PROGRAMMED PRIVACY PROMISES: P3P AND WEB PRIVACY LAW

WILLIAM MCGEVERAN*

A new computer protocol, the Platform for Privacy Preferences (P3P), now allows for the automatic translation of World Wide Web (Web) sites' privacy policies into an easily understandable form. In this Note, William McGeveran proposes a framework for lawmakers to take advantage of this new tool and respond to the threat to data privacy on the Web without unduly hindering the free flow of information. Like P3P's strongest supporters, he perceives advantages in a "P3P privacy market" where individuals could use P3P to understand Web site operators' privacy practices clearly, forcing below-par operators either to strengthen their policies or to offer visitors some benefit in exchange for personal data. While its libertarian proponents view this structure as a substitute for legal regulation, however, McGeveran argues that the regime should be predicated on contract rather than property principles and that law must play an active role in shaping and supervising the resulting market. He concludes by demonstrating how such a framework leaves lawmakers free to make a wide range of normative choices about privacy protection.

INTRODUCTION

Privacy policies of typical sites on the World Wide Web (the Web) contain hidden, verbose, jargon-cluttered statements that provide little guidance about the practices of the site's operator.[1] Now, a new computer protocol[2] called the Platform for Privacy Preferences (P3P) allows for the automated translation of these privacy policies into a

* I am grateful to Professors Sam Estreicher, Bill Nelson, and Yochai Benkler for their guidance through different stages of the writing process; to many of my fellow editors at the *New York University Law Review*—particularly Maggie Lemos, Shawn Larsen-Bright, Mina Park, and Jerry Dasti—for helpful suggestions and editing; and to Elizabeth Elliott McGeveran for her patience, love, and support.

[1] See Fed. Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace 24-26 (2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Sept. 4, 2001) [hereinafter FTC Report] (documenting problem of confusing and contradictory privacy policies at Web sites); Simson Garfinkel, Can a Labeling System Protect Your Privacy?, Salon, July 11, 2000, at http://www.salon.com/tech/col/garf/2000/07/11/p3p/index.html (bemoaning fact that "today's Web site privacy policies . . . are written by lawyers and their language can be fairly impenetrable"). This phenomenon is not limited to Web sites. See John Schwartz, Privacy Policy Notices Are Called Too Common and Too Confusing, N.Y. Times, May 7, 2001, at A1 (reporting on profusion of hard-to-understand privacy policies issued by financial institutions to comply with new requirements of federal law).

[2] A computer protocol is a set of standard rules governing computerized interactions, such as interactions between different types of software.

more understandable form.[3] Web users (or "surfers") can input their individual privacy preferences into P3P-compatible software.[4] Privacy-conscious surfers, for example, may wish to divulge a mailing address only when necessary to have an order shipped, while those who enjoy receiving catalogs may not mind if Web site operators add their addresses to mailing lists. Whenever surfers visit a P3P-compliant Web site, their computers interpret the site's policy, compare it to their preferences, and alert them in simple terms if there is a discrepancy. If the policy passes muster, a surfer may simply proceed to the site with confidence in its privacy practices—without needing to parse subordinate clauses.

P3P inspires polarized reactions. Its greatest supporters, including many Web businesses, view P3P as the key component of a libertarian privacy-protection regime requiring little or no intervention by the law.[5] They argue that P3P establishes a property-like entitlement to personal data[6] and empowers surfers to negotiate with Web site operators over its collection and use in an online privacy marketplace.[7] Critics of this laissez-faire approach emphasize its deficien-

[3] Lorrie Cranor et al., World Wide Web Consortium, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Working Draft (Sept. 28, 2001), at http://www.w3.org/TR/2001/WD-P3P-20010928/ [hereinafter P3P Specification]. For a detailed description of Platform for Privacy Preferences (P3P) technology, see infra Part II.

[4] See infra notes 106-20 and accompanying text (explaining functioning of this software).

[5] See, e.g., Developments in the Law: The Law of Cyberspace, 112 Harv. L. Rev. 1574, 1645-48 (1999) [hereinafter Harvard Developments] (declaring that use of P3P "will result in the optimal level of privacy protection"); Glenn R. Simpson, The Battle Over Web Privacy: As Congress Mulls New Laws, Microsoft Pushes a System That's Tied to Its Browser, Wall St. J., March 21, 2001, at B1 (describing computer industry lobbyists who argue that P3P obviates need for any Web privacy legislation); Leslie Walker, Browser Aimed at Protecting Users' Privacy, Wash. Post, Mar. 29, 2001, at E4 (reporting that Microsoft is promoting P3P "in a bid to help the Internet industry ward off new privacy laws from Congress"); see also Deirdre Mulligan et al., P3P and Privacy: An Update for the Privacy Community, at http://www.cdt.org/privacy/pet/p3pprivacy.shtml (Mar. 28, 2000) (conceding that "some have over-hyped the standard, claiming that P3P will, on its own, fully address privacy concerns").

[6] This Note will define "personal data" or "personal information" as any facts about a particular individual who is or can be identified. See P3P Specification, supra note 3, § 1.3 (providing similar definition for "identified data"). Note that the term includes information that can be tied to an individual indirectly. For example, data connected to a person's mailing address or social security number, which can then be mapped to the person, qualifies as personal data. See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1206-08 (1998) (describing indirect ways information can be "identifiable to an individual").

[7] See infra Part III.A (describing libertarian idea of P3P privacy market).

cies[8] and support a regulatory regime for privacy protection in which P3P would play no significant role.[9]

This dispute presents a false dichotomy between two ways of promoting privacy on the Web.[10] It springs from a broader market-or-regulation debate over privacy, a "quasi-religious war to resolve whether the nature of a person's interest in her personal data is a fundamental civil liberty or [a] commodity interest."[11] As Lawrence Lessig has explained, however, behavior in cyberspace is constrained by different "modalities," which include technology (or "code"), the market, and the law.[12] Because these modalities interact with one an-

[8] See infra Part III.B (analyzing shortcomings of libertarian approach).

[9] See, e.g., Electronic Privacy Information Center & Junkbusters Corp., Pretty Poor Privacy: An Assessment of P3P and Internet Privacy, at http://www.epic.org/reports/prettypoorprivacy.html (June 2000) [hereinafter EPIC/Junkbusters Report] (condemning P3P as privacy-protection setback and suggesting it delays adoption of effective political solutions); Jessica Litman, Information Privacy/Information Property, 52 Stan. L. Rev. 1283, 1297-98 (2000) (attacking "fairy-tale picture of easy bargaining" through P3P as "nonsense"); Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 Stan. Tech. L. Rev. 1, at ¶¶ 72-89, at http://stlr.stanford.edu/STLR/Articles/01_STLR_1 (critiquing P3P and concluding its code "maps nicely to the anti-regulatory views espoused by industry"); Christopher D. Hunter, Recoding the Architecture of Cyberspace Privacy: Why Self-Regulation and Technology Are Not Enough 12-14 (February 2000) (unpublished essay), at http://www.asc.upenn.edu/usr/chunter/net_privacy_architecture.html (determining that "P3P merely codes industry's view of privacy, and thus actually makes it harder for users to protect themselves").

[10] "World Wide Web" (the Web) is a narrower term than "Internet." The Web is just one Internet application, which functions through a routing protocol called HTTP (Hypertext Transfer Protocol). The "Internet" refers to a larger underlying network that uses a suite of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol) to route varied applications—including e-mail, file transfers, and Usenet—in addition to Web content. See Timothy Wu, Application-Centered Internet Analysis, 85 Va. L. Rev. 1163, 1165 (1999) (analogizing applications layered on top of TCP/IP's fundamental routing mechanisms to different household appliances layered on top of universal AC/DC electricity standard); see also Robert E. Kahn & Vinton G. Cerf, Internet Policy Institute, What Is the Internet? (And What Makes It Work) (December 1999), at http://www.internetpolicy.org/briefing/12_99_story.html (explaining functioning of TCP/IP). A still broader term, "cyberspace," refers to the entire modern global information infrastructure. This Note will focus on the Web, rather than the entire Internet or cyberspace, because (1) P3P is designed for the Web; (2) the bulk of current threats to privacy arise on the Web, which is particularly interactive and commercialized, see infra Part I.A; and (3) while future development of information technology is unpredictable, the user-friendliness and success of the Web make it likely that convergence in cyberspace will move toward Web-like applications, see, e.g., Michael Lewis, Boom Box, N.Y. Times, Aug. 13, 2000, § 6 (Magazine), at 36 (discussing advent of interactive television device called TiVo, which collects personal data by means similar to Web).

[11] Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125, 1157-58 (2000); see also Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815, 815-16 (2000) (criticizing "deeply flawed rhetoric" of market-state dichotomy).

[12] Lawrence Lessig, Code: And Other Laws of Cyberspace 86-90, 235-39 (1999) (defining "regulatory modalities"). Lessig also identifies a fourth modality, social norms, which is beyond the scope of this Note because it is not under the direct influence of lawmakers

other in complex ways, lawmakers[13] ought to blend all of them into systems of rules for the Web rather than choosing between them.[14]

This Note proposes such an integrated system for protecting privacy on the Web. The code of P3P is just one element of a solution, as its designers are the first to agree.[15] Lawmakers should combine P3P with carefully harnessed market forces and well-crafted legal rules.[16] They should create a regulated P3P privacy market that protects privacy using multiple modalities.

Part I of this Note identifies the tension between two goals lawmakers must reconcile: protecting personal data and promoting the unhindered flow of information on the Web. Part II explains how P3P actually functions. Part III turns to the dominant libertarian proposal for deploying P3P, first discussing this approach and its advantages before examining valid criticisms against it on both doctrinal and practical grounds. Part IV proposes an alternative that combines the code of P3P with the modalities of both market and law to protect data privacy without unduly constraining the flow of information on the Web.

I
Competing Goals for the Web

The Web gives surfers unprecedented access to information about the world while the world gains similarly unprecedented access to information about surfers. Americans appear enthusiastic about the

seeking to protect privacy. Nonetheless, lawmakers should recognize that the other modalities can influence norms profoundly, and that the resulting norms, in turn, reinforce the impact of code, market, and law. Thus, they should employ these other modalities with an eye to the norms they would thereby encourage. See generally Steven Hetcher, The FTC as Internet Privacy Norm Entrepreneur, 53 Vand. L. Rev. 2041 (2000) (discussing government's role in promoting behavioral norms that respect privacy).

[13] The term "lawmakers" will be used in this Note to describe legislators and regulators responsible for shaping the government's policy response to P3P. The possibly more accurate term "policymakers" creates too much potential for confusion with those writing Web sites' privacy policies.

[14] Lessig, supra note 12, at 235-39 (emphasizing interaction of modalities); Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Tex. L. Rev. 553, 555 (1998) (arguing that lawmakers should accommodate behavioral restraints imposed by technology when crafting legal rules).

[15] P3P Specification, supra note 3, §§ 1, 1.1.1 (explaining capabilities and limitations of P3P as purely technical mechanism); Mulligan et al., supra note 5 ("P3P needs a regulatory or policy context to help protect privacy, it cannot do this by itself."). The authors of the latter report are privacy advocates who participated in the P3P drafting process.

[16] See infra Part IV (proposing legal rules to complement P3P); see also Garfinkel, supra note 1 (determining that P3P requires legislative support to function, but that "combined with regulation, P3P could be a pretty impressive tool"); Lawrence Lessig, Op-ed, Technology Will Solve Web Privacy Problems, Wall St. J., May 31, 2000, at A26 (stating that, while P3P is "code-based solution," Congress should subsidize or mandate its use).

first attribute[17] but alarmed by the second.[18] This Part discusses these two competing responses and the architecture of the Web. On one hand, the unchecked flow of personal data raises serious concerns. On the other, information—at times including personal data—is the Web's lifeblood and restricting its flow threatens the Web's vitality.

A. *The Threat to Data Privacy*

While most people instinctively appreciate the importance of data privacy,[19] scholars have encountered some difficulty articulating its precise justifications. Historically, they often have pointed to interests in dignity and autonomy.[20] The disclosure of some types of personal data simply may be embarrassing.[21] Even when not inherently embarrassing, fragmentary personal facts taken out of context may lead others to misjudge us, undermining our integrity.[22] Without data pri-

[17] According to the Web monitoring service Nielsen//NetRatings, the number of Americans who used the Web increased by sixty-three percent between July 1999 and July 2001; fifty-eight percent of all Americans had access to the Internet in their home by July 2001. See Press Release, Nielsen//NetRatings Inc., Internet Captures 63 Percent Growth in the Past Two Years, According to Nielsen//NetRatings (Aug. 13, 2001), at http://www.nielsen-netratings.com/pr/pr_010813.pdf.

[18] One typical opinion survey found that eighty-four percent of the nation's Internet users were "concerned" or "very concerned" about "businesses or people they don't know getting personal information about themselves or their families" from their Internet use. Susannah Fox et al., The Pew Internet & American Life Project, Trust and Privacy Online: Why Americans Want to Rewrite the Rules 6 (Aug. 20, 2000), http://www.pewinternet.org/reports.

[19] All references to "privacy" in this Note refer to "data privacy," which is defined as control of the dissemination of one's personal data. See Alan F. Westin, Privacy and Freedom 7 (1967) (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"); Kang, supra note 6, at 1205 (defining "data privacy" as "an individual's claim to control the terms under which personal data . . . is used"); Frederick Schauer, Internet Privacy and the Public-Private Distinction, 38 Jurimetrics 555, 556 (1998) (defining "database privacy" as "right of individuals to control the distribution and availability of information about themselves"). This definition leaves open the threshold normative question of how *much* decisionmaking autonomy a surfer must have to qualify as exercising this "control." See infra note 141 and accompanying text (discussing differing conceptions of sufficient information autonomy).

[20] For examples of classic past efforts to define the interests protected by data privacy, see generally Westin, supra note 19; Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev. 962 (1964); William L. Prosser, Privacy, 48 Cal. L. Rev. 383 (1960); Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

[21] Tort law recognizes a particular interest in protecting personal data that is embarrassing. See Restatement (Second) of Torts, § 652D cmts. c, h (1977) (providing tort liability for disclosure of private facts only when "a reasonable person would feel justified in feeling seriously aggrieved by it").

[22] See Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America 8-11 (2000) (discussing how others jump to conclusions about us based on personal data that is incomplete or out of context).

vacy, in turn, we cannot reveal ourselves selectively to different audiences, which reduces our ability to form relationships,[23] to express our true selves,[24] and to experiment with nonconforming ideas.[25] Ultimately, the resulting fear of undesirable exposure can lead to self-censorship, further eroding dignity and autonomy.[26]

Whatever its exact philosophical basis, individuals certainly value data privacy.[27] Yet our personal data is also extremely valuable to others. A mammoth, multibillion-dollar industry now engages in collecting and processing it for direct marketing purposes.[28] Insurers, employers, and government[29] also find personal data useful.[30]

The law does little to counterbalance the incentives to collect personal data on the Web,[31] except for a few narrow statutes and regulations.[32] As currently interpreted, tort law provides little protection for

[23] See generally Charles Fried, Privacy, 77 Yale L.J. 475 (1968) (arguing that selective revelation of personal data is basis for friendship, love, and trust).

[24] In one famous case, a gay sailor discussed his sexual orientation in a seemingly anonymous online profile, only to have it revealed to his military superiors, who commenced proceedings to discharge him. See McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

[25] Neil Weinstock Netanel warns that fear of monitoring makes a surfer "significantly more likely to eschew controversial website content, thus moving towards the bleak conformism that Mill saw as the greatest threat to 'personal liberty' . . . in a modern democracy." Neil Weinstock Netanel, Cyberspace 2.0, 79 Tex. L. Rev. 447, 466-67 (2000) (book review).

[26] 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) (arguing that chilling effect of monitored reading makes right to read anonymously central to exercise of First Amendment freedoms).

[27] See supra note 18 (citing opinion survey showing concern about data privacy).

[28] See Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century 164-68 (2000) (describing functioning of data collection industry, using $1.5 billion company Experian as example).

[29] Government interests include, but are not limited to, law enforcement. See Gavin Skok, Establishing a Legitimate Expectation of Privacy in Clickstream Data, 6 Mich. Telecomm. & Tech. L. Rev. 61, 68-70 (2000) (describing personal data gathered from surfer's Web use as "fertile source of information for law enforcement"). Political candidates also use profiles of personal data to target their appeals. See, e.g., Leslie Wayne, Voter Profiles Selling Briskly as Privacy Issues Are Raised, N.Y. Times, Sept. 9, 2000, at A1 (describing company that provides detailed profiles of voters and other services, including targeted Web advertising for political candidates).

[30] See Rosen, supra note 22, at 164-65 (providing examples of personal data of interest to insurers, employers, and government).

[31] For surveys of data privacy law applicable to the Web, see generally Fred H. Cate, Privacy in the Information Age 80-100 (1997); Priscilla M. Regan, Legislating Privacy (1995); Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law (1996); Jeff Sovern, Protecting Privacy with Deceptive Trade Practices Legislation, 69 Fordham L. Rev. 1305, 1312-20 (2001).

[32] A notable exception is the Children's Online Privacy Protection Act, 15 U.S.C.S. §§ 6501-6505 (LEXIS 2001), which substantially regulates Web site operators' collection of personal data from minors. For adults, however, data privacy is regulated on an industry-by-industry patchwork basis, without particular requirements for the Web. E.g., 15 U.S.C.

truthful personal data.[33] A constitutional right to data privacy never has been recognized.[34]

Meanwhile, the architecture of the Web makes intruding on data privacy easier than ever before in at least three different ways.[35] First, many of the Web's technical features, whatever their other purposes,

§ 1681 (Supp. IV 1999) (requiring credit bureaus to provide means for consumers to opt out of certain data-sharing practices); 15 U.S.C.A. § 6802 (West Supp. 2001) (requiring financial institutions to disclose certain uses of personal data and offer opt-out); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (1994) (prohibiting video rental businesses from disclosing customers' personal data); 47 U.S.C. § 551 (1994) (prohibiting cable television companies from disclosing certain personal data of customers); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164) (regulating disclosure of patients' personally identifiable health data to third parties by health care providers, insurers, and similar entities). Rules restricting government collection of personal data tend to be somewhat stricter. E.g., Privacy Act of 1974, 5 U.S.C. § 552 (1994) (regulating federal government's collection and use of personal data); Drivers' Privacy Protection Act of 1994, 18 U.S.C.A. § 2721 (2000) (upheld in Reno v. Condon, 528 U.S. 141 (2000)) (requiring opt-in for state motor vehicle departments to release personal data from records to marketers); Pub. L. 106-346, § 501 (enacting by reference H.R. 5394) (2000) (restricting federal government collection of personal data on Web without surfers' knowledge). Some states also have modest privacy laws. Sovern, supra note 31, at 1315-17 (listing examples of state privacy laws).

[33] Cate, supra note 31, at 89-90 (concluding that existing privacy torts offer little protection for data privacy); Schwartz & Reidenberg, supra note 31, at 334 (same); Litman, supra note 9, at 1304 ("Unfortunately, as the literature has made very clear, the invasion of privacy tort is too narrowly defined [to protect data privacy].").

[34] The Supreme Court once hinted at its possible existence. Whalen v. Roe, 429 U.S. 589, 605 (1977) (noting, in dicta, that data privacy interest "arguably has its roots in the Constitution"). Academic commentary supporting such a right is less coy. See, e.g., Cohen, supra note 26, at 1003-38 (basing data privacy rights on First Amendment); Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609, 1647-66 (1999) (arguing that data privacy is necessary for political discourse and exercise of constitutionally protected rights); Francis S. Chlapowski, Note, The Constitutional Protection of Informational Privacy, 71 B.U. L. Rev. 133, 150-59 (1991) (arguing that data privacy is protected under Due Process Clause). But see A. Michael Froomkin, The Death of Privacy?, 52 Stan. L. Rev. 1461, 1540-41 (2000) (suggesting that "[p]rivacy-destroying technologies do not line up particularly well" with constitutional analysis); Steven A. Bibas, Comment, A Contractual Approach to Data Privacy, 17 Harv. J.L. & Pub. Pol'y 591, 602 (1994) (emphasizing that *Whalen* involved state action and that present Supreme Court is "unlikely to extend" any such right to cover private-sector entities).

[35] For general descriptions of the characteristics of the Web that enable collection of personal data, see, for example, Jerry Berman & Deirdre Mulligan, Privacy in the Digital Age: Work in Progress, 23 Nova L. Rev. 549, 554-68 (1999); Kang, supra note 6, at 1223-31; Leslie A. Kurtz, The Invisible Becomes Manifest: Information Privacy in a Digital Age, 38 Washburn L.J. 151, 154-69 (1998); Lawrence Jenab, Comment, Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress, 49 U. Kan. L. Rev. 641, 642-47 (2001); Daniel Tynan, In Web We Trust?, PC World, June 2000, at 103; Center for Democracy and Technology, CDT's Guide to Online Privacy, at http://www.cdt.org/privacy/guide/start/track.html (last visited Aug. 22, 2001) [hereinafter CDT Guide]; Hunter, supra note 9, at 2-4; Junkbusters Home Page, at http://www.junkbusters.com (last visited Aug. 22, 2001).

enable undetected collection of personal data. As you navigate the Web, you create a "clickstream" which documents the exact sequence of movements you make, down to the number of seconds you linger on each page.[36] Data collectors can learn about you and your clickstream from such mechanisms as IP addresses,[37] referrers,[38] search strings,[39] smart browsing features,[40] Web bugs,[41] hardware IDs,[42] spyware,[43] and other software.[44] In the offline world, a persistent person can take steps to reduce the transfer of personal data (and the amount of junk mail received in return).[45] On the Web, however,

[36] See CDT Guide, supra note 35 (discussing clickstream data, and providing as synonyms "mouse droppings" and "data trail"); FTC Report, supra note 1, at 46 n.59 (defining clickstream data).

[37] An IP address routes content to a particular computer. If you obtain Internet access through work or school, your IP address probably reveals this affiliation. See Kang, supra note 6, at 1224-25.

[38] When you click a link on Site A to jump to Site B, you also send a "referrer" to Site B which reveals that you just visited Site A. See CDT Guide, supra note 35.

[39] When you enter terms into a search engine and then link to one of the resulting hits, the search engine's referrer likely includes your entire search query. See Junkbusters Home Page, supra note 35. Search strings could be quite revealing, potentially suggesting, for example, a person's interest in particular sexual, medical, or political topics.

[40] See Joel Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L.J. 771, 780 (1999) (noting features of Netscape and Microsoft browsers that can upload clickstream data).

[41] Web bugs are tiny bits of content on a Web page that allow invisible collection of clickstream data. See Schwartz, supra note 11, at 819 & n.19 (noting that Web bugs allow collection of surfers' personal data from multiple sites); Robert O'Harrow, Jr., Fearing a Plague of Web Bugs, Wash. Post, Nov. 13, 1999, at E1 (same).

[42] See Froomkin, supra note 34, at 1490-94 (describing move to add unique identifying tags to hardware and resulting interaction between IDs and other personal data). In the longer term, as household appliances become networked and require hardware IDs, this concern will become more pressing. Id.

[43] A few companies have invisibly installed these small programs on individuals' computers; the programs transmit information about the user's computer back to the servers that installed them. See Neil J. Rubenking, Who's Watching You Surf?, PC Magazine, July 2000, at 110.

[44] See Ann Bartow, Our Data, Ourselves: Privacy, Propertization, and Gender, 34 U.S.F. L. Rev. 633, 678 (2000) (discussing Comet Systems animated cursor that tracked clickstream for large companies); Sara Robinson, CD Software Said to Gather Data on Users, N.Y. Times, Nov. 1, 1999, at C1 (reporting that popular RealNetworks software for playing music on computers also monitored user's listening habits and transmitted this data, tied to identity, back to company). Inventive computer scientists continue to find new possibilities for invisible monitoring in an environment as technologically complex as the Web. See, e.g., Ian Austen, Study Finds That Caching by Browsers Creates a Threat to Surfers' Privacy, N.Y. Times, Dec. 14, 2000, at G11 (reporting on paper by Princeton computer scientist speculating that Web site operators could easily discern some clickstream data by using Java applet to infiltrate browser caches).

[45] See Co-op America, The WoodWise Consumer Guide 13 (2001), available at http://www.coopamerica.org/woodwise (last visited Oct. 18, 2001) (suggesting techniques to reduce transfer of personal data to marketers and stay off mailing lists); Junkbusters Home Page, supra note 35 (providing similar advice).

there are few means to express this preference, and surfers may not even realize the need to do so if their personal data was collected without their knowledge.

Second, while such invisible data collection may garner the most media attention, the Web's interactive nature also makes surfers more likely to divulge personal data voluntarily. When surfers order products from Web merchants, for example, they provide their names and addresses for shipping and credit card numbers for payment, a far cry from anonymous cash-and-carry transactions at a store.[46] Personal data collected for one purpose can be squirreled away for use in other contexts that consumers might not have imagined when they first revealed the data. In some cases, the supposed reason for data collection is a mere pretense for building profiles of individual surfers.[47]

Third, a surfer's personal data, whether generated knowingly or not, is less evanescent than it may seem.[48] A lone surfer may not comprehend the value of small pieces of personal data and thus feel more willing to reveal it.[49] Because it is already in a computerized format, however, the personal data is easy to store, manipulate, aggregate,

[46] As other examples, you may complete a survey about your political opinions on a news site, rate a book or movie at an entertainment site, or reveal your music tastes when customizing a music site. All of this information is of potential use to marketers.

[47] See Kang, supra note 6, at 1253 & nn.255-56 (citing practices of some data collectors, including deriving address information from credit card numbers and administering ostensible surveys truly aimed at extracting personal data); Seth Schiesel, Is 'Flack Whacking' Good Public Relations?, N.Y. Times, Oct. 2, 2000, at C4 (describing game on Web site, http://www.whackaflack.com, where reporters throw paper airplanes at caricatures of public relations people and vent complaints about them, allowing sponsor to create database of 5000 reporters' e-mail addresses and views on different public relations agencies); Bob Tedeschi, Internet Merchants Turn to Online Sweepstakes, N.Y. Times, June 19, 2000, at C11 (noting marketers' common use of sweepstakes on Web sites to entice players "to fork over their e-mail addresses and other valuable personal information").

[48] Indeed, some personal data on the Web is archived and available to the public permanently. See, e.g., Fred Bernstein, Op-ed, An Online Peek at Your Politics, N.Y. Times, Oct. 4, 2000, at A35 (questioning privacy implications and chilling effect of Web site that provides individuals' political campaign contributions indexed by zip code); Pamela LiCalzi O'Connor, Tracking a Suspect on an Online Trail, N.Y. Times, Jan. 8, 2001, at C4 (describing movie tastes of alleged mass murderer based upon his video gift registry at Web site); Deborah Schoeneman, Don't Be Shy Ladies—Google Him!, N.Y. Observer, Jan. 15, 2001, at 1 (chronicling trend among Manhattan singles of investigating background of prospective dates using search engine).

[49] See Froomkin, supra note 34, at 1501-05 (describing "privacy myopia" of surfers who value individual pieces of personal data less than do data collectors who can add value through aggregation); Neil Weinstock Netanel, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, 88 Cal. L. Rev. 395, 476-77 (2000) (describing average surfer's surprise that "bits of personal information" can be aggregated into "pervasive profile"). P3P may reduce transaction costs enough to overcome this problem by making the cost of expressing preferences even lower than the value the "myopic" surfer places on individual bits of personal data. Froomkin, supra note 34, at 1505.

and transfer.[50] Some is stored routinely as an aspect of the Web's architecture.[51] In addition, data collectors store information about a surfer and his or her clickstream by placing a file on his or her personal computer called a cookie, which is retrieved and augmented each time the surfer returns to a Web site.[52] A majority of commercial sites place additional cookies on behalf of third parties,[53] particularly advertisers.[54] Once personal data is amassed in these ways, businesses can manipulate and aggregate it to create a profile greater

[50] See Netanel, supra note 49, at 473-74 (discussing "virtually limitless possibilities for compiling, analyzing, and systematizing" digitized personal data).

[51] See, e.g., CDT Guide, supra note 35 (summarizing personal data contained in Web sites' user logs). An Internet service provider (ISP) has the ability to use stored information to build a profile of a surfer's movements throughout the entire Web, rather than just within a particular site. See The Predictive Network for ISPs, at http:// www.predictivenetworks.com/products/digital_sil.html (last visited Sept. 4, 2001) (selling product for ISPs called Digital Silhouette, which allows ISP to create profile of each customer, although asserting that profiles contain no personally identifiable information and require user opt-ins).

[52] See Jessica J. Thill, Comment, The Cookie Monster: From Sesame Street to Your Hard Drive, 52 S.C. L. Rev. 921, 921-24 (2001) (describing cookies as "numerical identifiers deposited onto a user's hard drive"); CDT Guide, supra note 35 (describing use of cookies). Cookies, like many of the other features of the Web described in this Section, also have benign or beneficial purposes unconnected to data collection. See Information Privacy: Industry Best Practices and Technological Solutions, Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce, 107th Cong. 22 (2001) (statement of Michael Wallent, Product Unit Manager, Internet Explorer, Microsoft Corp.), available at 2001 WL 21756455 [hereinafter Wallent Testimony] ("Without cookies, the web wouldn't work as people expect it to. There would be no customization, no e-commerce and the economics of the web would be called into question."); Thill, supra, at 921 (noting benefits of cookies).

[53] The FTC found that fifty-seven percent of commercial Web sites polled overall, and seventy-eight percent of the most popular sites, allowed the placement of cookies by third parties. FTC Report, supra note 1, at 21.

[54] For example, if you visit two of the 1500 Web sites where DoubleClick places advertising, see John Schwartz, Trade Commission Drops Inquiry of DoubleClick, N.Y. Times, Jan. 23, 2001, at C5, information from your browsing sessions at *both* sites could be stored on DoubleClick's cookie. DoubleClick has cookies for a staggering 100 million surfers; the Web profiling company Engage has 52 million surfer profiles. See Tynan, supra note 35, at 106. DoubleClick purchased an offline profiling company in 1999 and was denounced for plans to link cookie data with its profiles; the Federal Trade Commission (FTC) has dropped an inquiry into these issues. See Schwartz, supra. Privacy advocates remain skeptical. See Tynan, supra note 35, at 106 (quoting privacy advocate Robert Ellis Smith as saying that DoubleClick "simply agreed to defer their plans until the heat's gone"). More recently, the company explored plans to link the data but hire a third party to "cleanse" it by stripping personal identifiers. Bob Tedeschi, E-Commerce Report: DoubleClick is Seeking Ways to Use Online and Offline Data and Protect Users' Anonymity, N.Y. Times, Jan. 29, 2001, at C9. Even this plan, however, would involve the use of unique numbers, a form of personal identifier. See supra note 6 (defining personal data to include indirectly identifiable information).

than the sum of its parts, which then may be sold to or shared with anyone.[55]

Thus, the Web's character radically expands the disclosure and collection of personal data[56] far beyond the levels possible offline.[57] Calls for increased protection of data privacy on the Web are based firmly on the reality of its architecture.

B. *The Importance of Free Information Flows*

Nonetheless, lawmakers eager to protect data privacy should proceed with caution. The value of the Web as a "global library" lies in the unprecedented availability of information it affords.[58] Many of the more significant advantages of the Web involve customized content, and such individualized tailoring naturally requires personal data. Moreover, much of the information that makes the Web a useful resource is personal data. Regulations to protect privacy must be balanced against the costs of constraining the flow of personal data.

First, surfers choose to reveal some amount of personal data in order to enjoy the full advantages of the Web's resources.[59] By dis-

[55] As media ownership becomes more concentrated, once-independent businesses presumably will share data with their postmerger affiliates. In addition, numerous companies now are developing an interoperability standard to facilitate the computerized transfer of such files. Robert O'Harrow, Jr., Internet Firms Act to Ease Sharing of Personal Data, Wash. Post, Dec. 5, 2000, at E1 (describing development of "Customer Profile Exchange" by companies including IBM and First Union).

[56] A survey of a random sample of commercial Web sites conducted in 2000 found that ninety-seven percent collected personal data. FTC Report, supra note 1, at 9.

[57] Jerry Kang dramatizes the overall impact by comparing a typical visit to the mall with a similar excursion on the Web. In the real-space mall, your movements and casual browsing are unrecorded, and only a credit card purchase yields personal data. In contrast,

> [a]s soon as you enter the cyber-mall's domain, the mall begins to track you . . . . It automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyberbookstore notes which magazines you skimmed, recording which pages you have seen and for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John's Wort, read for seven minutes a newsweekly detailing a politician's sex scandal, and flipped ever-so-quickly through a tabloid claiming that Elvis lives. . . . All these data generated in cyberspace are detailed, computer-processable, indexed to an individual, and permanent.

Kang, supra note 6, at 1198-99.

[58] See, e.g., Kathleen M. Sullivan, First Amendment Intermediaries in the Age of Cyberspace, 45 UCLA L. Rev. 1653, 1666, 1669-70 (1998) (extolling ability of Web to create "global library" and enable abundance of speech).

[59] Of course, this tradeoff is not limited to the Web. "Instant credit, better targeted mass mailings, lower insurance rates, faster service when ordering merchandise by telephone, special recognition for frequent travelers, and countless other benefits come only at the expense of some degree of privacy." Cate, supra note 31, at 30-31.

closing personal data, surfers may receive benefits such as access to a particular site,[60] increased convenience,[61] personalized content,[62] targeted marketing information,[63] free merchandise,[64] or self-expression.[65] Surfers' varying individual decisions to exchange personal data for benefits reflect their differing tastes for privacy.[66]

In addition to considerations of surfers' expressive choices, lawmakers also must attend to the equivalent interests of data collectors. The Supreme Court has ruled that the First Amendment applies with full force to the Web.[67] Yet many potential regimes for restrict-

[60] For example, those who wish to visit the New York Times Web site, at http://www.nytimes.com, must register and divulge personal data.

[61] See Rosen, supra note 22, at 197-98 (noting that convenience is often more important to consumers than protecting personal data about purchases). Surely, most readers can think of examples in their own surfing. This author keeps an account at Drugstore.com with a list of frequently ordered items, allowing reorders with simple clicks. The Web site operator thus creates an excellent profile of the exact products purchased and how often they are purchased, but ease and speed outweigh the problem of exposure of the medicine cabinet.

[62] On many sites, for example, you can enter your zip code to receive local weather reports or sports scores. See, e.g., My Netscape, at http://my.netscape.com (allowing users to register and personalize content of Netscape home page).

[63] Personalization might range from offering travel services that appeal to individual interests to suggesting cosmetics that complement the customer's particular skin tone. See Rebecca Gardyn, Swap Meet: Consumers Are Willing to Exchange Personal Information for Personalized Products, Am. Demographics, July 2001, at 52 (reporting survey results indicating that seventy-eight percent of adults would exchange some personal information for customized products and services). Younger consumers are most interested in such targeted sales. Id. (reporting that different survey finds eighty-five percent of those between ages eighteen and twenty-four wish that more products and services were customized).

[64] As one analyst notes cynically, "We're Americans. We'll give up anything for 50 frequent flier miles." Deborah Lohse, Paying for Privacy Market Could Be Huge, but Consumers Are a Tough Sell, San Jose Mercury News, Nov. 24, 2000, at 1C, LEXIS, News Library, San Jose Mercury News File (quoting Jonathan Gaw of technology research firm IDC). This expert says his research found that consumers would reveal information they wanted to keep secret in exchange for gift certificates of fifty or one hundred dollars. Id.; see also Karen Kaplan, In Giveaway of 10,000 PCs, the Price is Users' Privacy, L.A. Times, Feb. 8, 1999, at A1 (describing consumers who volunteer to have surfing monitored in exchange for free computer).

[65] Personal Web pages posted at sites such as Yahoo! Geocities, at http://geocities.yahoo.com, include everything from family photo albums to fan pages devoted to music or film stars to pages whose creators simply describe themselves and their personal interests and tastes. There are also extreme examples of those who see value in self-expression—and sometimes profit—that they derive from revealing vast quantities of personal data on exhibitionist Web sites. See, e.g., Jennicam, at http://www.jennicam.org (transmitting pictures from constantly active cameras in home of Jennifer Ringley, along with her journal entries and poems).

[66] Sovern, supra note 31, at 1312-13 (noting that individual taste for privacy varies from person to person); Bibas, supra note 34, at 603-05 (same).

[67] Reno v. ACLU, 521 U.S. 844 (1997) (overturning Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (1996), on First Amendment grounds). Although the decision's language generally refers to the entire Internet, its substance actually focuses

ing the disclosure of personal data could run afoul of the First Amendment, because Web site operators and data collectors arguably have rights to communicate factual information about their customers for commercial purposes.[68] Moreover, a privacy-enforcing "right to have the government stop you from speaking about me"[69] stands atop a slippery slope of closely analogous speech controls: If privacy concerns justify constraining a Web site operator from divulging personal data, what stops the application of the same rationale to, for example, a journalist?[70] While the exact scope of the conflict between data privacy and the First Amendment is debatable, lawmakers must at least remain cognizant of the tension and tailor rules narrowly enough to avoid infringing freedom of speech.[71]

Finally, restrictions on disclosure of personal data create economic costs.[72] Advertising revenue on the Web has plummeted recently because of dissatisfaction with its effectiveness.[73] Commercial

on the Web in particular. See Wu, supra note 10, at 1171-74 & 1172 n.17 (distinguishing *Reno* analysis of Internet and Web).

[68] See, e.g., U.S. West, Inc. v. FCC, 182 F.3d 1224, 1240 (10th Cir. 1999) (overturning, on First Amendment grounds, regulations concerning handling of personal data); Kang, supra note 6, at 1277-82 (acknowledging First Amendment obstacles to data privacy rules); Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 Stan. L. Rev. 1049, 1122 (2000) (concluding that most restrictions on revealing personal data violate First Amendment); Scott Shorr, Note, Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment, 80 Cornell L. Rev. 1756, 1795-1812 (1995) (determining that credit bureaus' disclosure of personal data is protected by First Amendment). But see Trans Union Corp. v. FTC, 245 F.3d 809 (D.C. Cir. 2001) (holding that First Amendment does not apply to use of personal data in credit reports and upholding regulations under Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994), restricting its sale for marketing purposes); Paul M. Schwartz, Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence, 52 Stan. L. Rev. 1559, 1560-64 (arguing that many privacy protection rules are "nonsilencing" and thus do not infringe freedom of speech).

[69] Volokh, supra note 68, at 1051.

[70] Id. at 1051-53, 1080-1120 (analyzing justifications often provided for data privacy protections and warning that they also could support more speech-restricting proposals, including limits on news reporting).

[71] See supra note 68 (collecting sources on both sides of question). A full analysis of the First Amendment arguments on each side is beyond the scope of this Note. The proposal developed in Part IV avoids conflict with the First Amendment. See infra notes 187-88 and accompanying text.

[72] See Solveig Singleton, Cato Institute, Privacy as Censorship 8-13 (Jan. 22, 1998), http://www.cato.org/pubs/pas/pa-295.pdf (describing economic function of personal data). Restrictions on collecting personal data might have a disproportionate impact on new or small businesses and charities that cannot rely on preexisting lists of potential customers or donors. Id. at 13.

[73] See Saul Hansell, Free Rides Are Now Passé on Information Highway, N.Y. Times, May 1, 2001, at A1 (describing precipitous drop in Web advertising rates, including one Web site which went from charging between fifty and seventy-five dollars to charging between three and five dollars for equivalent advertising).

Web sites must respond, presumably in one of two ways. They can improve their advertisers' results, most likely by increasing the ability to target appeals to probable customers with clickstream-based personalization.[74] Or they can turn to a different revenue source, most likely by imposing access fees or service charges on surfers.[75] Increased profiling may intensify intrusions on data privacy, but the alternatives would radically change the open character of the Web and make it more expensive to surf—perhaps prohibitively so for some Americans.[76] If broad privacy-protection rules make personalization impractical, fees may become inevitable, externalizing the cost of some surfers' desires for privacy on all who use the Web.[77]

[74] For example, clickstreams that lead to Web sites describing London's tourist attractions might trigger an advertisement for British Airways. The Web profiling company Engage claims that surfers are fifty percent more likely to click on an ad if it is targeted to them through such profiling rather than merely placed on a Web page with related subject matter. Josh McHugh, Hall of Mirrors, Forbes, Feb. 7, 2000, at 120; see also Susan Stellin, Internet Companies Learn How to Personalize Service, N.Y. Times, Aug. 28, 2000, at C8 (describing trial-and-error efforts by companies to improve personalization and "targeted merchandising"). It is possible that changes in the style and technology of Web advertising also may help somewhat, although more effective ads are probably more intrusive ads. See, e.g., Susan Stellin, We Now Interrupt Your Browsing for This Commercial Message, N.Y. Times, Dec. 18, 2000, at C34 (describing "interstitials," ads that interrupt surfing and play while other Web pages are loading and yield better response rates than standard banner ads).

[75] See Hansell, supra note 73 (listing many examples of Web sites that were once supported by advertising but now charge for access or services). Even newspaper Web sites, where paid subscriptions have been considered "anathema," are now rethinking the idea in the face of shrinking advertising revenue, and may choose to imitate the Wall Street Journal, which has 500,000 paid subscribers to its Web site. Felicity Barringer, Rethinking Internet News as a Business Proposition, N.Y. Times, Jan. 22, 2001, at C1; see also Hansell, supra note 73 (noting that more news and information sites are charging fees or considering doing so). Consumer Reports, which does not accept advertising in its magazine or on the Web, charges for access to its Web site. See Consumer Reports Online, at http://www.consumerreports.org (last visited Oct. 18, 2001).

[76] The socioeconomic "digital divide" between those who use the Web and those who do not is already a serious problem. See National Telecommunications and Information Administration, Falling Through the Net: Toward Digital Inclusion 33, 36-37 (Oct. 2000), available at http://www.ntia.doc.gov/ntiahome/digitaldivide (reporting that 70.1% of those with household incomes above $75,000 were Internet users, compared to 18.9% of those with household incomes under $15,000 and 25.5% in category between $15,000 and $24,999). These economic disparities correspond with racial differences. See id. at 37-38 (reporting that 50.3% of whites, 29.3% of blacks, and 23.7% of Hispanics use Internet).

[77] See Harvard Developments, supra note 5, at 1648 (identifying reduced Web advertising revenue as potential "social cost" of privacy). Scholars long have recognized that data privacy externalizes costs—for example, by forcing lenders or auto insurers to abandon differential pricing based on personal data—with the resulting costs falling on borrowers with good credit histories or drivers with clean records. See generally Richard A. Posner, An Economic Theory of Privacy, in Philosophical Dimensions of Privacy 333 (Ferdinand David Schoeman ed., 1984) (arguing that value of "prying," for both commercial and personal reasons, should be weighed against value of privacy in economic analysis); Richard A. Posner, John A. Sibley Lecture: The Right of Privacy, 12 Ga. L. Rev. 393 (1978) (same);

Thus, any proposal for protection of data privacy must balance that goal against strong competing interests: individual surfers' autonomy, First Amendment constraints, and the externalized costs of privacy.

II
CODE: HOW P3P WORKS

Because technology has exacerbated the data privacy problem, it is understandable to hope that technology also might solve the problem. A number of authors have discussed (and entrepreneurs have sold) "privacy-enhancing technologies" (PETs) that use code to protect privacy.[78] While many are effective in limited circumstances,[79] P3P is the only PET[80] that enhances data privacy regardless

Singleton, supra note 72, at 8-10 (noting benefits of access to personal data, including availability of credit).

[78] See generally Herbert Burkert, Privacy-Enhancing Technologies: Typology, Critique, Vision, in Technology and Privacy: The New Landscape 125 (Philip E. Agre & Marc Rotenberg eds., 1997) (defining and categorizing privacy enhancing technologies (PETs) and their implementations); Rotenberg, supra note 9, ¶¶ 62-67 (reviewing concept of PETs and arguing that definition should include only technologies that inherently limit collection of personal data).

[79] Some PETs allow anonymous or pseudonymous surfing. See, e.g., Anonymizer, at http://www.anonymizer.com (last visited Aug. 24, 2001) (permitting surfer to visit sites through proxy server that strips all identifiers); see also Rotenberg, supra note 9, ¶¶ 51-58 (discussing virtues of anonymity and encryption for privacy protection). These PETs eliminate the transfer of personal data but require an all-or-nothing choice by surfers rather than allowing them to provide personal data where revealing it is necessary or desirable. See supra notes 60-65 and accompanying text (discussing circumstances where surfers may wish to divulge personal data). Other PETs respond to specific privacy threats by thwarting the code behind them. See, e.g., Guidescope, at http://www.guidescope.com (last visited Aug. 24, 2001) (blocking placement of third-party advertisement and, therefore, advertisers' monitoring through cookies or bugs); IDCide Privacy Companion, at http://www.idcide.com (last visited Aug. 24, 2001) (allowing surfer to block placement of all cookies or only those transmitted by third parties). Their utility is limited to the particular privacy-invading techniques in question, however, and they are superceded whenever data collectors come up with new methods or technology. See supra note 44 (discussing innovative data-collecting techniques). Of course, both these and other PETs can serve as useful complements to the legal framework proposed later in this Note. See infra Part IV; cf. Harvard Developments, supra note 5, at 1646 n.70 (suggesting use of P3P "in conjunction with anonymizing and cookie-blocking technologies").

[80] Because Rotenberg defines a PET as technology that inherently reduces transfer of personal data, he objects that P3P is not a PET. Rotenberg, supra note 9, ¶ 67. The following discussion will demonstrate that P3P is a technology which increases data privacy, as defined in note 19, supra. At a minimum, "[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); see also Mulligan et al., supra note 5 (supporting P3P as technological tool that improves privacy).

of where surfers venture on the Web or how sites gather personal data.[81]

The P3P Specification is awaiting final approval by the World Wide Web Consortium (W3C), the independent international standard-setting body for the Web.[82] The W3C's volunteer working groups promulgate new standards through an elaborate, consensus-based development process.[83]

P3P represents no real technological breakthrough; it uses basic principles of computer science and a popular Web programming language.[84] More specifically, the P3P protocol establishes a standard computerized vocabulary to define both the types of data that Web site operators might collect and the ways they might use it. It then prescribes a sophisticated set of rules to guide the interaction of independently designed software using that vocabulary. P3P's "code" thus reads more like a statute than software.[85] This Part discusses the vocabulary and the rules in turn.

[81] In the future, perhaps another protocol might supplant P3P as an interoperability standard for evaluating privacy policies through intelligent agents. The focus here on P3P does not suggest that no other such technology could exist, but that P3P is currently the only one.

[82] For more information about the W3C and its membership, see World Wide Web Consortium, W3C Process Document (July 19, 2001), §§ 1-2, at http://www.w3.org/Consortium/Process-20010719 (describing W3C organization and membership); see also Reidenberg, supra note 14, at 591 & n.205 (noting W3C as example of effective nongovernmental rulemaker for cyberspace).

[83] See World Wide Web Consortium, supra note 82, § 6 (describing W3C's formal approval process). Membership of the P3P working groups was dominated by industry, but also included some representatives of academia, government privacy regulators, and privacy advocacy groups. The final P3P working group, which wrote the specification, was chaired by Lorrie Cranor of AT&T Labs; of the thirty-five official members of this group, at least twenty-two represented companies. See P3P Specification, supra note 3, app. 8 (listing members of P3P Specification Working Group as well as previous working groups that assisted in development of protocol). While some privacy groups, notably the Center for Democracy and Technology, participated in P3P's development, see Mulligan et al., supra note 5, others have opposed the protocol strenuously. See David McGuire, Privacy Supporters Clash Over P3P, Newsbytes, July 20, 2001, at http://www.newsbytes.com (describing how P3P "remains a source of debate within the privacy community").

[84] The language is XML, or Extensible Markup Language, itself a W3C standard. See Extensible Markup Language (XML) 1.0 (Tim Bray et al. eds., 2d ed.), W3C Recommendation (Oct. 6, 2000), at http://www.w3.org/TR/2000/REC-xml-20001006 (setting XML standards).

[85] Thus, the P3P Specification is a particularly good demonstration of Lawrence Lessig's aphorism that "[c]ode is law." Lessig, supra note 12, at 5-6, 53 (comparing computer code, or "West Coast code," to legal code, or "East Coast code," as different modalities for regulation of behavior in cyberspace); cf. Rotenberg, supra note 9, at n.1 (predicting with some acidity that "law school bookstores will soon offer bumper stickers and T-shirts with the now famous slogan").

A. *The P3P Vocabulary*

The P3P vocabulary encompasses all the personal data that typically would be gathered on the Web. A Web site operator uses this vocabulary to encode a "P3P policy"[86]—a machine-readable version of the site's human-readable privacy policy[87]—which is posted on the site for a surfer's computer to retrieve and parse.[88] Individual pieces of data, such as a first name, a birth date, or a telephone number, are called data elements.[89] P3P organizes these data elements into several overlapping groupings: data sets,[90] data structures,[91] and data categories.[92] These interwoven classifications permit a small number of defined terms to express complex relationships by using numerous cross-references.[93]

The P3P protocol defines many typical data elements and assigns them to appropriate groupings where possible.[94] Web sites can sup-

[86] A Web site's P3P policy is the XML-encoded version of a privacy policy—a file that represents the practices of the Web site operator concerning treatment of personal data. P3P Specification, supra note 3, § 1.1.3 (introducing concept of P3P policy).

[87] The term "human-readable" distinguishes a traditional privacy policy expressed in natural language from a machine-readable P3P policy encoded in XML. See id. § 1.1.5 (referring to translation of "human-readable privacy policies into P3P syntax").

[88] See infra notes 106-19 and accompanying text (explaining user agent software employed by surfer).

[89] P3P Specification, supra note 3, § 1.3 (defining "data element" as "[a]n individual data entity, such as last name or telephone number"); see also id. § 5 (describing use of data elements in P3P policy); id. § 5.6, app. 3 (defining numerous specific data elements).

[90] A data set is simply a collection of data elements with common characteristics. Id. § 1.3. For instance, the user data set includes elements representing an individual's name, date of birth, gender, and mailing address. Id. § 5.6.1.

[91] Data structures establish hierarchical relationships between elements, sets, or other structures. Id. § 1.3. For example, the contact structure includes the structures "postal" (for mailing address), "telecom" (for phone numbers), and "online" (for e-mail and Web page addresses). Id. § 5.5.6.

[92] Data categories broadly describe types of personal data based on their characteristics or functions. Id. § 3.4. The sixteen specified data categories include <computer/> for information about the surfer's computer, such as IP address or operating system; <demographic/> for data such as gender or income; and <preference/> for information about individual likes and dislikes, such as favorite colors or musical tastes. Id. The same data might fall into more than one category, depending on context: The elements referring to dates might refer to a credit card expiration, placing it in the <purchase/> category, or to a date of birth, placing it in the <demographic/> category. In these cases, a site's P3P policy must indicate which categories apply to the site operator's particular uses of personal data. See id. § 5.7.2.

[93] See id. § 5. As one example of this modular language, the "telecom" structure, see supra note 91, includes elements for telephone, fax, cell phone, and pager numbers. Id. § 5.5.6.2. Each of these, in turn, adopts the structure "telephonenum," which is broken into elements such as area code, telephone number, and extension. Id. § 5.5.5.

[94] See id. § 5.5 (describing basic data structures); id. app. 3 (giving formal XML definition of P3P Base Data Schema).

plement this lexicon by posting their own additional definitions,[95] although they are barred from changing P3P-defined terms or reassigning their predetermined data categories.[96]

In addition to defining individual pieces of data, P3P also standardizes the nomenclature for a Web site operator's data-handling practices. The protocol requires that a P3P policy specify every item of personal data collected from visitors to the site.[97] For each one,[98] the policy must identify the purpose of collection[99] and all recipients of the collected data beyond the Web site operator,[100] among other mandatory disclosures.[101] In addition, the policy may spell out whether an individual can elect to withhold personal data in particular circumstances.[102] As with the vocabulary for data, Web site operators

[95] See id. § 5; see also id. § 3.5 (describing extension mechanism). The Web site's additional definitions, or "data schemas," are incorporated in the site's P3P policy. Any change in a site's data schema requires the posting of a new P3P policy. See id. § 5.4; see also id. § 1.3 (defining term "data schema").

[96] Id. § 5.7.1 (prohibiting P3P policies from overriding classification of fixed-category data elements or data structures). User agents, see infra note 106 and accompanying text, are required to ignore such interference with established category classifications. Id.

[97] Id. § 1.1.5 ("A P3P policy MUST cover all data generated or exchanged as part of a site's HTTP interactions with visitors.").

[98] Data elements may be grouped together and the groups associated with the same explanatory statement, but the policy will then be read inclusively—as stating that any of the actions in the statement could be taken with any of the associated data elements. See id. § 3.3.1.

[99] Id. § 3.3.4 (listing values for <PURPOSE> element). The twelve identified purposes for collecting personal data range from <current/>, indicating that the data are used to support only the current activity (such as placing an e-commerce order) to <telemarketing/ >, indicating that the data could be used to make sales-oriented telephone calls. Id.

[100] Id. § 3.3.5 (listing values for <RECIPIENT> element). This element distinguishes, for example, between third parties that act as the Web site operators' agents and those that do not. Id.

[101] Mandatory elements must be present in every P3P policy. See id. § 3.2.2 (listing required elements of complete P3P policy). In addition to requirements discussed in text, a P3P policy also must: link to a human-readable version of the site's privacy policy, id. (requiring that P3P policy include link to "natural language privacy statement"); provide the identity and contact information of the Web site operator, id. § 3.2.4 (defining <ENTITY> element); disclose whether the Web site operator allows individuals access to their stored personal data (it can allow access to <all/>, <none/>, or several gradations between the two), id. § 3.2.5 (defining <ACCESS> element); and state a policy for retaining personal data, which may differ depending on the data element (practices range from <no-retention/> to <indefinitely/>), id. § 3.3.6 (listing values for <RETENTION> element).

[102] Unlike the others, inclusion of this element is optional. A Web site operator could require a surfer's affirmative consent for a particular data-handling practice (an opt-in), or allow the surfer to block that practice on request (an opt-out), or offer the surfer no choice in the matter. See id. §§ 3.3.4, 3.3.5. These alternatives can be tied to particular purposes or recipients. For example, a P3P policy might require that the surfer allow collection of a mailing address, but allow the surfer to opt out of providing that data to third parties and require an opt-in before it can be used to send marketing solicitations. See id. If individuals have an opportunity to opt out or opt in, a P3P policy must provide a link to a clear explanation of the procedure to be followed. Id. § 3.3.4. A P3P policy may also offer

may customize their policies further to describe practices that do not fit into the existing terminology.[103]

Thus, the P3P vocabulary creates a comprehensive, standardized, machine-readable language to describe both personal data and data-handling practices, yet offers flexibility for Web site operators to add new terminology.

B. *P3P in Operation*

Because this standardized vocabulary is rendered in computer code, people will need software to use it. To ensure that independently designed software functions properly, the P3P protocol establishes interoperability rules telling the different programs how to interact with one another.

The first challenge is to help Web site operators convert their human-readable privacy policies into P3P-compliant code. They can do so themselves if they have moderate programming capabilities, or they can use automated translation software called a policy generator, which asks a series of questions about privacy practices to create a P3P policy.[104] The promoters of one policy generator claim that a Web site operator using their product can complete a P3P policy in ten minutes.[105]

Similarly, surfers rely on software, called a "user agent," to encode their data privacy requirements.[106] Different user agents would implement P3P in dramatically different ways, but they all share some attributes. First, a surfer instructs the user agent about his or her privacy preferences—what types of personal data the surfer will divulge to what entities and for what purposes. Once established, these pref-

reasons for a particular practice, presumably aimed at persuading the individual to consent. See id. § 3.3.2 (explaining <CONSEQUENCE> element).

[103] See id. § 3.5 (describing extension mechanism for adding new descriptions of practices).

[104] IBM and Privacybot.com are developing policy generators. See Martin Pressler-Marshall et al., P3P Policy Editor, at http://www.alphaworks.ibm.com/tech/p3peditor (updated July 18, 2001); PrivacyBot Privacy Policy Generator, at http://www.privacybot.com (last visited Aug. 23, 2001). Microsoft also intends to develop a policy generator. See Wallent Testimony, supra note 52, at 24 (stating that Microsoft was developing P3P-compliant "Privacy Statement Wizard" to be posted at http://privacy.bcentral.com). A Web site operator who uses a policy generator might never even see the machine-readable code that represents a P3P policy.

[105] PrivacyBot FAQ, at http://www.privacybot.com/about.shtm (last visited Aug. 23, 2001).

[106] See P3P Specification, supra note 3, § 1.3 (defining "user agent" as "a program whose purpose is to mediate interactions with services on behalf of the user"). A user agent is a type of intelligent agent—sometimes also called a smart agent or "bot"—which is programmed to perform actions on the user's behalf. See Netanel, supra note 25, at 451 (defining smart agent).

erences are retained as a set of standing orders for the user agent, although a surfer could change preferences at any time or, presumably, override them in a particular instance. Whenever a surfer with a P3P user agent visits a site with a P3P policy, the user agent quickly retrieves the policy first.[107] When there is a discrepancy, the user agent notifies its owner, perhaps using prompts such as icons or dialog boxes,[108] and may prevent the page from loading. If, however, the policy complies with the surfer's previously specified preferences, then surfing is not disrupted and the page loads. The computerized evaluation of the P3P policy would be invisible to the surfer.[109]

Microsoft has included a modest P3P user agent in the latest version of its browser, Internet Explorer 6.0 (IE 6.0), which is part of the company's new operating system, Windows XP.[110] This user agent's implementation of P3P is limited in several crucial respects: For example, it merely examines the placement of cookies, rather than all

[107] The mechanics of retrieval are outlined in P3P Specification, supra note 3, § 2.2. The process is designed to prevent the dissemination of personal data, such as details about the user's computer system or IP address, that could be divulged in the process of fetching the policy. Id. § 2.4.3 (defining safe zone practices). Keeping these initial interactions anonymous allays concerns that an individual's privacy preferences themselves constitute valuable personal data. See Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 Wis. L. Rev. 743, 768-69 (2000) (describing P3P's possible creation of "privacy meta-data" about individual surfer's privacy preferences). If Web pages have content from multiple sources, the policy for the hosting Web site operator may state whether its terms apply to those other sources. See P3P Specification, supra note 3, § 2.3.2.5 (defining <INCLUDE> and <EXCLUDE> elements). A policy similarly can state whether it applies to cookies. Id. § 2.3.2.7. If the policy does not cover the other sources, the user agent should request separate P3P policies from each one. These provisions may not adequately cover the interactions between the surfer and third-party data collectors. See infra text accompanying note 207 (suggesting legal response to this problem).

[108] See P3P Specification, supra note 3, § 1.1.4 (suggesting that user agent can "display symbols, play sounds, or generate user prompts that reflect a site's P3P privacy practices" relative to surfer's preferences). User agents could issue similar warnings if a site had no P3P policy.

[109] Several performance optimizations in the P3P Specification help to speed the process of fetching and parsing policies to avoid disrupting browsing. See, e.g., P3P Specification, supra note 3, § 2.1 (describing policy reference files). This seamless navigation is an important feature of P3P user agents. See Wallent Testimony, supra note 52, at 22 (arguing that privacy technology "needs to work in a way that provides the protection consumers want, but without disrupting or slowing their web browsing experience").

[110] See Aaron Goldfeder & Lisa Leibfried, Microsoft Corp., Privacy in Internet Explorer 6, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpriv/html/ie6privacyfeature.asp (updated Oct. 16, 2001) (describing privacy features of Internet Explorer 6.0 (IE 6.0)). A different feature of Windows XP that has drawn fire from privacy advocates is Passport, an electronic wallet that stores personal data and allows the surfer to fill in forms automatically. See Steve Lohr, Privacy Group Is Taking Issue With Microsoft, N.Y. Times, July 25, 2001, at C1 (reporting that Electronic Privacy Information Center planned to file complaint with Federal Trade Commission about Passport).

collection of personal data,[111] and it employs condensed versions of P3P policies called compact policies which forgo the richness of the entire P3P vocabulary.[112] Nonetheless, IE 6.0 gives surfers the opportunity to set preferences and use them to evaluate Web site privacy policies automatically. A surfer selects one of six preconfigured preference sets, or uses the "medium" default setting.[113] There are also some "advanced" options, which allow further customization.[114] The response when a compact policy does not comply with these preferences depends on the level of privacy selected and on whether the cookie is placed by a third party rather than the operator of the main page the surfer visits. IE 6.0 may block the cookie, delete it when the surfer leaves the site, or limit its later retrieval.[115]

Microsoft's dominance of the browser market has not prevented other companies from developing more ambitious user agents that operate separately from the browser.[116] Sophisticated user agents would ask the surfer a series of questions to yield a more elaborate set of privacy preferences, using the P3P vocabulary to link particular types

[111] Goldfeder & Leibfried, supra note 110 (describing focus of IE 6.0 privacy features as "advanced cookie filtering").

[112] See P3P Specification, supra note 3, § 4 (explaining compact policies, which are included in protocol because they take up less space and load more quickly); Goldfeder & Leibfried, supra note 110 (describing use of compact policies in Microsoft user agent and noting that "Internet Explorer 6 does not make use of full P3P policies"). Furthermore, IE 6.0 evaluates only a few of the data categories in the P3P vocabulary: those covering location (either mailing addresses or e-mail addresses), government identification numbers (such as social security numbers), and financial data. Id. The company considers these categories the most sensitive personal data. Aaron Goldfeder, Microsoft Corp., Internet Explorer 6 Privacy Features, Online Presentation, at http://www.microsoft.com/winme/01mitt/01may/15364/features/default.htm (June 11, 2001) (describing rationale for limiting recognized categories to those containing what Microsoft considers "personally identifiable information"). But see supra note 6 (offering broader definition of personal data).

[113] Goldfeder & Leibfried, supra note 110 (describing six preset levels in detail). The medium setting is installed "out of the box" without the surfer taking any action. It allows cookies to be placed as long as the surfer is offered an opt-out. Id.; see also Walker, supra note 5 (reporting that privacy advocates have objected that IE 6.0 default setting is inadequate).

[114] See Rob Franco, Microsoft Corp., Internet Explorer 6 Privacy User Experience, Online Presentation, at http://www.microsoft.com/winme/01mitt/01may/15364/Experience/default.htm (last visited Aug. 23, 2001) (noting surfer's ability to set site-by-site preferences, to request prompts in certain circumstances, and to gain access easily to site's full policy); Goldfeder & Leibfried, supra note 110 (describing advanced settings).

[115] Goldfeder & Leibfried, supra note 110.

[116] One company has designed a user agent that works as a browser extension. See IDCide Privacy Companion, at http://www.idcide.com (last visited Aug. 24, 2001). Several programs were demonstrated at a W3C-sponsored interoperability session in New York City on June 21, 2000. See 21 June 2000 Platform for Privacy Preferences (P3P) Project Interop Report, at http://www.w3.org/P3P/P3P-interop-report-20000621.html (last visited Aug. 24, 2001); see also P3P Specification, supra note 3, § 1.1.4 (noting that user agent could be built as Java applet or run from proxy server, among other potential applications).

of data[117] with particular data-handling practices the surfer considers permissible.[118] In addition, P3P allows independent persons or organizations to write model sets of preferences for surfers to import into their user agents.[119]

Implemented in full, P3P would allow user agents to elicit highly nuanced sets of preferences. For example, you might place no restrictions on data about your computer's technical capabilities, but allow disclosure of your mailing address only for the purpose of having purchases shipped to you, and refuse altogether to reveal other demographic information. You could divulge financial information in order to complete transactions, but not if the Web site operator plans to retain it afterwards. You might permit monitoring of your clickstream for one-time automated tailoring of a dynamic site, but not to build a permanent dossier of your personal tastes. The P3P vocabulary easily can express all of the conditions in this paragraph as one comprehensive preference set.[120]

Using P3P as a tool, surfers fully can understand how particular Web sites collect and handle personal data. They can then decide for themselves whether they would rather avoid a site with policies they find inadequate. Even the IE 6.0 user agent increases surfers' control, thereby improving their data privacy somewhat. As Part III will explain, this power becomes more significant when combined with the market modality.

[117] Data categories, supra note 92, are especially important for this exercise, because the surfer does not need to instruct the user agent about every possible data element in order to establish comprehensive preferences. For example, a preference applied to the <demographic/> category would cover age and gender without any more specific preference applying to either. See generally P3P Specification, supra note 3, § 3.4 (explaining that data categories "allow users to express more generalized preferences and rules").

[118] Surfers might be willing to part with the same personal data for some purposes but not for others. One survey found that ninety percent of consumers would divulge an e-mail address in exchange for personalized content, but the figure dropped to eighteen percent if the e-mail address would be shared with third parties, thus raising the risk of unsolicited marketing e-mails. Gardyn, supra note 63, at 54.

[119] See P3P Specification, supra note 3, § 3.6 (requiring that user agents allow importation of privacy preferences). IE 6.0 also allows surfers to import preference sets, although these imported sets remain limited in the same ways as the preconfigured preference sets, such as using only compact policies. See supra notes 110-13 and accompanying text (discussing limitations of Microsoft user agent). The W3C is also working on a supplemental language for these model preference sets called A P3P Preference Exchange Language (APPEL). See Lorrie Cranor, et al., World Wide Web Consortium, A P3P Preference Exchange Language 1.0 (APPEL 1.0), W3C Working Draft (Feb. 26, 2001), at http://www.w3.org/TR/P3P-preferences.html. At present, the P3P protocol does not require that user agents be compatible with APPEL.

[120] See supra Part II.A (describing P3P vocabulary).

III
THE MARKET: THE LIBERTARIAN P3P PRIVACY MARKET

Some of P3P's promoters suggest that its code establishes a market structure for disclosure of personal data, which protects privacy. Enthusiasts consider this market so effective that it minimizes or eliminates the need for significant legal intervention.[121] This Part first describes the notion of a "P3P privacy market" and its advantages, and then turns to the shortcomings of this libertarian vision. It concludes that the modalities of code and market alone are not enough to protect privacy effectively without active intervention by the law.

A. *The Case for a P3P Privacy Market*

Many commentators have proposed, in the abstract, that we consider control over personal data a transferable property right.[122] If the exchange of personal data is so lucrative, this argument runs, then let its collectors pay for it—if not with money, then with other benefits.[123] If the offers are not attractive enough, individuals can withhold data about themselves; that is, they can exercise their right to exclude others from their property and refuse to sell. Thus, its proponents argue, ownership confers control over personal data, creating both an efficient market for personal data and a safeguard for privacy.[124]

Although academically interesting, the notion of a personal data bazaar faces obvious practical obstacles such as the unavailability of market information and the high transaction costs of individual negotiations. While schemes to overcome these obstacles have been envi-

[121] See supra note 5 and accompanying text.

[122] See, e.g., Anne Wells Branscomb, Who Owns Information?: From Privacy to Public Access 180-81 (1994) (listing benefits of treating personal data as property); Bartow, supra note 44, at 687-99 (analogizing property right in personal data to copyrights, trademarks, and publicity rights); Kenneth C. Laudon, Markets and Privacy, 39 Comm. Ass'n for Computing Machinery 92 (1996) (proposing elaborate trading system for property rights in personal data); Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Geo. L.J. 2381 (1996) (arguing that economic value of privacy should not be overlooked in law-and-economics analysis of privacy rules). The basic idea is not new. For example, Alan Westin, in his landmark 1967 book, envisioned treating private information as property in order to protect individuals against unwarranted government intrusion. Westin, supra note 19, at 324; see also Chlapowski, supra note 34, at 158-59 (tracing treatment of data privacy as property right to John Locke's notion of "self-ownership").

[123] See generally supra notes 60-65 and accompanying text (listing benefits surfers might receive in exchange for divulging personal data).

[124] See supra note 19 (defining data privacy as based in control over personal data).

sioned,[125] the advent of P3P makes the propertization of privacy a realistic option as never before.[126]

According to supporters of this libertarian approach, in a P3P privacy market surfers could own their personal data and use P3P to negotiate with those who wish to collect it.[127] A lively personal data marketplace would spring up in response, with little or no legal intervention.[128] The most laissez-faire flavor of this proposal builds on Calabresi and Melamed's idea of property rules[129] to suggest that the mere existence of P3P creates an entitlement to personal data equivalent to ownership rights.[130] Another analysis suggests that law might declare the existence and enforceability of the property right but otherwise play little role.[131]

P3P allows the privacy market to function by reducing the transaction costs of providing extensive details about a site's privacy pol-

[125] See, e.g., Laudon, supra note 122, at 99-101 (proposing intricate "National Information Market" to enable buying and selling "baskets" of personal data).

[126] See Lessig, supra note 12, at 160 ("What is needed is a way for the machine to negotiate our privacy concerns for us . . . ."); Harvard Developments, supra note 5, at 1645-48 (concluding that P3P and market solve data privacy problems); Kang, supra note 6, at 1258-59 & n.272 (discussing possible automation of market negotiation over privacy, and mentioning early version of P3P).

[127] See Lessig, supra note 12, at 159-63 (proposing P3P-enhanced property regime); Harvard Developments, supra note 5, at 1645-48 (same); see also supra note 5 and accompanying text (citing P3P supporters who envision P3P enabling market for privacy).

[128] In Lessig's terms, this model regulates largely through the modalities of code and market, rather than law (or norms). See supra note 12 and accompanying text (listing modalities); see also supra note 5 and accompanying text (citing supporters of P3P who believe role of law in protecting privacy could be limited or nil). It is notable that Lessig, who otherwise persistently emphasizes the mixture of modalities regulating cyberspace, see supra notes 12-14 and accompanying text, sometimes downplays the importance of law in connection with his P3P-property proposal for privacy. See Netanel, supra note 25, at 484 ("At least with regard to P3P, however, [Lessig] seems to rely too heavily on the deployment of the right kind of code [and resulting market forces] as a means to guarantee individual liberty."); Steven Hetcher, Climbing the Walls of Your Electronic Cage, 98 Mich. L. Rev. 1916, 1931-32 (2000) (reviewing Lessig, supra note 12) (arguing that Lessig fails to prove that code, as opposed to "traditional methods of regulation," "is the most important regulator of cyberspace"); Rotenberg, supra note 9, ¶¶ 33-38 (attacking Lessig for ignoring legal tradition in formulating privacy protection proposal); see also infra note 151 (citing Lessig speech extolling market). But see Lessig, supra note 12, at 160 (conceding that P3P "will not emerge on its own. It needs the push of law"); Lessig, supra note 16 (noting that market solutions require some support from both code and law).

[129] See generally Guido Calabresi and A. Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 Harv. L. Rev. 1089 (1972).

[130] Harvard Developments, supra note 5, at 1645-48 (declaring that "P3P establishes a technologically—as opposed to a legally—protected property right in personal information" and that this "P3P regime will result in the optimal level of privacy protection").

[131] Lessig, supra note 12, at 160 (proposing that lawmakers create property right in personal data, establishing P3P privacy market).

icy.[132] A P3P policy is an explicit,[133] comprehensive,[134] and unambiguous[135] statement of the Web site operator's data-handling practices. A surfer, as a market actor, needs this information to negotiate for privacy. A surfer then can accept the terms of a P3P policy, either by setting compatible privacy preferences in advance or by overriding them in order to visit a particular site after being informed of its policy by a user agent.[136]

The P3P privacy market offers noteworthy advantages for a privacy-protection regime. First, by arming surfers with the capacity to compare privacy policies easily, the P3P privacy market forces Web sites to compete with one another to offer more attractive privacy policies.[137] Sites offering less privacy than surfers demand would need to compensate by providing other benefits. Alternatively, a site could offer strong privacy protection in order to attract more visitors, or visitors who value privacy enough that they are willing to pay a premium

[132] Id. at 160-61 (contrasting use of P3P with "wildly high" transaction costs of reading Web sites' privacy policies, because "[n]o one has the time or patience to read through cumbersome documents describing obscure rules for controlling data"); Harvard Developments, supra note 5, at 1647 (praising P3P for reducing transaction costs in market negotiations over privacy). But see Litman, supra note 9, at 1297-98 (protesting that lack of proprivacy incentives, not transaction costs, is relevant obstacle to privacy market).

[133] The process for retrieving a P3P policy, see supra note 107, ensures that data-handling practices are announced outright. Many disclosures are mandatory. Supra notes 99-101 and accompanying text (listing disclosures required by P3P protocol).

[134] P3P Specification, supra note 3, § 1.1.3 (requiring that "P3P policies must cover all relevant data elements and practices"); id. § 1.1.5 ("A P3P policy MUST cover all data generated or exchanged as part of a site's HTTP interactions with visitors."). But see supra note 107 (noting that site's P3P policy may omit third-party data collection).

[135] P3P Specification, supra note 3, § 2.4.1 (requiring that only one policy apply to each piece of data at any given time and establishing which applies if multiple policies are posted). More generally, the protocol's very specific definitions of terms greatly reduce ambiguity. See, e.g., id. §§ 5.5-5.6, app. 3 (defining different data groupings). Only in the unforeseen situations where this substantial vocabulary is insufficient would Web site operators extend it. See supra notes 95, 103, and accompanying text (describing extension mechanisms in P3P vocabulary).

[136] See supra note 108 and accompanying text (discussing means for user agent to inform surfer of discrepancies). A more sophisticated "virtual bargaining" feature was dropped from the protocol during development, but may be added to future versions; it would allow more complex negotiations about privacy practices, such as a series of automated offers and counteroffers. See P3P Specification, supra note 3, § 1.1.6 (listing eliminated features, including features "to allow sites to offer a choice of P3P policies to visitors" and "to allow visitors (through their user agents) to explicitly agree to a P3P policy").

[137] See Harvard Developments, supra note 5, at 1647 (predicting "intense competition" between Web sites to offer attractive P3P policies and "a high level of site responsiveness to user preferences").

for access or services.[138] The P3P privacy market requires data collectors to pay a price for access to personal data and internalize the cost to surfers of sacrificing privacy. It transforms privacy into a valuable commodity on the Web.

Even more important, the P3P privacy market responds to each surfer's choices about privacy. Respect for autonomy requires not only the freedom to keep personal data private,[139] but also the freedom to disclose it, motivated by any of a wide range of personal considerations.[140] The definition of a truly autonomous choice, to be sure, is a normative issue that is open to debate.[141] But lawmakers must afford surfers some level of autonomy, however defined.

For these reasons, even staunch critics of "commodifying" privacy[142] usually do not go as far as proposing inalienable data privacy rights in place of transferable market-oriented rights.[143] Indeed, the

[138] See Steven M. Zeitchik, Pitching Privacy, Net Persuasion Newsletter, June 6, 2001, at http://www.thestandard.com/article/0,1902,26955,00.html (describing new trend of companies marketing enhanced privacy policies to consumers).

[139] See supra notes 20-26 and accompanying text (describing dignity and autonomy interests in data privacy).

[140] See Hetcher, supra note 128, at 1932-34 (criticizing idea that "people who choose to [disclose personal data] are somehow less free than those who choose not to"); see also supra notes 60-64 and accompanying text (listing benefits surfers might receive in exchange for divulging personal data).

[141] Some scholars, recognizing that individuals make choices bound by a context that limits their actual freedom, advocate a richer understanding of autonomy which inquires into the extent of constraint on a decision before considering it sufficiently independent. See Yochai Benkler, Siren Songs and Amish Children: Autonomy, Information, and Law, 76 N.Y.U. L. Rev. 23, 32-41 (2001) (advancing "thicker" definition of autonomy as decisionmaking capacity bounded by individual's context and circumstances); Schwartz, supra note 11, at 821-34 (criticizing control-based definitions of data privacy, see supra note 19 and accompanying text, for failure to recognize limits on self-determination). The regime proposed in this Note accommodates a wide range of possible normative decisions by lawmakers about the required level of autonomous choice and the safeguards necessary to guarantee it. See infra Part IV.B.

[142] E.g., Simon G. Davies, Re-Engineering the Right to Privacy: How Privacy Has Been Transformed From a Right to a Commodity, in Agre & Rotenberg, supra note 78, at 143, 161 (declaring such "commodification" to be "inimical to privacy"); Open Letter from Jason Catlett, President of Junkbusters Corp., to Members of the P3P Working Group (Sept. 13, 1999), available at http://www.junkbusters.com/ht/en/standards.html ("[P]rivacy is a fundamental human right that should be universally expected.... [P3P] promotes the view that personal information is a secondary currency or commodity to be bartered...."); see also Lessig, supra note 12, at 161 ("There are those, especially on the left, who are radically skeptical about a property regime to protect privacy. Property is said to commodify, to marketize, to monetize....").

[143] See generally Calabresi & Melamed, supra note 129, at 1111-15 (discussing inalienable entitlements); Kang, supra note 6, at 1266 (considering and rejecting inalienability rule for data privacy); cf. Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960) (barring disclaimer of implied warranty of merchantability); Hilder v. St. Peter, 478 A.2d 202 (Vt. 1984) (holding that tenant cannot waive rights available under warranty of habitability). Such inalienability proposals have been attributed to privacy advocates, see Lessig,

strongest privacy rules in existence allow individuals to waive their privacy rights.[144] So long as surfers have the option to disclose personal data—as they must—their decisions to do so will be governed by the market modality.

Thus, skeptics of the libertarian approach ought to accept the P3P privacy market and concentrate on augmenting it, not replacing it. For example, they might wish to install safeguards to ensure that surfers' decisions to reveal personal data meet a high standard for informed and autonomous choice, and then give weight to preferences that satisfy this strict test.[145] There are huge differences between such a stringent baseline and weak industry self-regulatory standards,[146] but they are differences of degree, not kind.

This Note follows suit, turning next to an analysis of the problems with a libertarian market for deploying P3P,[147] and then to legal means for fixing them.[148]

supra note 12, at 161 (claiming that some privacy advocates, including Marc Rotenberg, "view privacy as a kind of inalienable right," the sale of which should be "criminalized"), but it is inaccurate to suggest that they generally have embraced such proposals, see Rotenberg, supra note 9, at n.60 (refuting Lessig's characterization). But cf. Anita L. Allen, Coercing Privacy, 40 Wm. & Mary L. Rev. 723 (1999) (suggesting that liberal democracy requires government to "impos[e] privacy norms" on individuals).

[144] E.g., Children's Online Privacy Protection Act, 15 U.S.C.S. § 6502(b)(1)(A)(ii) (LEXIS 2001) (lifting ban on "collection, use, or disclosure" of children's personal data upon receipt of "verifiable parental consent"); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164) (setting high but largely waivable default rule for data privacy); Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (same). A frequently cited set of model "Fair Information Practices" also includes consent as a core principle along with notice, security, and access. These principles are most authoritatively embodied in a set of guidelines promulgated by the Organization for Economic Cooperation and Development (OECD). See OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980), available at http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.htm (last visited Aug. 26, 2001). For an overview of the content and evolution of the Fair Information Practices, see Regan, supra note 31, at 71-77; Rotenberg, supra note 9, ¶¶ 36-50.

[145] See Schwartz, supra note 11, at 834, 856 (calling individual choices to divulge information consistent with "constitutive" view of data privacy, provided state has acted to increase individuals' ability to secure their preferences and bargain around objectionable policies).

[146] Voluntary "seals of approval" from organizations such as TRUSTe and BBBOnLine impose light restrictions on Web site operators, enforced even more lightly. See Netanel, supra note 49, at 477-78 (discussing flaws in trustmarks, including need for surfers to ascertain which marks are reliable); Reidenberg, supra note 40, at 777-78 (outlining enforcement shortcomings of TRUSTe and BBBOnLine).

[147] See infra Part III.B.

[148] See infra Part IV.

B. Problems With a Libertarian Privacy Market

The antiregulatory libertarian approach described in Section III.A, despite its benefits, suffers from doctrinal and practical limitations. These are serious enough that lawmakers cannot abdicate the protection of data privacy to an extralegal privacy market if they wish to strike a balance between the competing goals for the Web discussed in Part I.

Proposals for a privacy market, including those that incorporate P3P, generally analyze it from the same doctrinal starting point: creating property rights for personal data.[149] Property and markets tend to go together, of course, but observers also might gravitate toward this property rationale for a variety of other reasons. First, the law increasingly protects other rights to information through propertization,[150] and the political success of this strategy might encourage data privacy supporters to imitate it.[151] Furthermore, the fact that businesses gather personal data for free and resell it for profit may suggest that it has monetary value which has been misappropriated from individuals.[152]

However, conflicts between the objectives of data privacy and some core tenets of property doctrine undermine this rationale. At the broadest level, the trend of converting information into property is itself deeply troubling, because the removal of information from the public domain impoverishes discourse.[153] There are particular justifications for doing so in areas such as copyright[154] or trademark,[155] but

[149] See supra notes 122-26 and accompanying text (describing and citing property-centered proposals for privacy market).

[150] See Diane Leenheer Zimmerman, Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights, 33 Wm. & Mary L. Rev. 665, 674-724 (1992) (tracing increase in propertization of information from eighteenth century to present).

[151] Lawrence Lessig, Presentation at Social Research Conference on Privacy at New School University (Oct. 6, 2000) (notes on file with the *New York University Law Review*) (suggesting that propertization trend taps political sentiment that might benefit advocates of data privacy protection). Contra Mark A. Lemley, Private Property: A Comment on Professor Samuelson's Contribution, 52 Stan. L. Rev. 1545, 1547 (2000) (arguing that property right in personal data is "politically unsaleable").

[152] See Bartow, supra note 44, at 683-90 (arguing, somewhat mischievously, that "[i]f the rigid commodification of information is indeed inevitable, perhaps it is time for individuals to appropriate the intellectual property framework so eagerly constructed by corporate interests" through creation of property right in personal data).

[153] See Benkler, supra note 141, at 84-88 (arguing that progressive "enclosure" of public domain through propertization unduly restricts access to information "commons"); Zimmerman, supra note 150, at 739-40 (comparing incursions of property rights into public domain to "land rush" which should be contained by law).

[154] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984) ("[A copyright] is intended to motivate the creative activity of authors and inventors by the provision of special reward, and to allow the public access to the products of their genius after the

these are limited exceptions, which do not apply to personal data. Property rights in personal data raise more serious concerns by establishing ownership of facts, an outcome that traditional intellectual property doctrine studiously avoids.[156] Facts, unlike creative works, are necessary precursors to subsequent thought and expression.[157] Recent proposals to establish property rights over databases[158] have come under sharp attack because they effectively may remove facts from the public domain.[159] These concerns echo some of the problems of free expression discussed more generally in Part I.[160]

More specific aspects of property doctrine also correspond poorly to data privacy concerns. The central purpose of a property right is to facilitate transfer.[161] If you own your clickstream and sell it in ex-

limited period of exclusive control has expired."); Mazer v. Stein, 347 U.S. 201, 219 (1954) ("The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors . . . .").

[155] In traditional doctrine, exclusive control over a trademark prevents customer confusion about the source of goods. As Judge Hand famously declared, "one merchant shall not divert customers from another by representing what he sells as emanating from the second. This has been, and perhaps even more now is, the whole Law and the Prophets on the subject . . . ." Yale Elec. Corp. v. Robertson, 26 F.2d 972, 973 (2d Cir. 1928). Recent expansion of trademark law has been criticized sharply for moving past this limited rationale. See, e.g., Mark A. Lemley, The Modern Lanham Act and the Death of Common Sense, 108 Yale L.J. 1687, 1688 (1999) ("[T]he changes in trademark doctrine over the last fifty years . . . have loosed trademark law from its traditional economic moorings and have offered little of substance to replace them.").

[156] See Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (holding that listings in telephone directory are facts which are not entitled to intellectual property protection); Harper & Row v. Nation Enters., 471 U.S. 539, 559-60 (1985) (upholding copyright restrictions but limiting scope to exclude ownership of facts); see also Volokh, supra note 68, at 1066 (emphasizing this aspect of *Harper & Row* reasoning).

[157] See *Feist*, 499 U.S. at 346-50 (stating that while law protects creative aspects of authors' works, it does not protect facts and ideas, and in fact "encourages [others] to build freely upon" them); Litman, supra note 9, at 1294 ("Facts are basic building blocks; building blocks of expression; of self-government; and of knowledge itself.").

[158] See The Collections of Information Antipiracy Act, H.R. 354, 106th Cong. (1999) (proposing copyright-related protection for databases of factual information). Under the bill, for example, an author would not be allowed to extract information from the Physician's Desk Reference for use in a publication about prescription drugs sold to the general public, even though information about pharmaceuticals approved by the Food and Drug Administration is publicly available. H.R. Rep. No. 106-349, pt. 1, at 17 (1999).

[159] See Yochai Benkler, Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information, 15 Berkeley Tech. L.J. 535, 558-59 (2000) (arguing that property right over databases undermines personal autonomy and democratic self-governance by restricting information available to individuals). Creating a property right in personal data would provide ammunition to supporters of database protections and other proposals to propertize facts. Lemley, supra note 151, at 1548; Volokh, supra note 68, at 1079-80.

[160] See supra notes 68-71 and accompanying text.

[161] Litman, supra note 9, at 1295-96 ("The raison d'être of property is alienability.").

change for access to a Web site, presumably the Web site operator now owns your clickstream and can resell it to a marketing firm.[162] Yet data privacy requires the ability to prevent exactly this type of later transaction, and such a restraint on alienation is heavily disfavored by traditional property law.[163]

Similarly, a property right confers the power to exclude. Yet there are numerous situations where society requires disclosure of personal data, without either consent or compensation, each of which would abrogate this right.[164] Perhaps most significantly, we allow the press to divulge personal data without consent all the time.[165] We also need unhindered access to personal data, for example, to investigate fraud,[166] to gauge the value of stocks,[167] or to take the census.[168]

Beyond this doctrinal mismatch, there are serious practical problems with a libertarian P3P privacy market. Surfers are in a comparatively weak bargaining position and need support from legal regulation of this market. They may not understand the full costs of divulging data[169] as clearly as Web site operators comprehend the value of collecting it.[170] In addition, the diffuse demand for privacy is probably insufficient to persuade businesses to adopt P3P in the first place.[171] Without legal ground rules to structure the bargaining process, surfers would be vulnerable to manipulation. Without effectual

[162] See id. at 1300-01 (describing implications for resale of alienable proprietary rights over personal data); Samuelson, supra note 11, at 1138 ("Free alienability works very well in the market for automobiles and land, but it is far from clear that it will work well for information privacy.").

[163] Restatement of Prop. § 489 cmt. a (1944) ("The policy of the law has been, in general, in favor of a high degree of alienability of property interests.").

[164] As a further possible complication, which will be mentioned here only briefly, if personal data were truly conceived of as a property right, government might even be constitutionally barred from appropriating it without compensation. See U.S. Const. amend. V ("[N]or shall private property be taken for public use, without just compensation.").

[165] See Volokh, supra note 68, at 1063-65 (discussing how property-based right to exclude others from personal data curtails expression, including freedom of press).

[166] See Schwartz, supra note 11, at 827 (citing fraud investigation among examples of mandatory disclosures of personal data).

[167] See Lemley, supra note 151, at 1550 (pointing to price of individuals' stock purchases as example of private individual financial transactions that must be available to public for market to function).

[168] See Posner, supra note 77, at 336-37 (describing absurd results of requiring government census-takers to pay individuals for their personal data).

[169] See supra note 49 and accompanying text (discussing "privacy myopia").

[170] See supra notes 28-30 and accompanying text (discussing potential value of personal data to Web site operators).

[171] See infra Part IV.B.1 (describing legal rules to overcome incentives against adoption of P3P).

legal enforcement of their property rights, they could not prevent misappropriation of their personal data.[172]

These flaws are too pervasive to be remedied with a few minor adjustments.[173] Rather than tinkering with a property right to the point of distortion, lawmakers should discard the premise entirely and start with one more closely tailored to P3P's strengths: enforcement of the privacy policy itself. Part IV builds on this alternative to propose a regime that offers the market modality's advantages of flexibility, utility, and competition, but also contemplates effective regulation by the legal modality.

IV
The Law: A P3P Privacy Market With Regulation

Lawmakers must step in to shape the P3P privacy market and ensure its effectiveness.[174] Their goal, of course, should be to preserve its advantages while discarding its shortcomings. They should embrace P3P,[175] but give the modality of law a more active regulatory role to address the P3P privacy market's flaws.[176]

This final Part recommends such a plan. Instead of enforcing a problematic new property right, the law would enforce the promises contained in a P3P policy. Then, legal regulation would help surfers overcome bargaining disadvantages they might have in a P3P privacy market, much as features of contract law protect vulnerable parties.

Reconceptualized in this way, the P3P privacy market has the capacity to provide robust data privacy while respecting the importance of free information flow.[177] Contrary to the assumptions of both its

[172] See infra Part IV.B.3 (describing importance of enforceable remedies for privacy violations).

[173] As Mark Lemley concludes, by the time all the flaws of a libertarian property right were addressed with alterations and exceptions, "a properly designed right would look rather more like a system of regulation than a system of property rights." Lemley, supra note 151, at 1554.

[174] Even some industry figures acknowledge this fact. See, e.g., Erich Luening, Tech Trade Group Turns About-Face on Privacy, CNet News, Jan. 18, 2001, at http://news.cnet.com/news/0-1007-200-4522635.html (describing sudden move by major industry group American Electronics Association to support limited federal regulation as preferable to patchwork of state laws). Contra David McGuire, U.S. Chamber Vows to Fight Privacy Legislation, Newsbytes, Jan. 9, 2001, at http://newsbytes.com/news/01/160268.html (reporting U.S. Chamber of Commerce plans actively to oppose any federal legislation concerning Web privacy).

[175] See Reidenberg, supra note 14, at 586-92 (urging policymakers to shift tactics and shape legal rules to existing technical architecture).

[176] See Laudon, supra note 122, at 99 ("Markets don't just happen. . . . Sometimes markets need to be created, encouraged, monitored, and regulated by governments.").

[177] See supra Part I (outlining these competing goals).

boosters and its critics,[178] P3P offers lawmakers great scope to design strong privacy protections within this framework. Far from a substitute for privacy law, or a hindrance to it, P3P thus becomes a powerful tool for lawmakers.

A. *The Promise Rationale for the P3P Privacy Market*

Ownership rights may be the most obvious source of legal protection for data privacy in a market, but they clearly are not the best.[179] As an alternative, lawmakers should shift their focus from property to contract. A few commentators have advanced this type of promise-based proposal, derived from various sources.[180] Doctrinally, it is similar to binding a party with an implied contract through promissory estoppel.[181]

A promise rationale takes advantage of the central features of P3P, helping lawmakers to integrate the protocol into this legal regime. A Web site operator who posts a P3P policy makes a commitment to observe certain data-handling practices. A surfer who visits the site may have done so relying on that commitment.[182] Law based on the promise rationale would presume this reliance, infer an agreement between the two parties, and create a legal duty for the Web site operator to fulfill the terms of a P3P policy.

[178] Supra notes 5-11 and accompanying text (describing assumption of both supporting and opposing camps that lawmakers should ignore P3P, with camps respectively arguing for nonintervention by law or for regulatory regime in which P3P plays no significant role).

[179] See supra Part III.B (critiquing property rationale for P3P privacy market).

[180] See, e.g., Samuelson, supra note 11, at 1151-67 (proposing licensing regime for personal data based on trade secret law); Volokh, supra note 68, at 1057-62 (defending data privacy protections based on contract and promissory estoppel as best suited to First Amendment interests); Kalinda Basho, Comment, The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?, 88 Cal. L. Rev. 1507, 1530-42 (2000) (proposing licensing regime for data privacy based on Uniform Computer Information Transactions Act (UCITA)). For similar proposals that predate the dominance of the Web, see Bibas, supra note 34, at 605-11 (proposing contractual approach for data privacy); Shorr, supra note 68, at 1834-50 (proposing contractual approach to protecting data privacy from credit bureaus).

[181] See Restatement (Second) of Contracts § 90 (1979) (binding promisor to promise that could reasonably be expected to induce action by promisee). The promise rationale also resembles consumer protection laws that ban deceptive trade practices. See infra note 223 and accompanying text (discussing regulatory actions against Web sites for violations of their privacy policies).

[182] A number of commentators recognize an expectation of data privacy. See, e.g., Berman & Mulligan, supra note 35, at 563-68 (cataloguing individuals' expectations of data privacy in different circumstances); Litman, supra note 9, at 1307-11 (describing consumers' expectation of privacy as giving rise to duty); Samuelson, supra note 11, at 1152-53 (tracing derivation of trade secret protection from doctrines of breach of contract and breach of confidential relationship); Skok, supra note 29, at 81-88 (arguing that Web users have legitimate expectation of privacy of clickstream data and that Fourth Amendment jurisprudence should adjust to recognize it).

Instead of enforcing a surfer's preexisting privacy rights or ownership interests, this approach focuses squarely on enforcing an agreement between the parties. Indeed, because the resulting regime simply provides an entitlement to a promise, it sidesteps the whole debate over the precise nature of an individual's claim to privacy.[183] Just as contract law generally applies the same rules to a sales agreement transferring property and a settlement agreement forgoing a personal claim, so the promise rationale would protect data privacy—despite scholarly disagreement about its precise moorings.[184]

The promise rationale also avoids specific problems associated with property rights in personal data. Because the surfer does not own personal data, the promise rationale does not contribute to the creeping propertization of information or facts.[185] Nor does it confer an overly broad right to exclude that would compel constant invasion when society needs access to personal data.[186]

Furthermore, when limitations on speech derive from an agreement by the parties, they rest on much firmer First Amendment grounds.[187] Even commentators who warn most strongly against data privacy restrictions that they consider unconstitutional would find it permissible for the state to enforce promises of privacy.[188] When data collectors promise through P3P not to disseminate surfers' personal data, they surrender any right they might have had to do so, and the enforcement of the promise is therefore constitutional.

Finally, contract law, in general, is far more hospitable than property doctrine to restrictive rules and policy-driven exceptions.[189] Pri-

[183] See supra notes 11-13 and accompanying text (citing commentary questioning relevance of "quasi-religious" dispute over rationale).

[184] See supra notes 20-26 and accompanying text (listing possible rationales for individual's claim to data privacy); see also Samuelson, supra note 11, at 1157-58 (describing how focus on promises sidesteps debate over nature of privacy).

[185] See supra notes 153-57 and accompanying text (discussing concerns that property rights in personal data encroach on public domain and grant ownership over facts).

[186] See supra notes 164-68 and accompanying text (discussing problems of broad right to exclude others from personal data).

[187] See Cohen v. Cowles Media, 501 U.S. 663 (1991) (rejecting First Amendment challenge to contractual speech restriction).

[188] See Richard A. Epstein, Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism, 52 Stan. L. Rev. 1003, 1047 (2000) (concluding that it is consistent with First Amendment to constrain communication of personal data where doing so would be "breach of confidence or contract"); Volokh, supra note 68, at 1057-63 (determining that promise model for data privacy is "eminently defensible" under First Amendment).

[189] See Samuelson, supra note 11, at 1155-56 (comparing amenability of contract and property doctrines to restrictive rules); cf. supra notes 161-63 and accompanying text (discussing hostility of property doctrine to restrictions necessary to protect data privacy in property rights regime).

vacy protection requires this type of intervention.[190] For example, while property law discourages the restraints on alienation necessary to safeguard data privacy, contracts by their nature are documents filled with restrictions and conditions. Similarly, contract doctrines such as unconscionability[191] routinely protect vulnerable parties rather than leaving them at the market's mercy.

As a result, lawmakers adopting a P3P privacy market based on a promise rationale would enjoy enormous flexibility in writing data privacy rules. The standard contracts toolkit includes mandatory rules that structure the bargaining process and that cannot be waived,[192] as well as default rules that the parties can contract around.[193] Lawmakers can borrow from both types of rules to establish their normative preferences for privacy protection.[194] The next Section offers some illustrations of this flexibility to prove that the P3P privacy market gives lawmakers the necessary tools to guarantee strong data privacy protection.

B. Legal Rules in a P3P Privacy Market

If lawmakers combine the code of P3P, market forces, and a legal rationale of promise enforcement, they will lay the foundation for an effective regime that balances the needs for data privacy and free information flow. Needless to say, this framework is just the beginning. Numerous decisions await them as they erect substantive rules on top of this foundation. This Section notes four issues that require lawmakers to make complex normative judgments: (1) adoption of P3P; (2) permanence of P3P promises; (3) enforcement of P3P promises; and (4) baseline standards for the negotiation process. For each one, this Note suggests the outlines of possible answers as an illustration of the regulated P3P privacy market's flexibility and strength.

[190] Supra notes 169-72 and accompanying text (describing how libertarian property rationale fails to protect potentially vulnerable surfers).

[191] See U.C.C. § 2-302 (1999).

[192] See, e.g., U.C.C. § 2-201 (1999) (codifying Statute of Frauds, requiring certain contracts to be written, as mandatory rule).

[193] See, e.g., Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, 15 U.S.C. § 2308(b) (1994) (allowing written limitation of warranty duration to shorter period than default under certain circumstances); U.C.C. § 2-308 (1999) (establishing default rules for delivery location).

[194] See infra Part IV.B.4 (illustrating ability of lawmakers to write protective rules under promise rationale).

1. *Adoption of P3P*

An obvious problem comes first: The existence of P3P technology does not ensure its use.[195] Absent any requirement to declare their data-handling practices, Web site operators will not want to discourage their visitors from providing personal data, or to emphasize the potentially unsavory collection of personal data on the Web.[196]

These barriers to adoption create a chicken-and-egg quandary: Individual surfers may not bother to employ user agents until they can fetch P3P policies from a critical mass of Web sites, but meanwhile Web site operators will not perceive a market demand that encourages them to support P3P.[197] The wide distribution of Microsoft's user agent may spur the adoption of at least compact policies for cookies.[198] Full deployment of P3P on Web sites, however, most likely will require legal intervention.[199]

The most straightforward method to jumpstart adoption of P3P would be simply to mandate that Web sites post P3P policies outlining their privacy practices. This idea is less intrusive than it may first appear. Disclosure requirements are commonplace in consumer-protection law, sometimes down to the exact format of a label. Moreover, the government often creates technological standards to ensure uniformity and interoperability.[200] The protocol could evolve to keep

[195] See Garfinkel, supra note 1 ("[A]s long as the protocol remains optional, organizations will have few incentives to create P3P labels that can help consumers."); Jason Sykes & Glenn R. Simpson, Some Big Sites Back P3P Plan; Others Wait, Wall St. J., Mar. 21, 2001, at B1 (reporting that operators of many large commercial Web sites have not decided whether to adopt P3P).

[196] See Murphy, supra note 122, at 2414 ("Raising the privacy issue may evoke negative reactions in consumers who otherwise would not have thought about the issue."); Kenneth Lee & Gabriel Speyer, White Paper: Platform for Privacy Preferences Project (P3P) & Citibank (Oct. 22, 1998), at www.w3.org/P3P/Lee_Speyer.html (last visited Aug. 22, 2001) (expressing major bank's concern that "P3P would let ordinary users see, in full gory detail, how their personal information might be misused by less trusted or responsible web site operators").

[197] See Netanel, supra note 49, at 479 (noting need for critical mass of surfers using P3P); Hunter, supra note 9 (describing "the chicken or the egg" dilemma of P3P adoption).

[198] See Greg Brooks, Sales Houses Struggle to Avoid New Browser Cookie Problems, New Media Age, June 21, 2001, at 5, 2001 WL 11318799 (reporting that third-party sites such as DoubleClick are scrambling to add compact policies to their cookies to avoid having them blocked by Internet Explorer 6.0); Walker, supra note 5 ("Most large commercial Web sites, however, are expected to adopt P3P eventually, because . . . [otherwise] they risk becoming inaccessible to many users of Microsoft's dominant browser."); supra notes 110-15 and accompanying text (describing Microsoft user agent).

[199] Netanel, supra note 49, at 479 (arguing government would need to require or encourage adoption of P3P).

[200] Lawmakers reluctant to choose a *particular* protocol in advance might instead set interoperability standards which could be met by P3P or by potential future intelligent agent systems. See supra note 81 (noting possibility of competing technology in future).

pace with change, whether under the aegis of the W3C or through another upgrading process.[201] Government could participate actively in this development.[202] Government could also shape other law—particularly intellectual property—to promote open and universal standard-setting.[203]

An alternative for those uncomfortable with a P3P-specific mandate would be to set a very strong default rule that bans collection of personal data but allows Web site operators and surfers to contract around it with a specific opt-in agreement.[204] Such a rule forces would-be data collectors to secure surfers' consent; Web site operators most likely would find the automated mechanism of P3P the easiest method for securing that consent.

The law also could influence the *quality* of P3P's adoption. Lawmakers may wish to write either mandates or default rules that would require or encourage user agents to offer robust privacy protection in a user-friendly format.[205] Such user agents would help surfers

[201] The W3C updates its recommendations regularly. World Wide Web Consortium, supra note 82. The P3P Specification expressly contemplates future versions of the protocol. See P3P Specification, supra note 3, § 1.1.6.

[202] See Consumer Privacy Protection Act, S. 2606, 106th Cong. § 707 (2000) (citing P3P by name and requiring National Institute of Standards and Technology to "encourage and support the development" of protocols "that would reflect the user's preferences for protecting personally-identifiable or other sensitive, privacy-related information, and automatically execute the program, once activated, without requiring user intervention"); Reidenberg, supra note 14, at 586-89 (urging lawmakers to achieve goals by influencing independent standard-setting bodies through participation in development of technical rules and funding of technical-capability development).

[203] The W3C recently advanced a controversial new proposal to include patented technology in its standards. Michele Herman et al., World Wide Web Consortium, W3C Patent Policy Framework, W3C Working Draft (Aug. 16, 2001), at http://www.w3.org/TR/2001/WD-patent-policy-20010816. A "blizzard" of criticism met the plan; opponents charge it could allow powerful companies to demand licensing fees from anyone who writes programs to comply with a W3C standard that incorporates patented material. See George A. Chidi Jr., W3C Proposal Could Allow Patent Grabs on Standards, InfoWorld Daily News, Oct. 2, 2001, 2001 WL 6589094; see also Janet Daly & Daniel J. Weitzner, World Wide Web Consortium, Response to Public Comments on the W3C Patent Policy Framework Working Draft (last modified Oct. 2, 2001), at http://www.w3.org/2001/10/patent-response (responding to criticism and extending public comment period on patent proposal).

[204] See, e.g., Kang, supra note 6, at 1271-73 (proposing default rule that personal data can be processed only in "functionally necessary" ways unless parties explicitly contract around rule); Netanel, supra note 49, at 479 n.347 (suggesting default rules with high standards); Samuelson, supra note 11, at 1155 & n.158 (noting strong opt-in requirement for use of trade secrets, with default ban on use for other than agreed-upon purposes, and recommending it as template for promise-based data privacy law); see also infra notes 231-32 and accompanying text (discussing high default rules with opt-in requirements).

[205] Direct legal intervention to require user-friendliness would help prevent what Paul Schwartz identifies as the "'blinking twelve' problem"—like countless Americans who do not set the clocks on their VCRs, leaving them to constantly blink "12:00," surfers who find user agents cumbersome may ignore them. Schwartz, supra note 107, at 754 (applying

better protect themselves in a regulated P3P market. Under many versions of these rules, the Microsoft user agent might not suffice.[206] Similarly, the law might set standards that require or encourage the adoption of P3P policies by every entity that collects data on a site, rather than just the site's principal host.[207]

Whether requiring the use of P3P or just encouraging it, the law has the power to overcome a collective action problem that resists its adoption. Rather than remaining technologically neutral, law in an integrated framework should promote the code that works best.[208]

2. *Permanence of Promises*

At present, Web site operators often reserve the right to modify their privacy policies unilaterally and without notice. Prominent Web sites such as EBay and Amazon have altered their privacy policies and applied the new, more intrusive policies to personal data collected under the old rules.[209] The economic troubles now buffeting many commercial Web site operators may intensify the temptation to raise cash by selling personal data, even when forbidden by the sites' original privacy policies.

This potential for midcourse alterations badly undermines the promises contained in privacy policies. In traditional contract law, courts look with suspicion on terms that allow one party to make uni-

blinking twelve image to P3P). Likewise, a strong opt-in default rule would help prevent nonuse by encouraging industry to develop more user-friendly software. Id. at 786.

[206] Kang, for instance, states that in order to suspend his proposed default rule, "a small icon at the bottom of a Web page would not suffice." Kang, supra note 6, at 1272. This is just the type of notification that IE 6.0 provides, along with some blocking and deleting of cookies. See Franco, supra note 114 (describing icons to notify user of discrepancies between preferences and compact policies).

[207] See supra note 107 (noting that host site's P3P policy can disavow data-handling practices of third parties that collect data on host site).

[208] See H.R. Res. 159, 107th Cong. (2001) (proposing that House of Representatives declare in nonbinding resolution that "any legislation relating to online privacy should take into consideration the terminology of the P3P specification" and that federal government Web sites should employ P3P); Lessig, supra note 16 (urging Congress and FTC to promote code solutions such as P3P through either subsidy or mandate); Reidenberg, supra note 14, at 587-93 (urging lawmakers actively to promote technological solutions to regulatory problems).

[209] See Lisa Guernsey, When It Came to Privacy on EBay, No Became Yes, N.Y. Times, Jan. 11, 2001, at G3 (reporting that EBay unilaterally switched preferences of at least six million members who had opted out of receiving unsolicited marketing messages); Saul Hansell, Technology Briefing: How Amazon Uses Information, N.Y. Times, Sept. 1, 2000, at C2 (reporting changes in Amazon's privacy policy which added practice of sending marketing e-mail messages on behalf of other companies and right to sell personal data with other assets if Amazon is purchased).

lateral changes in the promised performance.[210] Rules of both code and law need to apply this presumption forcefully to P3P promises.

P3P's code already restricts the ability of Web site operators to amend their promises. The P3P Specification declares that "when a Web site changes its P3P policy, the old policy applies to data collected when it was in effect."[211] In addition, to optimize user agent performance, a P3P policy may guarantee its effectiveness for a particular length of time so that the user agent need not retrieve the policy repeatedly.[212] These rules discourage changes in the policy by making them prospective only, by providing technical incentives against modifications, and by requiring full disclosure.

Legally, the act of posting a P3P policy should signal a Web site operator's acceptance of the protocol's permanence rules. While this variant of statutory adoption flows naturally from the logic of the promise rationale, it would probably need to be codified, particularly to deal with special situations such as mergers or bankruptcy.[213] In general, changes in the policy should be prospective only, though lawmakers may wish to allow specific exceptions.[214] Thus, law can reinforce code in guaranteeing that privacy promises are not surreptitiously rewritten after they are made. Once more, the P3P privacy market will not achieve this result without the modality of law.

[210] See Restatement (Second) of Contracts § 77 & cmt.a (1979) (stating that promise is "illusory" and not valid as consideration for contract if promisor reserves right to deliver alternative performance which would not constitute consideration).

[211] P3P Specification, supra note 3, § 2.4.6.

[212] See id. § 2.3.2.3 (explaining methods for informing user agents of policy lifetimes). If a policy has expired since the last time a user agent fetched it, the user agent must retrieve the newest version and conduct a fresh comparison of the current policy with the surfer's preferences. Thus, longer policy lifetimes increase the speed of browsing by eliminating the P3P transaction in more instances. Id.

[213] See Susan Stellin, Dot-Com Liquidations Put Consumer Data in Limbo, N.Y. Times, Dec. 4, 2000, at C4 (reporting on unclear status of consumers' personal data under bankruptcy law). The FTC and at least forty state attorneys general filed suit to prevent the sale of customers' personal data by the bankrupt Web site Toysmart.com. Id. The case ended in a settlement when a subsidiary of Disney, which owned a large stake in Toysmart, agreed to pay the bankrupt company $50,000 in exchange for destruction of the data. Stephanie Stoughton, Toysmart.com List To Be Destroyed, Boston Globe, Jan. 30, 2001, at D7.

[214] Lawmakers may wish to design a mechanism to allow for changes made with the surfer's agreement, but would need to determine the rules for consent. For mergers and bankruptcies, perhaps the law could allow a one-time transfer of personal data to a merger partner or creditor that was not authorized by the privacy policy, but then require the new party to honor the original promises. This would not depress the value of the personal data as an asset, because it remains tied to the same conditions that always had governed its use.

3. *Enforcement of Promises*

Without enforcement, P3P's facilitation of promise-making becomes an empty exercise.[215] The surfer must have remedies available when Web site operators fail to live up to the commitments they make.[216]

In theory, existing causes of action provide some recourse against a Web site operator who breaks a promise, even if not for the underlying privacy invasions.[217] Surfers might make claims, alone or in class actions, based on fraud, breach of contract, or unfair trade practices.[218]

Calculation of damages, however, presents a serious obstacle to proceeding under current law. A plaintiff could not prove significant economic damage from the misuse of personal data, and courts would be reluctant to recognize claims for emotional harm in all but the most extraordinary cases.[219] Injunctive relief does surfers little good once their personal data already has been transferred far and wide.

Therefore, law must supplement code again, by establishing a statutory remedy that compensates the individual.[220] The precise amount of damages is a policy judgment, but it must be sufficient to make pursuit of a remedy worthwhile to the wronged surfer and to deter Web site operators from violating their promises.[221]

[215] See P3P Specification, supra note 3, § 1 ("[P3P] . . . does not provide a technical mechanism for making sure sites act according to their policies. . . . P3P is complementary to laws and self-regulatory programs that can provide enforcement mechanisms.").

[216] Privacy expert Larry Ponemon estimates that eighty percent of companies violate their privacy policies, usually through inadvertence caused by poor training of employees and a failure to place a high priority on compliance. See Andrea Petersen, Private Matters: It Seems That Trust Equals Revenue, Even Online, Wall St. J., Feb. 12, 2001, at R24.

[217] See supra notes 31-34 and accompanying text (describing lack of legal recourse for violations of data privacy).

[218] See Sovern, supra note 31, at 1349-57 (discussing enforcement under states' "little FTC acts," including citizen suits).

[219] See, e.g., Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356-57 (Ill. 1995) (holding that plaintiffs fulfilled all elements necessary under Illinois Consumer Fraud Act to make claim that release of purchasing history by credit card company was deceptive practice, but rejecting claim for lack of damages).

[220] But see Jennifer Jones, Microsoft Touts P3P as Consumer Safeguard, Infoworld, Mar. 26, 2001, at 5 (quoting industry lobbyist opposing any private right of action for data privacy violations).

[221] See Bibas, supra note 34, at 607 n.108 (suggesting that "damages should be set at a statutory sum of liquidated damages plus attorney's fees because it would be impossible to prove the quantum of actual damages"). The Privacy Protection Act of 1988 allows for liquidated damages of up to $2500 per violation, punitive damages, attorney's fees, and injunctive relief. See 18 U.S.C. § 2710(c) (1994). One current Senate proposal tracks this formula. See Spyware Control and Privacy Protection Act, S. 197, 107th Cong. § 2(c) (2001) (providing a private right of action against software providers for failure to provide notice and choice of data-collection practices).

In addition to a private right of action with liquidated damages, regulatory enforcement also would be essential, because individuals may not have the resources to prove how their personal data has been mishandled in violation of P3P policies.[222] Regulators have won settlements in some cases under current law,[223] but a statute should clarify their power to intervene on behalf of surfers when promises are broken. Such a law could vest this authority in an existing federal body, such as the FTC[224] (perhaps in combination with state attorneys general), or in a new privacy-oriented regulatory agency.[225] Administrative enforcement would enable resource-intensive investigations, such as the use of testers, and sustained pursuit of large Web site operators who have violated their policies.[226]

The libertarian P3P privacy market elicits privacy promises, but yet again, only the law can ensure that they are honored.

[222] See Kang, supra note 6, at 1272 & n.316 (stating logistical necessity of administrative enforcement); Netanel, supra note 49, at 480 (same); Sovern, supra note 31, at 1322 (noting that FTC can take action under FTC Act "when affirmative misrepresentations are made in the collection of information"). But see Bibas, supra note 34, at 607 & n.108 (agreeing that individuals might face practical problems suing, but proposing enforcement by entrepreneurial "information sleuths" who work as testers motivated by damage awards rather than "an inefficient government body to police violations").

[223] See, e.g., In re GeoCities, Fed. Trade Comm'n, No. C-3849 (Feb. 12, 1999), excerpted in Mark A. Lemley et al., Software and Internet Law 991-1001 (2000) (settling federal regulators' claim against Web site for violation of privacy policy); Mark E. Budnitz, Consumer Privacy in Electronic Commerce, 14 Notre Dame J.L. Ethics & Pub. Pol'y 821, 828-49 (2000) (discussing suit under state law by attorney general of Minnesota against bank for violating Web site privacy policy and resulting settlement); supra note 213 (discussing regulators' attempt to prevent sale of personal data by bankrupt Web site operator); see also FTC Report, supra note 1, at 33-34 (discussing existing FTC authority over Web site privacy policies).

[224] See Kang, supra note 6, at 1272 & n.316 (suggesting giving authority to FTC). But see Reidenberg, supra note 40, at 790-91 (stressing disadvantages of giving authority over data privacy to existing bodies such as Commerce Department and Federal Communications Commission). The FTC itself previously supported such a law, see FTC Report, supra note 1, at 36-38 (proposing legislation to expand FTC authority), but the FTC's new chairman recently indicated a reversal of this position. See Timothy J. Muris, Protecting Consumers' Privacy: 2002 and Beyond, Address Before the Privacy 2001 Conference (Oct. 4, 2001), at http://www.ftc.gov/speeches/muris/privisp1002.htm.

[225] See Charles Nesson, Threats to Privacy, Keynote Address, in 68 Soc. Res. 105, 111 (2001) (advocating "something approaching an Environmental Protection Agency for privacy"); Reidenberg, supra note 40, at 790 (calling for separate privacy agency).

[226] The agency could also disseminate information about individual Web sites' compliance with their privacy policies, "a classic public good." Netanel, supra note 49, at 480. The FTC recently took the first step in this direction by providing aggregate statistics on a range of issues concerning Web site privacy policies. FTC Report, supra note 1, at 7-28 (providing results of survey of privacy policies).

4. *Bargaining Process*

Even if the law required or encouraged every Web site to use P3P technology, rendered the resulting promises permanent, and enforced them, the surfer still would need protection during the negotiation process itself.[227] Unfortunately, critics who shun the P3P privacy market for this reason are missing a golden opportunity. P3P actually enhances, rather than reduces, the scope of legal rules lawmakers can write. This subsection will not attempt a comprehensive review of the myriad options but will make the point with two illustrations.

One example is the passionate debate over whether a Web site operator should be required to receive an affirmative opt-in from a surfer before collecting data, as privacy advocates demand, or simply offer the surfer an opportunity to opt out, as industry insists.[228] Opponents of an opt-in mandate typically protest that securing individual approval from each surfer for the use of personal data burdens Web site operators.[229] Although the P3P protocol itself is neutral on the question, it creates a technical mechanism to accommodate an opt-in rule inexpensively and easily.[230] A P3P opt-in could be paired with a default rule that forces Web site operators to secure consent from each surfer.[231] Lawmakers even could require that user agents' settings of privacy preferences default to a high level of privacy, so that surfers would need to take an affirmative step to adopt less protective preferences, thus opting in.[232] By streamlining and automating the opt-in process, P3P shapes the privacy market to focus on true consent

[227] See supra notes 169-72 and accompanying text (describing surfers' negotiating disadvantage).

[228] See, e.g., Jonathan Krim & Robert O'Harrow Jr., Democrats Focus on Internet Privacy, Wash. Post, July 12, 2001, at E2 (describing testimony at congressional hearing reflecting these viewpoints).

[229] Id. (stating that "many companies oppose [an opt-in requirement], saying it would be costly to implement and would hinder activity on the Web").

[230] See P3P Specification, supra note 3, §§ 3.3.4, 3.3.5 (creating optional means for P3P policy to offer opt-out or opt-in capability); supra note 102 and accompanying text (discussing opt-in and opt-out under P3P); see also P3P Specification, supra note 3, § 1.1.6 (explaining that mechanism to better enable surfers' explicit agreement to P3P policies, dropped from current protocol, may be added in future versions).

[231] See supra notes 204-06 and accompanying text (discussing concept of strong default rule with opt-in requirement).

[232] The Microsoft user agent would not satisfy this test. See supra note 113 and accompanying text (discussing default settings of Microsoft user agent). Mandating a high-standard default in user agents would take better advantage of P3P's ability to permit seamless navigation, rather than interrupting surfers repeatedly with opt-in requests. The normative question of what exact level of privacy should be set as a user agent's starting point is beyond the scope of this Note. The point here is that this framework allows lawmakers—in fact, positively assists them—to select any level of default settings they deem appropriate.

by informed surfers and makes it much more difficult for businesses to oppose opt-in credibly.

A second example illustrates how P3P allows lawmakers to create more complex restrictions without increasing the cost of compliance. In its last days, the Clinton Administration promulgated regulations governing the use of personal data by health care providers.[233] Privacy advocates praised the rules for their strength, and industry lobbyists condemned them as costly and burdensome.[234] In sum, the rules require a patient opt-in for collection of personal data, ban the transfer of data for certain nonhealth purposes such as marketing, and mandate disclosure of data-handling practices to patients.

While it is arguable whether these regulations are truly burdensome in real space, imagine similarly stringent rules in a P3P privacy market based on promises. For any medical data collected,[235] a site's P3P policy would list the recipients[236] and purposes[237] and attach them to an opt-in mechanism.[238] Perhaps a Web site operator would want to add an explanation of the reasons for these practices.[239] Presumably, the policy would not include practices banned by law.[240] The user agent would then report all of this to the surfer, who would have to click an "I accept" button before the Web site could collect data. The underlying substantive law even could be preprogrammed into the user agent's preferences, so that a site with an illegal policy would be identified and, perhaps, blocked. P3P conveys the fine-grained distinctions that this rule requires, without sacrificing flexibility or imposing gigantic costs.

[233] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

[234] Robert Pear, New Privacy Rules Are Challenged, N.Y. Times, Dec. 21, 2000, at A22 (quoting sources on both sides of debate); Melvyn B. Ruskin & Keshia B. Haskins, Reviewing New Federal Rules on Health Privacy, N.Y. L.J., July 18, 2001, at 1 (stating that rules have "received mixed reviews, with privacy advocates trumpeting them as much needed regulatory consumer protection and the health care industry labeling them as overbroad, burdensome and excessively costly to implement"); see also Robert Pear, House Republicans Urge Bush To Ease Health Care Rules, N.Y. Times, May 11, 2001, at A24 (reporting that chairs of relevant House committee and subcommittee consider rules "unworkable" and urged President Bush to revise them).

[235] That is, in P3P terms, any data in the <health/> category. See P3P Specification, supra note 3, § 3.4 (listing and defining data categories).

[236] See id. § 3.3.5 (defining <recipient/> element).

[237] See id. § 3.3.4 (defining <purpose/> element).

[238] See id. §§ 3.3.4, 3.3.5 (explaining how P3P can tie opt-in to <purpose/> and <recipient/> elements).

[239] This is easily accomplished with the <consequence/> element. See id. § 3.3.2 (defining <consequence/> element).

[240] In this example, the purpose would not include <individual-analysis/>, <contact/>, or <telemarketing/>, see id. § 3.3.4, and the recipient would not include <unrelated/>, see id. § 3.3.5.

For those concerned that a P3P privacy market would be overly laissez-faire, these examples demonstrate the potential for a framework of P3P promises to establish minimum standards even more effectively than a regulatory regime. Automating the negotiation over privacy allows surfers to exercise control over the collection of their personal data, and also makes it easier for lawmakers to regulate that process. Indeed, using P3P and the promise rationale, lawmakers could choose to write rules substantially more or less restrictive than the Clinton Administration regulations without sacrificing flexibility or confusing consumers.

Conclusion

P3P elicits "Programmed Privacy Promises."[241] Lawmakers hoping to strike the right balance between protecting privacy and promoting the free flow of information on the Web should use these promises as the foundation of a privacy-protection regime.

P3P combines with market forces to reduce transaction costs and spur privacy-enhancing competition. While this P3P privacy market is not enough to protect data privacy on its own, the addition of contract-oriented regulation completes an effective regime. Thus, lawmakers can combine the modalities of code, market, and law to protect privacy with rules as strong as they wish, while respecting surfers' individual choices and the need for flexibility when regulating the Web. Although previous commentary has associated the protocol with flawed laissez-faire or industry-supported proposals, P3P instead can serve as a tool for lawmakers who are concerned about the threats to data privacy on the Web.

[241] Understandably, the protocol's silly acronym has invited similar plays on its name from critics. See, e.g., EPIC/Junkbusters Report, supra note 9 (dubbing P3P "Pretty Poor Privacy," in implicit contrast to encryption program called Pretty Good Privacy); Catlett, supra note 142 (suggesting that use of P3P by lobbyists to argue for delays in legislation makes P3P "Pretext for Privacy Procrastination").