects the reliance on a choice-driven regime.

[56] *Id.* at 274 n.48.

[57] *Id.* at 160.

[58] *Id.*

[59] *Id.* Tim Berners-Lee, often credited with designing the key protocols for the World Wide Web, describes the P3P proposal in a recent book, but is also sympathetic to stronger privacy claims. TIM BERNERS-LEE, WEAVING THE WEB 147-48 (1999) ("I believe that when a site has no privacy policy there ought to be a legally enforced default privacy policy that is very protective of the individual.").

¶35 Lessig treats those who might be skeptical of the P3P/property regime dismissively, as extremists or leftists.[60] This is convenient shorthand that avoids the need to actually engage in a substantive discussion. But the more telling problem with the proposal is that Lessig does not attempt to place his solution in the context of any other regime for privacy protection. P3P simply exists as an opportunity to code a solution.

II. THE ROLE OF LAW AND FAIR INFORMATION PRACTICES

¶36 How is that Larry Lessig, who embraces the Brandeis dissent in *Olmstead*, agrees with the result in *Katz*, recognizes the value of anonymity, and is generally skeptical of free market solutions, ends his chapter on privacy supporting a market-based technique that is so very much at odds with a long history of privacy protection? The short answer is that he ignores most of the relevant history and does not consider how Fair Information Practices have, since the time of the *Katz* decision,

---

[60] *See* LESSIG *supra* note 1, at 161. ("Those who take this ideal of privacy to an extreme have a very different view about how the architecture should support it. The action group Privacy Now!, for example, threatens terrorist action to disable to the systems of data gathering and control. Marc Rotenberg of the Electronic Privacy Information Center (EPIC) argues strongly against any architecture that enables the trading or exchange of privacy rights. . . . They believe that none of theses rights ought to be sold, and that exchange of any of them should be criminalized.") (footnotes omitted).

At this point, let me note that I profoundly disagree with Lessig's characterization of my views on privacy; I wrote this article in part to set the record straight. In the excerpt above, Lessig cites to a speech I gave in Brussels at the 19th International Conference Privacy Data Protection Commissioners *available at* http://www.privacy.fgov.be/conference/pt1_3.html. Nowhere in the speech did I call for "criminalization" for privacy violations. Nor did I reject the idea that privacy rights should be sold. (It is obvious that entertainers, athletes and others make their livelihood from selling aspects of personality to others). I did, however, make a strong statement about the need to develop a common approach to privacy protection to solve the looming risk of disruption in transborder data flows. I closed the speech in Brussels as follows:

We must find a way forward. The Commission would have ample justification at this point if it decided to restrict certain data flows to the United States because of the absence of appropriate privacy safeguards. How can this point be disputed? Consumers in the United States know that we lack adequate privacy protection.

I think it is time to end what Colin Bennett has called "American Exceptionalism." There is little support in our public attitudes, law, or history for this stance. The United States should move quickly to establish a privacy agency, and then proceed to explore the application of the OECD Privacy Guidelines to the private sector. This useful framework provides a strong foundation for the development of technical means to protect privacy and the development of new privacy standards and legal safeguards. It is already found today in several U.S. privacy laws and in the practices of many U.S. companies.

I also propose today that the United States, Europe, and Asia join together to develop an international convention on privacy protection based on the OECD Guidelines. A simple framework of general goals combined with a consultative process that brings together a wide array of countries could help ensure that privacy standards are extended to all corners of the globe.

Only when we have established privacy standards and guidelines as strong as security standards and guidelines will users of advanced networked services have the trust and confidence to participate fully in the Information Society.

It is also my hope that in the process of working together toward a common goal that some of the current differences between the United States and Europe will diminish. There is too much at stake for consumers, and citizens, and users of the Internet to risk a clash of privacy rules.

We share a common interest in the protection of privacy. Let us go forward together and establish the policies that will launch the information economies of the next era while preserving the personal freedoms we cherish today.

I am pleased to note that over the last five years the United States and Europe have moved toward the approach that I and others urged back in the early 1990s. The Safe Harbor principles reflect the framework of the OECD Guidelines, many of the self-regulatory programs incorporate Fair Information Practices, and the U.S. has extended privacy rights increasingly to the private sector. Of course, there is a great deal more that needs to be done, including the establishment of a privacy agency in the United States.

But I cannot fathom to this day how Lessig could deal so dismissively and so snidely with such an extensive and central effort to develop privacy protections for the Internet.

enabled the translation of privacy norms into statutes, administrative practices, and ultimately technical standards of the type he terms "code." By ignoring this tradition and substituting in its place a cobbled-together marketing technique, he has done considerable damage to the privacy enterprise and his own call for the development of public code. Much of the problem is that Lessig, like many cyber pundits, imagines that the problem of protecting social values on the Internet of today ("cyberspace," if you must) is a completely new venture, without any historical or legal antecedents.[61] Fortunately the calls for a separate jurisprudence of cyberlaw and the autonomy of cyberspace from the real world are beginning to subside. But Lessig's final settling point in the chapter on privacy is particularly odd, given his frequent invitation in other parts of the book to public participation and government intervention in the evolving architecture of the communications infrastructure.

¶37 Lessig leaves the world of privacy law in 1967 with the *Katz* decision and returns roughly in the present day without any discussion of the intervening events.[62] This is unfortunate because if he traced the developments in statutory law he would have found considerable support for his larger argument on public code and avoided the rather odd conclusion to his chapter on privacy. *Katz*, for example, became the cornerstone for the federal wiretap statute adopted in 1968 that set out clear standards for the conduct of electronic surveillance by the government.[63] In effect, a decision of the Supreme Court that wire surveillance is limited by the Fourth Amendment was translated into code, of the legal type, that set out conditions under which such surveillance could take place. The federal wiretap statute requires law enforcement to follow an elaborate warrant procedure, far more detailed than is required to search for physical objects.[64] Limitations on the scope of wiretaps are established in statute (read: code), as are requirements to minimize the collection on communications that are not incriminating. [65]

¶38 This translation from a legal norm to a statutory framework is worth understanding in some detail because it is a recurring theme in the development of privacy law. Privacy law is not simply the result of courts extending privacy principles as Brandeis proposed in the *Olmstead* dissent, but also that of legislatures articulating statutory practices that are to be followed.[66] This is the democratic coding of privacy values.

---

[61] *See, e.g.*, David R. Johnson & David Post, *Law & Borders--The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); John Perry Barlow, *A Cyberspace Independence Declaration* (visited Dec. 19, 2000), *at* http://www.eff.org/pub/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration.

[62] *See* LESSIG, *supra* note 1, at 116-19.

[63] *See* Pub. L. No. 90-351, tit. 3, 82 Stat. 211 (codified as amended at 18 U.S.C.A. §§ 2510-2520 (West Supp. 2000)).

[64] *See* 18 U.S.C.A. § 2518 (2000).

[65] *See id.* § 2518(4).

[66] Legislatures have done this in response to judicial invitation; see, e.g., the New York Right of Privacy Act, L. 1903, ch. 132 (codified as amended at N.Y. Civ. Rts. §§ 50-51 (McKinney 1999)), which was enacted after New York's highest court held that there was no common law right of privacy but noted that the legislature could provide a remedy if it disagreed with the court's "hard rule." *See* Roberson v. Rochester Folding Box Co., 64 N.E. 442(N.Y. 1902); *see, e.g.* the Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C.A. § 2710 (West Supp. 1999)) (following disclosure of the video rental records of Supreme Court nominee Judge Robert Bork).

A. The Privacy Act and the Statutory Right of Privacy

¶39 The effort to extend privacy norms into code did not end with the federal wiretap statute. At about the same time that the Supreme Court was rendering decisions in *Berger v. New York*[67] and *Katz*, the United States Congress was holding hearings on the automation of personal information maintained by federal agencies.[68] A proposal in 1965 to create a centralized repository of records on U.S. citizens had sparked concerns about Big Brother.[69] The outcome of Congressional hearings, combined with the post-Watergate support for government reform, was the Privacy Act of 1974 ("Privacy Act").[70] The law set out a comprehensive regime limiting the collection, use and dissemination of personal information held by government agencies. The Privacy Act established penalties for improper disclosure and gave individuals the right to gain access to their personal information held by federal agencies.[71]

¶40 While Congressional findings are typically of minimal value, those contained in the Privacy Act were significant. Congress found that:

> (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies; (2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information; (3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems; (4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and (5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.[72]

¶41 The statement of findings contained in the Privacy Act provide the foundation for a sweeping policy goal—to regulate the use of information technology to protect the right of privacy. Congress followed the findings with a statement of purpose that establishes certain key aims:

> The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to— (1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies; (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent; (3) permit an individual to gain access to information pertaining to

---

[67] 388 U.S. 41 (1967).

[68] *See The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the House Comm. on Gov't Operations*, 89th Cong. (July 26, 27, and 28, 1966), *reprinted in* THE COMPUTER AND THE INVASION OF PRIVACY (1967). *See also* SMITH, *supra* note 49; WESTIN, *supra* note 25.

[69] *See* THE COMPUTER AND INVASION OF PRIVACY, *supra* note 68.

[70] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C.A. § 552a (West 1999)).

[71] *See id.*

[72] *Id.* at § 2(A).

> him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records; (4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information; (5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and (6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.[73]

¶42 It is not difficult to see in the introduction to the Privacy Act a set of instructions for the protection of privacy that would enable the development of future privacy code. The Privacy Act principles apply with equal force to different data, in different jurisdictions, and at different points in time. The concepts underlying the Privacy Act came to be known as Fair Information Practices, the principles that articulate the rights of data subjects and data collectors, in this instance U.S. citizens and the federal government.[74] More broadly, the Fair Information Practices set out an approach to the design of information systems that embeds certain normative political views. It is a very relevant example of the interplay between law and code and social organization, the focus of Lessig's book. Fair Information Practices also are technologically independent. There are no references in the Privacy Act to "PDP 11/70s," "VAX 350s" or "Winchester (3030)" disk drives. Fair Information Practices seek to ensure the fair collection and use of personal information, not the open-ended regulation of technology.

¶43 Notably, the concept of Fair Information Practices, like the development of a legal right of privacy, is very much an American creation. Those who have favored self-regulation and promoted market-based solutions to the privacy problem over the last few years have tried to ignore this history. But failure to reference this history leads to uninformed public policy decisions and legal analysis. Critics of privacy legislation or Fair Information Practices are of course welcome to find shortcomings in legal regimes or try to demonstrate the benefits of alternative approaches, but to ignore history, as industry lobbyists have done purposefully and I believe Lessig has done inadvertently, is to avoid engagement in a critical and necessary debate.

B. International Developments

¶44 Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection.[75] The most well known of these international guidelines are the Organization for Economic Co-operation and Development's Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD

---

[73] *Id.* at § 2(B).

[74] The concept of Fair Information Practices was first explicitly articulated in U.S. DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* XX-XXIII, at 50 (1973). The Advisory Committee's report provided the conceptual framework for the Privacy Act.

[75] *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 306 (1989).

Guidelines").[76] The OECD Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation: Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability.[77] The principles articulate in only a couple of pages a set of rules that have guided the development of national law and increasingly the design of information systems.

¶45 It is generally understood that the challenge of privacy protection in the information age is the application and enforcement of Fair Information Practices and the OECD Guidelines. While some recommendations for improvement have been made, the level of consensus, at least outside of the United States, about the viability of Fair Information Practices as a general solution to the problem of privacy protection is remarkable. As recently as 1998 the OECD reaffirmed support for the 1980 guidelines,[78] and countries that are adopting privacy legislation have generally done so in the tradition of Fair Information Practices.

¶46 While some commentators have made recommendations for updating or expanding the principles, there is general agreement that the concept of Fair Information Practices and the specific standards set out in the OECD Guidelines continue to provide a useful and effective framework for privacy protection in information systems.[79]

¶47 Commentators have also noted a remarkable convergence of privacy policies. Countries around the world, with very distinct cultural backgrounds and systems of governance, nonetheless have adopted roughly similar approaches to privacy protection.[80] Perhaps this is not so surprising. The original OECD Guidelines were drafted by representatives from North America, Europe, and Asia. The OECD Guidelines reflect a broad consensus about how to safeguard the control and use of personal information in a world where data can flow freely across national borders. Just as it does today on the Internet.

C. Looking Ahead

¶48 Viewed against this background, the problem of privacy protection in the United States in the early 1990s was fairly well understood. The coverage of U.S. law was uneven: Fair Information Practices were in force in some sectors and not others. There was inadequate enforcement and oversight. Technology continued to outpace the law. And the failure to adopt a comprehensive legal framework to safeguard privacy rights could jeopardize transborder data flows with Europe and

---

[76] PRIVACY LAW SOURCEBOOK, *supra* note 12, at 179-205, *available at* http://www.oecd.org/dsti/sti/it/secur/index.htm.

[77] *Id.* at 181-82.

[78] *See* Organization for Economic Development & Co-operation, *Ministerial Declaration on the Protection of Privacy on Global Networks* (October 1998), *reprinted in* PRIVACY LAW SOURCEBOOK, *supra* note 12, at 501-04, *available at* http://appli1.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)10-final.

[79] *See* Michael Kirby, *Privacy Protection--A New Beginning?*, *in* PRIVACY OF PERSONAL DATA, INFORMATION TECHNOLOGY & GLOBAL BUSINESS IN THE NEXT MILLENNIUM (1998). Paul Schwartz has provided a robust view of Fair Information Practices in his recent article that underscores the close ties between these principles of information processing and larger social goals of individual self-determination and democratic deliberation. *See* Paul M. Schwartz, *Privacy & Democracy in Cyberspace*, 52 VANDERBILT L. REV. 1609 (1999). Ronald Dworkin provided the useful observation about the relationship between "concepts" (broad, generally applicable principles) and "conceptions" (individual applications of those principles). *See* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY 134-36 (1977).

[80] *See* BENNETT, REGULATING PRIVACY, *supra* note 22, at 95-115; Bennett, *Convergence Revisited*, *supra* note 51, at 99-123.

other regions. These factors should all have played a significant role in coding a solution to the privacy problem. But in Lessig's analysis they did not.

¶49 As has already been noted above, one of Lessig's first missteps was his claim that the U.S. has not generally protected privacy by law.[81] It would be more accurate to say that in the absence of a general privacy law for the private sector, the U.S. has routinely protected privacy in law as new technologies have emerged. This raises the obvious question of why such laws have not yet been developed for the Internet. I am prepared to argue elsewhere that the explanation can be found in the rise of private power and the weakening of democratic institutions. There are associated problems of agency capture and the role of money in politics.[82] These are developments that should be genuine cause for concern particularly for Lessig because they suggest that as new issues arise for the Internet, public conceptions about code in the legal sense will be pushed aside by private conceptions of code in the architectural sense. But that is not my argument here. I am more concerned about the absence of the history of public code in Lessig's discussion of privacy.

¶50 Given the tradition of a legal right to privacy in the United States, the significance of Fair Information Practices in the structuring of privacy statutes, and the growth of privacy laws specifically to address monitoring by new technologies, it would seem that Lessig had at least some responsibility to address the question of whether privacy law would be up to the challenge of "cyberspace." Certainly his throwaway line that the U.S. has turned to law less often than the Europeans does not answer the question. Before addressing whether Lessig's proposal for a technique to negotiate privacy preferences does, it is worth filling in another part of the history—the development of technologies to protect privacy.

III. ARCHITECTURES OF PRIVACY

A. Anonymity, Digicash, and Virtual Credentials

¶51 In a 1992 article in *Scientific American*, David Chaum outlined a technique, based on encryption that would enable transactions that were "authenticated but not identifiable."[83] By this Chaum meant that it would be possible for an individual to transfer money (or credentials) over an electronic network and obtain a service without the service provider ever knowing the actual identity of the individual but with assurance that money would be received for the service or that the individual had the appropriate credentials to receive the service.

¶52 Chaum's technique, which is based on a particular cryptographic method called "blind signatures," is complex but real world examples suggest how this method may operate in practice.[84] In Washington, D.C. you may purchase a Metro card

---

[81] LESSIG, *supra* note 1, at 159.

[82] For illustrations of the agency capture problem in other contexts, see GRANT MCCONNELL, PRIVATE POWER & AMERICAN DEMOCRACY 230-38 (1966) (discussing the influence of the Farm Bureau on the Department of Agriculture and agricultural policy) and GABRIEL KOLKO, THE TRIUMPH OF CONSERVATISM: A REINTERPRETATION OF AMERICAN HISTORY 101-08 (1963) (discussing the meat packing industry's influence on the development of federal meat inspection laws). For a study regarding the influence of corporate campaign contributions on federal privacy law, see THE CENTER FOR PUBLIC INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY (1998), *at* http://www.publicintegrity.org/nothing_sacred.html.

[83] *See generally* Chaum, *supra* note 22.

[84] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 105-14 (1996) (describing how blind signatures could be used to ensure secure and anonymous electronic voting); PETER WAYNER, DIGITAL CASH: COMMERCE ON THE NET 159-67 (1996) (describing Chaum's DigiCash system).

with cash. The card contains a certain amount of value. Each time you ride on the Metro, the cost of the trip is deducted from the Metro card. When the value in the card is gone, you may choose to either add more value or simply discard the card.

¶53 What is remarkable about the Metro card, from a privacy viewpoint, is that the Washington Metropolitan Transit Authority has no interest in your actual identity. It simply needs to know that the card that you present to ride the Metro has a current value at least equal to the ride. Stored value or "debit cards" play a similar role in transactions for telephone services, photocopy services, even concession stands at the 1996 Olympics. They provide value to a service provider while maintaining the anonymity, that is to say the privacy, of the person who purchases the service.

¶54 Cards with credentials serve similar functions. A movie ticket presented to the ticket taker allows admission to the theatre regardless of one's identity. Even the problem of age verification has presumably been resolved at an earlier stage in the transaction when the moviegoer has provided credentials to establish, if necessary, an age sufficient to permit admission. And these credentials are of interest to the ticket seller only in that they provide a means of authenticating age. Actual identity continues to be irrelevant.

¶55 Chaum conceived that it would be possible to enable individuals to exercise control over the disclosure of personal information in a wide range of activities. This concept of providing only the elements of personal information necessary to enable transactions is very much in the spirit of privacy law. In effect, it attempts to embed the core principle of limiting the collection and use of personal information, and where possible, eliminating it altogether. Such credentialing schemes, as applied to the Internet, could permit age authentication where appropriate or admission to web sites not open to the general public while preserving the privacy of the individual.

¶56 Chaum's initial DigiCash scheme has not proved successful in the marketplace, though it is worth noting that it was better received in countries with well established privacy laws than those which lacked a comprehensive legal framework. But the DigiCash concept has inspired a number of other ventures, such as Zero-Knowledge's Freedom Network, that might genuinely be considered architectures of privacy.[85] Building on the techniques made possible by public key cryptography, these techniques enable not only the exchange of messages that cannot be intercepted but also the conduct of transactions that cannot be traced to a known individual. These designs transfer the physical experience of privacy and anonymity to the online environment.

¶57 These architectures of privacy, in preserving anonymity, also help protect important legal rights of citizens to express political views anonymously, to vote anonymously, and even to engage in political activities anonymously.[86] In some countries,[87] these techniques can also protect a legal interest in engaging in anonymous commerce.

---

[85] *See* Patrick Norton, *Freedom 1.1*, PC MAGAZINE, Dec. 23, 1999, *available at* http://www.zdnet.com/pcmag/stories/firstlooks/0,6763,2413285,00.html.

[86] *See* McIntyre v. Ohio Election Comm., 514 U.S. 334 (1995); Buckley v. American Constitutional Law Found., 525 U.S. 182 (1999); Michael Froomkin, *Anonymity and Its Enmities*, 1995 J. ONLINE L. art. 4 (1995), *at* http://www.wm.edu/law/publications/jol/froomkin.html.

[87] German Law for Information and Communication, art. 2 § 4, *reprinted in* PRIVACY LAW SOURCEBOOK, *supra* note 12, at 368-86.

¶58 Lessig addresses the possibility that public key encryption could enable the disclosure of aspects of identity without revealing actual identity in an earlier part of the book that considers architectures of control.[88] But the discussion is not carried forward into the chapter on privacy. Instead it is the springboard for a separate discussion about business on the Internet. Again, this is unfortunate, because the multiple credential model outlined by Lessig in chapter 4 would have provided a more robust conclusion to the chapter on privacy.[89] Such a conclusion might have argued that coding privacy in the world of the Internet would mean removing the barriers to adoption of these systems and encouraging the public to expect the availability of techniques that genuinely protect privacy.[90]

B. Canadian Standards Association

¶59 There are other efforts to translate the concept of Fair Information Practices into technical standards that could have informed Lessig's analysis of coding privacy. Perhaps the most noteworthy is the Canadian Standard Association's Model Code for the Protection of Personal Information ("CSA Model Code").[91] The CSA Model Code builds upon the OECD Guidelines and establishes standards that could be adopted by the private sector in the design and development of information systems. The ten principles in the CSA Model Code are Accountability, Identifying Purpose, Consent, Limiting Collection, Limiting Use, Disclosure and Retention, Accuracy, Safeguards, Openness, Individual Access, and Challenging Compliance. But whereas it was expected the OECD Guidelines would be translated into legal code, the CSA Model Code will be translated into architectural systems, i.e. information systems will be designed incorporating the element of the privacy code.

¶60 As applied to a business operating on the Internet it is not too difficult to imagine how such an enterprise might proceed. A company would display a statement that provides specific information about policies and practices relating to the management of personal information in order to comply with the Openness principle. The company could incorporate SSL in credit card processing to address the Safeguards principle. Information about individuals could be made available to them by means of the Internet to further the Individual Access principle. Data collection practices could be designed to comply with the goals of Limiting Collection and Limiting Use Disclosure and Retention. Where consent is required, it would be done so in accordance with the "knowledge and consent" standard set out in the CSA Model Code.

¶61 The Internet also enables a variety of techniques that could help code privacy techniques. Apart from anonymous payment systems, there are means to promote access to personal information. Banks, airlines, trading firms, and other online businesses are all providing to customers more information about their practices and activities. This is generally consistent with Fair Information Practices, but the companies could go further and allow customers to access their complete customer

---

[88] *See* LESSIG, *supra* note 1, at 30-42.

[89] *Id.*

[90] The choice formulation of privacy, the P3P standard, and other market-based approaches to privacy protection typically rely on the belief that there is little reason to expect privacy in the online world and that the privacy that can be obtained must therefore result from purchase, barter, or negotiation.

[91] *See* Canadian Standards Association, *Model Code for the Protection of Personal Information*, *reprinted in* PRIVACY LAW SOURCEBOOK, *supra* note 12, at 387-88. *See also* Media Awareness Network, *Your Guide to CSA's Model Code* (visited Dec. 19, 2000), *at* http://www.media-awareness.ca/eng/issues/priv/ involved/csa.htm.

profile, i.e., not simply the information that the customer provides to the company, but also the marketing information that the company uses to make decisions about customers. For individuals to make meaningful choices about the disclosure of personal information and their interaction with various firms access to their profile is particularly important.

C. Privacy Enhancing Technologies and Privacy Invasive Technologies

¶62 The search for an architecture of privacy has prompted a useful discussion of the various privacy techniques. One of the key questions of course is what constitutes an architecture of privacy. When the U.S. government first proposed the Clipper encryption scheme it said that it would protect privacy by enabling the government to apprehend criminals who break into computer systems and violate privacy interests. Even the recent computer security announcement from the White House, which called for expanded government monitoring of computer networks, echoed the theme that greater surveillance would promote greater privacy protection.[92]

¶63 It is necessary to develop analytic tools that make it possible to speak coherently about what constitutes an architecture of privacy. Herbert Burkert did this in part in an article entitled *Privacy Enhancing Technologies: Typology, Critique, Vision*.[93] Burkert provides a useful taxonomy of Privacy Enhancing Technologies (also known as Privacy Enhancing Techniques or "PETs") concepts and various strategies for implementation. Burkert notes that PETs are a "technological innovation that attempt to solve a set of socio-economic problems."[94]

¶64 The concept of PETs has resonated in the privacy world. Governments have undertaken studies to explore how Privacy Enhancing Techniques, oftentimes based on pseudonyms, could be implemented in the world of the Internet and e-commerce.[95] PETs typically seek to implement Fair Information Practices and where possible to minimize or eliminate the collection of personally identifiable information.

¶65 To understand the concept of PETs in more detail it is useful to have a contrasting notion. Elsewhere, I had proposed the term "privacy extracting techniques" as the appropriate counterpart to Privacy Enhancing Techniques, but here I will follow Roger Clarke's phrase "Privacy Intrusive Techniques" ("PITs"), which provides the useful pairing of PETs and PITs.

---

[92] WHITE HOUSE, *President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century*, Jan. 7, 2000 (press release), *at* http://www.ed.gov/PressReleases/01-2000/wh-0107.html (describing the National Plan for Information Systems Protection as "a government protections system . . . designed to protect privacy and enhance privacy").

[93] *See* AGRE & ROTENBERG, *supra* note 22, at 125-42.

[94] *Id.*

[95] *See* Marc Rotenberg, *Eurocrats Do Good Privacy*, WIRED, May 1996, *available at* http://www.wired.com/wired/archive/4.05/eurocrats.html.

	PETS	PITS
Central goal	"Control"	"Choice"
Policy implemented	Fair Information Practices	Notice and Choice
Data collection	Data minimization, finality	Data collection, multiple purposes
Key techniques	Anonymity	Persistent identifiers
Allocation of burden	Burden on data collector	Burden on data subjects
Examples	Debit cards, cash	

¶66 It is fairly obvious that techniques that covertly collect personally identifiable information might be considered intrusive.[96] Techniques that coerce the collection of personal information might also be considered intrusive. The interesting comparison arises from the voluntary disclosure of personal information. Here the distinctions between PETs and PITs are most apparent.

¶67 The key point in this example is that PETs will typically limit or eliminate the collection of personally identifiable information whereas PITs would facilitate it. Below I will discuss in some detail the privacy-negotiating scheme endorsed by Lessig as the solution to Internet privacy. It is worth noting here that P3P ("Platform for Privacy Preferences") would probably not be considered a Privacy Enhancing Technique. At best it is merely a Privacy Technique, neither Enhancing nor Intrusive, that enables some consideration of privacy terms in a market-based, microeconomic relationship.

D. Law Becomes Code Becomes Law

¶68 I have outlined above several of the various techniques to protect privacy that flow from Fair Information Practices, as well as a method to evaluate technology-based privacy solutions. It is possible to imagine that at a certain point these techniques could then be reincorporated into a legal regime. This is indeed what happened with the German multi-media law of 1997.[97] That statute, which covers a wide range of Internet topics from digital signatures to encryption and network security, sets out the protection of anonymity as a goal for businesses operating on the internet: "The provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed of these options."[98]

¶69 In this instance a legal code attempts to encourage the development of software code that implicates important privacy values. But unlike the Communications

---

[96] Marc Rotenberg, Presentation at the Standards Council of Canada International Meeting on Privacy and Data Protection (Sept. 16, 1999).

[97] PRIVACY LAW SOURCEBOOK, *supra* note 12, at 368-86.

[98] *Id.* at 371 (Art. 2, §4).

Assistance for Law Enforcement Act that was adopted by the U.S. Congress in 1994, the German Law for Information and Communication seeks to embed the value of data protection rather than data surveillance. The privacy provision in the German multi-media law is also interesting because it anticipates some of the emerging problems that are arising on the Internet. For example, the recent merger of Doubleclick and Abacus has raised the prospect of highly detailed profiles of individual consumers.[99] German multi-media law says simply that: "user profiles are permissible under the condition that pseudonyms are used. Profiles under pseudonyms shall not be combined with data relating to the bearer of the pseudonym."[100]

¶70 The German Internet law in effect controls the development of profiling techniques on the Internet. As a result, advertising firms, such as Doubleclick, operating in Europe are more careful about their data collection practices. The EU Data Directive should also regulate the effects of using cookies by commercial firms.[101]

¶71 Over the last three decades, there has been a useful interaction between the development of legal code and architectural code to protect personal privacy. There is general agreement about aims and now the rise of promising opportunities to embed Fair Information Practices and anonymity in the design of the Internet. Lessig ignores this history and chooses instead to back a market-based means to protect privacy going forward. It is time to look at the adequacy of this proposal.

E. Critique of P3P

¶72 Lessig concludes the chapter on privacy with a recommendation that the "Platform for Privacy Preferences" (P3P) is a possible way to code privacy.[102] He acknowledges that there may be problems with P3P but he does not actually spend more than a couple of pages pursuing the proposal. P3P remain nonetheless the recommended approach to code privacy. But why? Other than noting that P3P may enable a negotiation over privacy terms, why does Lessig believe this is a solution to privacy?

¶73 P3P was launched with much of the hype that accompanies most commercial services on the Internet. According to the early proponents,[103] "Products using P3P

---

[99] *See Internet Marketer DoubleClick in Hot Water; Watchdog Group is Preparing to File Complaint with FTC*, SAN FRANCISCO CHRONICLE, January 27, 2000, at B1; *Tracking Efforts to Halt, Firm Promises DoubleClick Will Await Guidelines on Web Privacy*, USA TODAY, Mar. 3, 2000, at 1B.

[100] PRIVACY LAW SOURCEBOOK, *supra* note 12, at 371 (Art. 4 §4).

[101] *See* Viktor Mayer-Schönberger, *The Internet and Privacy Legislation: Cookies for a Treat?*, W. VA. J. OF L. & TECH. (Mar. 17, 1997), *at* http://www.wvu.edu/~wvjolt/Arch/Mayer/Mayer.htm.

[102] LESSIG, *supra* note 1, at 160.

[103] Even the FTC fell for the ruse:

> In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.
>
> n. 44 Indeed, technological innovations soon may allow consumers and collectors of information to engage in "electronic negotiation" regarding the scope of information disclosure and use. Such "negotiation" would be based on electronic matching of pre-programmed consumer preferences with Web sites' information practices. The World Wide Web Consortium ("W3C") is currently in the final stages of developing its Platform for Privacy Preferences Project ("P3P"), which will allow implementation of such technology. Consumers may have access to P3P by early 1999. For general information on P3P, *see* the W3C's Web site (http://www.w3.org/P3P).

will allow users to be informed of site practices, to delegate decisions to their computer when possible, and allow users to tailor their relationship to specific sites. Users will see P3P in action both in the configuration of their client and during their Web browsing."[104] Some lobbyists went further and said that P3P would obviate the need for privacy legislation. Even former Vice President Al Gore was brought in by the proponents of self-regulation to offer a product endorsement, which was itself odd since the product didn't actually exist.[105]

¶74 The Federal Trade Commission endorsed the P3P standard.[106] Legislation was introduced to support P3P, another oddity since the standard was supposed to exist independent of legislation, and federal agencies were urged by industry lobbyists to embrace P3P as a method to provide privacy protection for federal web sites on the Internet.[107]

1. Pretty Poor Privacy

¶75 Today P3P shows few signs of life. As Professor Joel Reidenberg noted recently, "The World Wide Web Consortium 'W3C'), an influential standards setting body for the Internet, has led the development effort for P3P technology. Yet after three years, W3C has still not obtained sufficient industry agreement to conclude the development phase, let alone find companies willing to implement the technology. In addition, P3P faces a patent licensing problem that jeopardizes its ultimate adoption by industry."[108] At the end of 1999 there were only a few pilot projects involving P3P and the working group had announced a new last call working draft with the deadline of April 2000.[109]

---

n. 45 A system requiring consumers to specify privacy preferences before visiting any Web sites can be built into Internet browsers. *See supra* note 44 (discussing technological developments). The absence of default rules, and the concomitant requirement that consumers decide how they want their personal information used, help ensure that consumers in fact exercise choice.

Federal Trade Commission, Privacy Online: A Report to Congress at (III)(a)(2) (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23.htm.

[104] World Wide Web Consortium, *W3C Publishes First Public Working Draft of P3P 1.0* (May 19, 1998), http://www.w3.org/Press/1998/P3P.html.

[105] "I welcome this important new tool for privacy protection. It will empower individuals to maintain control over their personal information while using the World Wide Web." This statement and a whole range of testimonials for the non-existent product may be found at World Wide Web Consortium, *W3C Publishes First Public Working Draft of P3P 1.0 Testimonials* (May 19, 1998), http://www.w3.org/Press /1998/P3P-test.html. Significantly, there were no consumer or public interest organizations that supported the proposal.

[106] "A second task force will address how incentives can be created to encourage the development of privacy-enhancing technologies, such as the World Wide Web Consortium's Platform for Privacy Preferences (P3P)." *Hearing before the Subcomm. on Telecomm, Trade, and Consumer Protection of the Comm. on Commerce United States House of Representatives*, 106th Cong. (1999) (statement of Robert Pitfosky, Chairman of Federal Trade Commission), *available at* http://www.ftc.gov/os/1999/9907/pt071399.htm.

[107] At a Congressional hearing, I pointed out the absurdity of a citizen negotiating with a federal agency over privacy preferences. Could the agency really adopt privacy rules that fell below the legal requirements of the Privacy Act? Could a citizen really be denied access to a federal web site because of a privacy preference? What are the "market options" to the IRS? *Electronic Communication Privacy Policy Disclosure: Hearings Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. 78 (1999) (statement of Marc Rotenberg), *available at* http://commdocs.house.gov/committees/judiciary/hju62502.000/ hju62502_0f.htm ("The government is subject to the Privacy Act. It is a law that establishes basic privacy rights for all citizens. It is not something that you express a preference about.")

[108] Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 779 (1999).

[109] *See* Lorrie F. Cranor, *Agents of Choice: Tools That Facilitate Notice and Choice about Web Site Data Practices* (visited Dec. 20, 2000), *at* http://www.research.att.com/~lorrie/pubs/hk.pdf.

¶76 The problems with P3P have now been widely reported.[110] Technical experts have noted that the protocols are complex, difficult to implement, and unlikely to enable consumer to protect privacy. Privacy experts have emphasized that the standard is intended to enable collection of personal information rather than the protection of personal information. Industry analysts have also found shortcomings in the P3P proposal.[111]

¶77 Jason Catlett, the CEO of Junkbusters and a computer scientist, offered perhaps the most articulate critique of P3P.[112] In a letter to the P3P developers he wrote that the standard would favor a "technologically advanced minority," that without basis it presumes an "extremely diverse range of privacy preferences, and that access related to knowledge of a policy and not transparency of data practices." He concludes:

> As a product to protect the privacy of the average American shopper, P3P is doomed to fail, because such an outcome is not in the commercial interests of the organizations who decide whether and how it will be deployed. P3P has become a mirage in the desert of Internet privacy.[113]

¶78 A different type of analysis of P3P was put forward by the privacy working group of the European Commission, established by the EU Data Directive.[114] The Article 29 Working Group had the special obligation to assess the impact of the P3P proposal on the legal rights currently in force under the EU Directive, in other words, they compared the code with the Code. The European expert group observed simply that "[a] technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals." The expert group also said, "There is a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the on-line negotiation. In fact those businesses, organizations and individuals established within the EU and providing services over the Internet will in any case be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process."

¶79 The EU critique of P3P is particularly significant in the context of Lessig's larger call for a public role in the design of code. Here is the public institution with

---

[110] *See* Karen Coyle, *Some Frequently Asked Questions About Data Privacy and P3P* (Nov. 21, 1999), http://www.cpsr.org/program/privacy/p3p-faq.html.

[111] *See* Kenneth Lee & Gabriel Speyer, *White Paper: Platform for Privacy Preferences Project (P3P) & Citibank* (Oct. 22, 1998), http://www13.w3.org/P3P/Lee_Speyer.html. ("1.From a consumer standpoint using P3P may be quite confusing, as the user may feel inundated with 'legalese' and too many choices.2.Implementing P3P might limit the amount of marketing information, commerce and cross-selling a company can conduct online. 3.P3P is just one component of what should be a full framework for online privacy. For P3P to be widely deployed and properly used, other (perhaps costly) measures must be bundled with P3P implementation to reconcile consumers' and companies' preferences. Such measures would include: self-auditing, a process of recourse for users, education/enforcement and authentication.")

[112] Jason Catlett, *Open Letter 9/13 to P3P Developers* (Sept. 13, 1999), http://www.junkbusters.com/standards.html.

[113] *Id.*

[114] European Commission, Directorate General XV, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)* (June 16, 1998), *available at* http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/ wp11en.htm.

the expertise in the relevant social value reviewing a proposal for code that will regulate the transfer of personal information in cyberspace. The conclusion? The code is flawed. It fails to provide protection comparable to that which is provided in law. It shifts privacy burdens in a manner disadvantageous for citizens. It is potentially misleading to users and it could provide a way for institutions to get out from under their obligations to comply with legal code.

¶80 This is the critical test for whether Lessig's theory that code can reflect political norms will succeed. But the result is not what Lessig would predict. Either he has to accept the conclusion of the EU expert group and revise his assessment of P3P or he has to reconsider his broader call for public engagement in the structuring of the code that regulates cyberspace. Of course, he may also choose to reject the EU assessment and maintain his attachment to P3P as well as support in theory for public review of code, but this position at the very least requires a reasoned answer. He cannot ask the rest of the world to accept the public regulation of code and then run in the opposite direction when the public regulates his code.

¶81 If Lessig is not persuaded by the history of privacy law or the specific assessment of privacy experts who reviewed the P3P proposal, he might consider also the survey conducted by several of the designers of the P3P protocol. *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* explored a number of privacy issues, including whether Internet users favored "automatic data transfer techniques." Such techniques could include an auto-fill feature "that users could click on their browsers to have information they had already provided to another Web site automatically filled in to the appropriate fields in a Web form." According to the survey about 61% of respondents use such a browser feature, though the number drops to 51% if no human intervention is required before the transfer takes place.[115]

¶82 The most interesting results can be found when the researchers asked respondents about a P3P-like feature that would allow the automatic transfer of personal information to sites with acceptable privacy policies. According to the survey, "there was little interest in two features that would automatically send information to Web sites without any user intervention: a feature that notified the user that it had sent the information was of interest to 14% of respondents, and a feature that provided no indication that it had transferred data was of interest to only 6%."[116]

¶83 As the researchers who conducted the survey noted:

> Our respondents provided strong comments about automatic data transfer. A large number of respondents made comments about wanting to remain in control over [sic] their information and stating that they had no desire for automatic data transfer. Some respondents were concerned with the perils of automatic data transfer in general. For example, one respondent noted that 'I want to be in charge of all information sent to other companies. Just because they are similar, doesn't mean I [want] my information shared with them.' Another noted the need for updating personal information: 'To be able to update or correct the previous info is a good thing.' However, most comments revolved around the respondents' desire to maintain control of the process. For example: 'Auto[matic] features save time. . . . However, I do like to know when information

---

[115] Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* (Apr. 14, 1999), *at* http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm.

[116] *Id.*

> about me is being transmitted,' 'I want to be in control of what is done. This way I know what was done,' and 'I don't want anything sent automatically. I want to check out everything I am applying for.'[117]

A recent survey by Business Week suggested even higher levels of public opposition to the type of profiling that might be enabled by P3P.[118]

¶84 Perhaps the most significant criticism of the regime is the extent to which it codes the preferences of the P3P designer as opposed to say the general public. Who decides, for example, what basic elements should be made available to others? And why should techniques that ultimately shift burdens to the consumer be adopted? Do consumers really want to negotiate over privacy preferences? Wouldn't consumers prefer to disclose the minimal amount of personal information necessary to a transaction as Fair Information Practices generally?

¶85 It is possible to answer these questions with a general defense that P3P is "a work in progress," and that some of these problems may be resolved over time, though there is in fact little indication that such a process is progressing. But the larger question for Lessig is why should individuals settle for a cyberspace architecture that leaves them isolated in the marketplace to negotiate over privacy protection when there is a rich tradition of Fair Information Practices and an emerging architecture of privacy that seems far more likely to safeguard privacy interests.

¶86 Imagine, for example, a P3P-enabled world after an AOL Time-Warner merger where the merged entity chooses to adopt P3P standards that are generally not privacy respectful. One could easily imagine for example the rise of a company-wide policy that individuals reveal their actual identity and some additional information before they move beyond the home page of a particular web site. The P3P-empowered web users could if they wish simply refuse to visit of the AOL Time-Warner web sites. And if enough other prospective AOL Time-Warner customers acted in similar fashion, presumably AOL Time-Warner would change its policy. Or it might not.

¶87 This result, which probably would not disturb libertarians and those who are generally optimistic about the market's ability to respond to consumer wishes, should disturb Lessig. If his book is intended to build support for the view that cyberspace can be subject to political institutions, then a conclusion that ignores a rich and largely successful tradition of government regulation and chooses instead a socially-isolating marketing scheme designed to facilitate the collection of personal data is deeply flawed. The EU privacy group identified this problem at the outset in its review of P3P. It noted that "Surprisingly, given the intention that P3P be applicable worldwide, the vocabulary has not been developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalize lower common standards."[119]

¶88 How would the P3P approach work as applied to other social issues? Should consumers negotiate over the level of consumer protection, and what will become of these profiles that contain such detailed articulations of an individuals likes and dislikes?

---

[117] *Id.*

[118] *Privacy on the Net: A Growing Threat*, BUS. WK., Mar. 20, 2000, at 96, *available at* http://www.businessweek.com/2000/00_12/b3673010.htm.

[119] *See* European Commission, *supra* note 114.

¶89 Still, the argument over P3P is not simply a debate over the pros and cons of a particular approach to the privacy problem. It is rather a battle over public code versus private code, an argument about whether the designers of the communications infrastructure should be accountable to the views of lawyers, policymakers and especially citizens, or whether they should be free to pursue whatever architecture provides private advantage. P3P is a form of private code, much like the Windows operating system, that reflect a particular institution's views of how choices and behavior should be constrained in cyberspace. It elevates notice and choice as a preferred method for privacy protection and downplays the role and history of Fair Information Practices. It maps nicely to the anti-regulatory views espoused by industry but not at all to the well-established tradition of privacy protection in law. P3P is in the end an invitation to reject privacy as a political value that can be protected in law and to ask individuals to now bargain with those in possession of their secrets over how much privacy they can afford.

2. P3P as Political Response to Privacy Laws, Privacy Institutions

¶90 P3P arose at a particular point in time. There was growing support in the United States for comprehensive privacy legislation and the U.S. trading partners favored this outcome as well. But business was reluctant to support this approach and did not want its new practices, its code, to be subject to public regulation. And so an extended architecture of notice and choice was put forward as a privacy solution.[120] This was, at the end of the day, little more than the old "opt-out" box offered by the Direct Marketing Association whenever the DMA was pressed to provide a privacy solution. All of the problems of compliance, burden, enforcement, and effectiveness that were known about the DMA's opt-out program were present in the design of P3P.[121] P3P even added a layer of complexity that was sure to defeat whatever interest might remain to pursue privacy "choices." But there was little interest in addressing these concerns because there was little interest in developing a robust regime to protect privacy.

¶91 Lessig is caught in a bind. Having railed against the libertarian excesses in the world of cyber policy, when confronted with one of the most pressing social issues, he makes a beeline for the free market solution and tosses aside his own calls for the development of code that reflects public values and public interests. Even Lessig's call for a property-based notion of privacy in the context of his other arguments in favor of government regulation seems odd and out of place. Lessig expresses a preference for property regimes over privacy legislation, what he calls liability regimes.[122] The preference for a property regime over a liability regime is that it allows individuals to exercise choice, to negotiate, and to obtain value.[123]

---

[120] It is hardly coincidental that industry latched onto the Platform for Internet Content Selection (PICS), another technical standard put forward by the W3C that would reduce the likelihood of government regulation of Internet business. Interestingly, Lessig was one of the sharpest critics of PICS, arguing that "PICS is the devil," in Lawrence Lessig, *Tyranny in the Infrastructure: The CDA Was Bad—But PICS May Be Worse*, WIRED, July 1997, at 96. I suggest that the reason Lessig was so critical of a technical standard that "coded" speech interests, but far less critical of a technical standard that coded privacy interests, is simply that Lessig is far more familiar with the values underlying First Amendment interests than those underlying privacy interests.

[121] *See generally* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996) (discussing the failure of the DMA members to comply with the DMA's own privacy policy); Electronic Privacy Information Center, *Surfer Beware II: Notice Is Not Enough* (June 1998), http://www2.epic.org/reports/surfer-beware2.html (discussing the failure of the new DMA members to comply with the new DMA privacy policy).

[122] LESSIG, *supra* note 1, at 160-61.

[123] *Id.*

¶92 This analysis presupposes that individuals have a general interest in alienating the value of private information in the marketplace. Admittedly this is a popular argument in some corners, but where is the proof? Whereas Lessig analogizes the exercise of property rights in personal information to the sale of a used car, a common commercial transaction, the better analogy may be to vacation photographs or a high school diploma. Both the photographs and the diploma are items personal to the individual. A property regime allows the individual to exercise control over these items, to exclude others from use, but it is hardly intended to facilitate sale. It could well be argued that those items that are most personal to us are those where the disparity between what a willing buyer and a willing seller will pay is the largest. Do we really want to create markets in these circumstances so that individuals are encouraged to disclose—to alienate in the market—their HIV status, their email correspondence with colleagues, or their love letters from high school? Certainly it is a property-based regime that allows an individual to exercise control over these items and incidents of private life, but this is not a regime that, generally understood, encourages one to sell these things to others.

¶93 Brandeis and Warren understood the problem with market-based approaches to privacy when they wrote the article on the right to privacy more than a century ago.[124] They purposefully distinguished a privacy right from an intellectual property claim, noting that copyright typically protects an interest once publication occurs, privacy protects a right to simply not publish.[125] They further noted that copyright preserves values that are based on marketplace determinations, whereas privacy protects values that are unique to each individual.[126] Lessig's market-based model, which seeks to facilitate the transfer of control over privacy interests, is clearly at odds with this tradition. His skepticism elsewhere about the copyright regime[127] almost begs the question of why he saddles the privacy world with an approach he is uneasy about in the world of intellectual property.

¶94 A regulatory regime brings other benefits. In the privacy field, it will likely mean a government office with the expertise and authority to advocate on privacy

---

[124] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[125] *Id.* See MILLER, *supra* note 25, at 213-14 for further commentary on this point. Miller notes that Warren and Brandeis rejected the property theory and then comments, "The property rationale is inappropriate for other reasons. In contexts such as the sale of information by credit bureaus or mailing-list organizations, it is not the subject of the data but a third party who created the commercially valuable record." Miller further observes that, "Reliance on the recognition of a property right also would have the undesirable effect of placing responsibility on each individual to protect his own interests, rather than imposing clear duties of care or restrictions on those organizations that want the data, and usually have the leverage to extract them from the people. Credit bureaus, for example, probably would be no less successful in convincing data subjects to give up their 'property rights' by holding out the carrot of access to the credit economy than they presently are obtaining 'voluntary 'consents to credit investigations. The unequal bargaining position of an individual dealing with a government agency or an employer would lead to a similar result." Professor Miller concludes, presciently, "These considerations indicate that recognition of property rights in personal information is much too artificial a method of regulating important phases of a technology that still is in its infancy." *Id.*

[126] The opinion of the Minnesota Supreme Court in the recent case of Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998) provides an excellent illustration of these points. In *Lake* a young woman and her friend brought several rolls of film from a vacation to a Wal-Mart to be developed. On one of the rolls of film was a picture, taken by the sister of Lake's friend, of Lake and the friend naked in a shower. When Lake received the developed photographs along with the negatives, an enclosed written notice stated that one or more of the photographs had not been printed because of their "nature." But Lake subsequently learned a Wal-Mart employee had printed the negative and that the picture of her naked in the shower was circulating in the community. Lake brought a claim against Wal-Mart under common law tort theory and the Minnesota Supreme Court was asked to determine whether the state would recognize the privacy claim. The court concluded, "One's naked body is a very private part of one's person and generally known to others only by choice. This is a type of privacy interest worthy of protection. Therefore, without consideration of the merits of Lake and Weber's claims, we recognize the torts of intrusion upon seclusion, appropriation, and publication of private facts." *Lake*, 582 N.W.2d at 235.

[127] *See* LESSIG, *supra* note 1, at 122-41.

matters.[128] When, for example, a proposal is put forward by law enforcement to develop techniques for wiretapping, governments with privacy agencies, that is to say governments that have a regulatory structure to protect privacy which includes a privacy agency, will have also to contend with the competing claims of citizens' privacy interests.[129] Indeed, this has happened repeatedly in the last few years as countries with privacy regulations and privacy offices have rebuffed calls for expanded police surveillance while those that lack such agencies have remained in control of law enforcement agencies.

¶95 Privacy agencies also provide an effective resource for consumers with privacy concerns and are often times able to respond to privacy complaints without extensive and costly litigation.[130] Such agencies also provide a source of expertise and advice for emerging privacy issues. This has been the experience not only of privacy agencies in Europe but also of those in Canada.[131]

¶96 A property-based regime of the type Lessig describes lacks any commitment to an institutional structure (or more broadly democratic institutions) that could be established to protect an underlying public interest. Privacy interests that cannot be expressed in the marketplace through the exercise of P3P preferences simply do not exist. Again interests of common concern are pushed aside in the name of promoting market-based negotiation. Such an approach implicates not only public values but also public debate and public institutions.

¶97 A regulatory regime also allows the design of an architecture that reflects public values as opposed to simply private market power. Consider, once again, the resolution of the Caller ID debate. What would the result have been in the absence of a regulatory framework? The telephone companies would simply have announced that the new network architecture enables the disclosure of calling numbers to call recipients and the blocking of such numbers by call recipients. The telephone company would have offered services that allowed customers, for a price, to obtain the number of the calling party or, for a price, to withhold disclosure of one's number when calling another person. If ideal market conditions prevailed, it is even conceivable that the telephone company could price such services on a call by call basis. The telephone company would, under this scenario, become a very rich auctioneer, while telephone customers collectively would see the control of disclosure over personal information significantly diminished.

¶98 Now consider again the communications model that results from the AOL Time-Warner merger. Even if this is not in fact a monopoly, there will certainly be monopoly like practices. Indeed mergers in the hi-tech communications field are

---

[128] Privacy commissioners have also sponsored an annual conference to promote research and understanding of emerging privacy issues. The 21st annual meeting of the International Privacy Protection and Data Protection Commissioners was held in September 1999 in Hong Kong SAR. The conference web site provides an extensive resource on privacy issues. *See 21st International Conference on Privacy and Personal Data Protection* (visited April 2, 2000), http://www.pco.org.hk/conproceed.html. The United States sponsors no similar event. Even where the Federal Trade Commission has sponsored workshops on privacy topics, the events have typically been open-ended fact-finding exercises, dominated by industry lobbyists, with little interest in privacy research or scholarship.

[129] Privacy officials from Europe and Canada played a significant role in the decision of the Organization for Economic Cooperation and Development to reject the U.S.-backed key escrow regime. The privacy commissioner in Italy has recently undertaken an inquiry into illegal wiretapping.

[130] *See* David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective?*, *in* AGRE & ROTENBERG, *supra* note 22, *available at* http://www.oipcbc.org/publications/presentations/surveil.html.

[131] A good summary of the activities in Europe may be found in the *Second Annual Report of the Article 29 Working Group*, *in* PRIVACY LAW SOURCEBOOK *supra* note 12, at 466-500. Annual reports are also published by privacy agencies around the world including those in the European Union as well as Canada, New Zealand, Australia, Hungary, Hong Kong, and elsewhere. No similar report is published in the United States because there is no agency tasked with the protection of privacy.

predicated on the various barriers that discourage customers from moving between various providers. Would a property-based regime of the type that Lessig proposes or a regulatory regime of the type that limited the telephone company's ability to extract personal information from its customers do a better job in protecting privacy? I leave it to the reader to make this judgment.

¶99 Why does Lessig settle for P3P? It is possible he genuinely believes it will work.[132] It may also be, consistent with the somewhat pessimistic conclusion of the book, that he simply assumes that government will not succeed in its efforts to regulate the Internet to protect privacy. But if that is indeed his view, then his own call for action takes on a Sisyphean dimension. Sure, you can roll the rock, but don't expect much to happen.

¶100 I suspect that Lessig is somewhat more circumspect of his support for P3P today than he was when he wrote *Code*. But I am troubled that the author of *Code and Other Laws of Cyberspace* who invites us to reconsider the relationship is able to so easily substitute a relatively thin idea without any consideration of a robust pre-existing regime.

IV. ECONOMIC ANALYSES

¶101 Since the operation of P3P relies on certain assumptions about the ability of consumers to exercise choice and the nature of markets, it is worth looking closely at some of the comments that Lessig makes about market forces in his discussion of privacy. I am troubled, for example, by Lessig's assertions that the disclosure of individual privacy preferences makes "the market work more smoothly"[133] and that price discrimination is "overall a benefit." While an argument can surely be made that the widespread availability of price and quality information about competing products is a benefit to consumers, it is less clear that information about a consumer's own interests produces similar benefits.

¶102 There is the obvious consideration that marketing does not simply react to demand but is intended also to stimulate demand. It is unlikely that a consumer will at any point in time have a pre-determined disposition to purchase a particular product. Marketers are fond of saying that the benefits of profile-based marketing are that you will learn only about products that are of interest to you, but of course marketers are not simply offering you the same products that you currently possess. They are taking your past purchases and profile information and extrapolating to create a model of new products that you may be persuaded to buy. Moreover, marketers may draw on personal facts to reach these decisions that consumers might well find offensive or intrusive if they were aware of the operation of the marketing industry. Do you really want to purchase a book from an online merchant that, unbeknownst to you, knows not only the books that you have purchased from that company but the web sites you visit, the type of home you own, and the ages and names of your children?

¶103 Lessig is no doubt aware of these criticisms, but he treats them somewhat dismissively. An approach that incorporated Fair Information Practices would quickly show that one solution to the problem of this form of profiling is the

---

[132] "A world without P3P is a world with less control over privacy; a world with P3P is a world with more control over privacy." Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 762 (1999).

[133] "[P]roducts are matched to people, and interests to people, in a way that is better targeted and less intrusive than what we have today." LESSIG, *supra* note 1, at 153. *See also id.* at 155.

requirement that companies make available to the individual all information about the individual that is in the possession of the company.

A. Privacy and Price Discrimination

¶104 But the more interesting economic problem in this discussion is Lessig's implicit endorsement of price discrimination. While he ascribes the view to economists generally and notes a competing interest in equality, he seems unwilling to explore what the implications of price discrimination in Internet commerce may be. This is a topic worth examining since the privacy model proposed by Lessig lead to extensive price discrimination.

¶105 By price discrimination, I mean the sale of differing units of a good or service at price differentials not directly corresponding to differences in supply costs.[134] Price discrimination occurs when firms offer discounts to senior citizens and students. It occurs also when an electric utility company charges less for additional units of power consumption. Price discrimination also occurs when a seller alters a price to obtain the maximum amount that the consumer is willing to pay.

¶106 Companies that have access to a personal information about prospective customers can price discriminate more effectively. If for example, the *New York Times* sells its daily newspaper for $1 but knows that there are some people who are willing to pay 75 cents for the paper and it can produce additional papers for less than 75 cents, it might choose to sell papers to that market segment for only 75 cents. Conversely, it might also choose to sell papers to those who are prepared to pay $1.25 for $1.25. In theory the supplier could take advantage of the reservation price of each potential customer to produce exactly the amount of papers at exactly the price willing consumers are prepared to pay. Economists would describe this production model as "efficient," and the benefit to some consumer can be shown by the availability of some papers at 75 cents that would not otherwise be available if the *New York Times* could not price discriminate.

¶107 But the conditions that allow price discrimination are not without problems. In the first instance, price discrimination involves a net transfer of rents from consumers to suppliers. This is an equity effect that essentially leaves consumers as a whole less well off.

¶108 There are also market effects. For price discrimination to occur, three conditions must exist. First, the sellers have some monopoly power. Second, the seller must be able to effectively segregate customers into categories with differing price elasticities. Third, it must be able to control arbitrage, that is to say, the resale by low-price customers of the product to high-price customers. Price discrimination is typically easier to achieve in markets for personal services, such as medical care or legal services, than it is for consumer goods.

¶109 Competitive firms may price discriminate to attract new customers; monopolistic firms may price discriminate to defeat competitors or to extract rents from consumers, effectively depriving customers of some of the value that would be available in a competitive market. And where this monopoly power exists, prices to consumers may also rise above what they would be in competitive markets.

¶110 Price discrimination is only really possible when there is market power, so it happens in precisely those cases where assumptions of perfect competition are

---

[134] FREDERIC M. SCHERER, INDUSTRIAL MARKET STRUCTURE AND ECONOMIC PERFORMANCE 315 (3d ed. 1990).

violated. When you combine market power, consumer profiling and price discrimination, consumers may be less well off. In bargaining, no one wants to give up their "reservation" price to the other side. With profiling, the consumers give up the privacy of their reservation price, but the seller doesn't. So it changes the power in the bargaining, against consumers. This is an example of information asymmetries that are likely to arise more frequently as consumer profiles are more widely disclosed to sellers.

¶111 Privacy rules that allow individuals to withhold disclosure of actual identity leave consumers in a more effective bargaining position. Consumers always have the ability to disclose actual identity and to take advantage of whatever special price a supplier may offer, but they retain the ability to forego that opportunity if there are others interests to consider. Thus regimes that enable price discrimination by making available personal information of prospective customers to suppliers are likely to support monopoly behavior and to leave consumers, taken as whole, less well off then they might otherwise be. The allocation of goods might still be considered "efficient," but the distributional effects as well as the market effects would be a basis for concern.[135]

¶112 The problem of price discrimination is interesting in another respect. Under the P3P regime, consumers are effectively required to reveal their privacy "reservation price" as a condition of transacting with a particular web site. Thus consumers transfer whatever value maybe assigned to their privacy preferences to the web site, when under a Fair Information Practices regime, a consumer could interact with the site without revealing a privacy profile. In effect the web site learns more about the consumer than is necessary to enable the transaction and the associated problems of market power and distributional transfer described above are replayed over the value of the privacy profile.

¶113 The Fair Information Practices approach, supported by the architectures of privacy described above, is built on the premise that individuals need only disclose the elements of identity that are necessary to enable the transition, and a preference is established at the outset for transactions that do not disclose actual identity. The Fair Information Practices regime would add the additional consideration that certain types of inquiry, such as race in a housing loan, should simply not be disclosed even if a consumer is willing to do so.

B. Efficiency of Privacy Rules

¶114 In addition the discussion of price discrimination, there are other interesting economic questions concerning privacy protection. More than twenty years ago Richard Posner argued that in the privacy rules for mailing lists, an opt-out regime was more efficient than an opt-in regime because of the transaction costs associated with obtaining consent.[136] Posner's description make certain assumptions about the costs associated with opt-in in the physical world. But these costs may go to zero in the online world, and if that is the case then the economic argument against opt-in should be revisited. At least there is a claim to be made that it is economically

---

[135] In some cases, evidence of price discrimination can be the basis for anti-trust action.

[136] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 398-99 (1978).

efficient, as economists use the term, to allocate a property interest in personal information to the consumer.[137]

¶115 I do not intend in this section to offer a definitive assessment of whether price discrimination of the type enabled by the collection of information of prospective customers necessarily produces a bad result on economic grounds nor do I have a full answer for Richard Posner about the application of the Coase Theorem in the age of the Internet. I simply wish to point out that these topics deserve far more attention than it received in *Code.*

V. CONCLUSION

¶116 There is much to be said for an inquiry that asks us to consider how the Internet is to be regulated. The United States, in particular, has struggled with this question, arguing on the one hand for "self-regulation" and at the same time adopting more legislation for the Internet than any other government in the world.[138] In the privacy field in particular there is a great need to understand the interaction between law, the design of information systems, and the political right of privacy, which however difficult to describe still remains one of the central concerns of citizens in the information society.

¶117 The United States provides a rich history for this examination. From the articulation of a legal theory for a right of privacy in the nineteenth century through the adoption of comprehensive privacy legislation in 1974 and the privacy laws of the 1980s that targeted new technologies, there has been an ongoing effort to bring technological design within the control of the public and to safeguard the right of privacy. But something happened in the 1990s that set the United States on a strange course. At roughly the same point in time that Europe and other governments were developing new legal regimes to protect privacy, the United States was pursuing legal and technical measures to enable surveillance.[139] While Europe faced the challenge of ensuring compliance by all the member states with the requirements of the Data Directive, the U.S. took on the challenge of trying to enforce compliance with the FBI's technical scheme to enable wire surveillance. And when consumers called for privacy safeguards to address the growing problems with the Internet, the United States government turned to the private sector for self-regulatory measures that offered little in the way of actual privacy protection.

¶118 Today industry groups continue to press on with self-regulation, P3P, and other market-based approaches to the privacy issue that shift burdens back to consumers and reject the use of public institutions to resolve problems of common concern. Meanwhile, consumer organizations call on their governments to establish

---

[137] Many business-funded thinktanks are fond of making arguments against opt-in regimes. But these arguments rarely turn on a rigorous economic discussion of efficiency; invariably they are generalized appeals to protecting business freedom and the presumed desire of consumers to receive junkmail.

[138] *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998); No Electronic Theft Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997); Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986); Communications Decency Act, Pub. L. No. 104-104, 110 Stat. 56 (1996); Children's Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998); Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998); Export Administration Act, Pub. L. No. 96-72, 93 Stat. 503 (1979) (*amended by* Pub. L. No. 99-64, 99 Stat. 120 (1985)) (export rules for encryption).

[139] *See* ELECTRONIC PRIVACY INFORMATION CENTER & PRIVACY INTERNATIONAL, PRIVACY & HUMAN RIGHTS 1999: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (1999).

safeguards in law for the emerging digital economy and to extend the approaches that have been established in the past to the technologies of the future.[140]

¶119 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. This problem—a problem that concerns the functioning of democratic institutions—is a far more serious threat to Lessig's ideal about public control of cyberspace than the rhetoric of libertarians. But it will take determination to ask hard questions about the operation of our political system, a rediscovery of America's own privacy tradition, and a willingness to move beyond the technological fetishism that has seduced even some the nation's most brilliant legal scholars before it will be possible to begin a genuine debate about the future of privacy protection in America. Lessig has not helped this enterprise and may have caused it some harm.

¶120 With the publication of *Code*, Larry Lessig invites readers to begin a long overdue discussion—at least in the United States—about the regulation of cyberspace.[141] He implores us to "choose what kind of cyberspace we want and what freedoms we will guarantee." And he reminds us that on the Internet "code is the most significant form of law" and it is up to "citizens to decide what values that code embodies."[142] But when confronted with a pressing social concern he turns from the values that citizens have traditionally sought to protect in code and asks us instead to surrender our political rights to market forces. Our ability to act collectively, that is to say to act as citizens, is suddenly no longer important. We are on our own, isolated in a marketplace where the rules are framed by the marketers, trying to buy back our privacy. Thus a titanic legal theory hits an iceberg shortly after it has left the port.

¶121 I have offered in this essay a somewhat sharp critique of Larry Lessig's discussion of privacy in his popular *Code and Other Laws of Cyberspace*. It is a critique that grows out of great regard for the vision of *Code* and great disappointment in the application of *Code*. While I agree with Lessig's recommendation that we need to consider more carefully the relationship between the architecture of cyberspace and the protection of social values, his discussion of privacy is deeply flawed. He fails to identify the relevant policy considerations, ignores much of the relevant history, and proposes an architecture of private ordering at odds with the public interests he otherwise seeks to protect. Lessig owes us a more thoughtful, rigorous discussion of privacy issues than the one presented in *Code*.

---

[140] *See, e.g.*, Trans Atlantic Consumer Dialogue, *Resolution on the Safe Harbor Proposal* (February 2000), http://www.tacd.org/ecommercef.html#harbor. It is significant that in the negotiation over the Safe Harbor proposal, what separates the U.S. government industry position from the U.S. consumer position is whether the full range of rights contemplated by the Fair Information Practices will be incorporated in the Commerce Department proposal. There is little interest among the consumer groups in pursuing the notice and choice regime of P3P. P3P as with other industry proposals is simply viewed as a way to avoid compliance with Fair Information Practices.

[141] Conferences about the regulation of cyberspace are routinely held by governments around the world. *See, e.g., IST99: Information Society Technologies Conference: Exploring the Information Society: People, Business, Technology*, http://www.ist99.fi; *Political for the Information Society* (March 1999), http://www.europa.eu.int/comm/dg24/policy/developments/info_soci/info_soci03_en.html (EU Rome Conference).

[142] LESSIG *supra* note 1, at hardcover edition book jacket.