Perspektive Datenschutz

Praxis und Entwicklungen in Recht und Technik

Herausgegeben von

Dr. Bruno Baeriswyl
Datenschutzbeauftragter des Kantons Zürich

Dr. Beat Rudin
Advokat, Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit, Basel

Schulthess Juristische Medien AG Zürich
Nomos Verlagsgesellschaft Baden-Baden
Verlag Österreich GmbH Wien

Veröffentlichung in der Schweiz:
Schulthess Juristische Medien AG, Zürich – ISBN 3 7255 4329 1

Veröffentlichung in Deutschland:
Nomos Verlagsgesellschaft, Baden-Baden – ISBN 3 7890 7744 5

Veröffentlichung in Österreich:
Verlag Österreich GmbH, Wien – ISBN 3 7046 3606 1

Inhaltsübersicht

Privacy, Participation, and Cyberspace: An American Perspective*

PAUL M. SCHWARTZ

Table of contents

«Wer die Kommunikationsfähigkeit ernst nimmt und sie deshalb nicht mit der Installation des Netzwerkes gleichsetzt, sondern nach dessen Konsequenzen für die Selbstbestimmung und Partizipationschancen des einzelnen fragt, hat keine Wahl: Er muss die Technologie einspannen, um Störungen und Verzerrungen zu korrigieren.»[1]

1 Introduction

Cyberspace is our new arena for public and private activities. It reveals information technology's great promise, which is to form new links between people and to marshal these connections to increase col-

* Last updated in january 2001 (Clinton Administration).

1 SPIROS SIMITIS, Internet oder der entzauberte Mythos vom «freien Markt der Meinungen», in: Wirtschafts- und Medienrecht in der offenen Demokratie (Freundesgabe für Friedrich Kuebler) (1997).

laboration in political and other activities that promote democratic community.[2] In particular, cyberspace has a tremendous potential to revitalize democratic self-governance at a time when a declining level of participation in communal life endangers civil society.

Yet, information technology in cyberspace also affects privacy in ways that are dramatically different from anything previously possible.[3] By generating comprehensive records of online behavior, information technology can broadcast an individual's secrets in ways that she can neither anticipate nor control. Once linked to the Internet, the computer on our desk becomes a potential recorder and betrayer of our confidences. In the absence of strong privacy rules, cyberspace's civic potential will never be attained.

At present, however, no successful standards, legal or otherwise, exist in the United States for limiting the collection and utilization of personal data in cyberspace. The lack of appropriate and enforceable privacy norms poses a significant threat to democracy in the emerging Information Age. Indeed, information privacy concerns are the leading reason why individuals not on the Internet are choosing to stay off.[4]

2 The Supreme Court invoked cyberspace's potential contribution to democratic community in Reno v. ACLU where it spoke of the «vast democratic fora of the Internet.» 117 S.Ct. 2329, 2343 (1997). It also noted cyberspace's creation of a «dynamic, multifaceted category of communication» with unlimited possibilities for speech. Id. at 2337, 2343. See infra Part II. See also LAWRENCE LESSIG, The Zones of Cyberspace, 48 Stan. L. Rev. 1403, 1407 (1996) (cyberspace «is a space filled with community»).

3 See PETER P. SWIRE AND ROBERT E. LITAN, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive vii (1998) («The Internet has made it easier for anyone to collect personal information about others.»); JERRY KANG, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1198 (1998) (in cyberspace, «you are invisibly stamped with a bar code»).

4 A Little Privacy Please, Business Week, March 16, 1998, at 98 [hereinafter Business Week Poll]. This Business Week/Harris Poll also found that of people who already use the Internet, «78% say they would use the Web more if privacy were guaranteed.» Id. The Graphic, Visualization, and Usability Center's («GVU») Tenth World Wide Web User Survey also revealed a high level of public concern for information privacy. Graphic, Visualization & Usability Center, Tenth World Wide Web Survey Results (October 1998) <http:www.gvu.gatech.edu/user_surveys/>. This survey, which relied on the self-reporting of visitors to the GVU Web site, found that over seventy-five percent of Internet users rated privacy as more important than convenience, and seventy percent agreed that a need existed for Internet privacy laws. Id. In addition, eighty percent of Internet users disagreed that content providers had a right to resell user information. Id.

The stakes are enormous; the norms that we develop for personal data use on the Internet will play an essential role in shaping American democracy in the Information Age. Nevertheless, the Clinton Administration and legal commentators increasingly view the role of the Internet and of law on it as facilitating wealth creating transmissions of information, including those of personal data.[5] In this Essay, I take a different tack; my perspective does not oppose a commercial function for cyberspace, but argues for the necessity of something other than shopping on the Internet. In my view, moreover, unfettered participation in democratic and other fora in cyberspace will not take place without the right kinds of legal limits on access to personal information.

In this essay, I argue that the Internet's potential to improve shared life in the United States will be squandered unless we structure the kind of information use necessary for democratic community and individual self-governance. Participants in cyberspace need access to public, quasi-public and private «spaces» where they can engage in civic dialogue and the process of individual self-definition. My analysis centers on the current policy debate regarding three potential, and potentially overlapping, regulatory techniques for Internet privacy. These techniques look to: (1) the market, (2) industry self-regulation; and (3) the law's imposition of standards. Of these options for privacy protection, industry self-regulation is the most popular policy alterna-

5 For the views of the Clinton Administration, see U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, First Annual Report (1998) («Electronic commerce should be a market-driven arena and not a regulated one» and the role of government is to «support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.») [hereinafter WORKING GROUP ON E-COMMERCE]; THE WHITE HOUSE, A Framework for Global Electronic Commerce, Principles, Sec. 2 at 2(1997) <http://www.whitehouse.gov/WH/New/Commerce/read.html> («Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention.»). For the views of academic commentators regarding the centrality of wealth creation on the Internet, see SWIRE & LITAN, supra note 3, at 88 («[While] people will engage in more electronic commerce if they believe their privacy will be protected[,]» at the same time «[a]ny such increases may be offset by the decreases in commerce that can occur because of interference with the free market.»); FRANK EASTERBROOK, Cyberspace and the Law of the Horse, 1996 U. Chi. Legal F. 207, 210-212 (1996) (emphasizing the essential role in cyberspace of «private transactions» and the establishment of property rights, «without which welfare-increasing bargains cannot occur.»). See also JUSTIN MATLICK, Don't Restrain Trade in Information, Wall St.J., Dec. 2, 1998, at A22 («New privacy regulations would be at best redundant. At worst, they would raise the start-up costs of Web-based businesses that don't need privacy policies.»).

tive for the Clinton Administration at present.[6] Yet, Congress has indicated a modest preference for the third option by enacting a law to protect children's privacy on the Internet.[7] In the closing days of the last Congress, President Clinton cooperated in this creation of legal standards by signing this privacy law for one small corner of cyberspace.[8]

My conclusion is that all three of these techniques, including self-regulation, have an important role in developing effective privacy norms. Under current conditions in cyberspace, however, it is the law's imposition of standards that is of essential importance. A statutory expression of privacy norms for cyberspace will be the most effective first step in promoting democratic deliberation and individual self-determination in this new realm. This legal action will lead to significant benefits: (1) the prevention of a lock-in of poor privacy standards on a societal level; and (2) the creation of preconditions for effective market and self-regulatory contributions to privacy protection.[9] The good news is that is not too late to develop privacy rules for cyberspace; the bad news is that the price of delay will be high.

2 The Creation of Fair Information Practices: The Market, Self-Regulation, and Law

Current debate about cyberspace privacy in the United States focuses on three possibilities: the market, industry self-regulation, and the law. By far, the most popular of these alternatives at present is industry self-regulation. This essay argues, however, that reliance on the market and industry under current conditions will have unsatisfactory

6 See WORKING GROUP ON E-COMMERCE, supra note 5, at iv (noting «President's proposals for private sector leadership and self-regulation of the Internet»). Nevertheless, the Clinton Administration has also stated that the government should take action «through law or regulation ... to protect the privacy of especially sensitive information and to prevent predatory practices.» Id. at 17. See also KEN MAGILL, Gore's Privacy Plans Signal No Clear Agenda: White House ‹still ducking the hard problems›, DM News, August 10, 1998, at 1 («[P]eople from all sides of the [privacy] debate are struggling to find where their agendas fall on the White House scorecard.»).

7 Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (codified at 15 U.S.C.A. §6501).

8 Id.

9 Id.

results unless the law first imposes the necessary fair information practices.

3 Let's Make A Deal: The Privacy Market

A pure market approach to privacy relies on interactions between individuals and data processors to generate and maintain appropriate norms for information privacy. Yet, the market, like government, is a creation of human choice, and all markets do not function equally well to serve different aims.[10] In particular, I would like to distinguish at this point between making the Web safe for e-commerce, which is the focus of much information policy at present in the United States, and the possibility of using market exchanges to develop information territories for privacy in cyberspace.

At present, information policy in the United States focuses on facilitating wealth-creating transfers over the Internet. The Clinton Administration is striving to make the Web and the world safe for e-commerce. In this Essay, I take a different tack; my perspective is not in opposition to a commercial function for cyberspace, but argues for the necessity of something other than shopping on the Internet. Specifically, cyberspace has the potential to revitalize participatory democracy if we can establish the right level of disclosure/confidentiality in it. While the marketplace can have a role in generating the borders of multidimensional territories in cyberspace, the current market for privacy is unlikely to reach a result that will promote democratic self-rule. Once fair information practices are firmly established, however, the market can play an important role in maintaining and enforcing these norms.

Two reasons exist for caution regarding a pure market approach under present conditions. These are: (1) the «knowledge gap,» which refers to the widespread ignorance regarding the terms that regulate disclosure or non-disclosure of personal information, and (2) the «consent fallacy,» which points to weaknesses in the nature of agreement to data use. Both support a conclusion that reliance on a privacy mar-

10 For more on this perspective on the market, see ARTHUR ALAN LEFF, Economic Analysis of Law: Some Realism About Nominalism, 60 Va. L.Rev. 451, 468-70 (1974).

ket will not generate appropriate rules regarding personal data use in cyberspace.

To begin with the «knowledge gap,» individuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed. This widespread individual ignorance hinders development through the privacy marketplace of appropriate norms about personal data use; the result of this asymmetrical knowledge will be one-sided bargains that benefit data processors.[11] As JAMES GLAVE, a reporter for *wired.com*, has written, «[T]he vast majority of the Internet-viewing public still has no idea how to judiciously use their personal information, or even why they should.»[12] The lack of knowledge of processing practices is, moreover, a systematic consequence of the social and institutional structure of personal data use.

This lack of knowledge rests on two factors. First, at a time when more Americans from all backgrounds are going online, the extent of privacy in cyberspace largely depends on an opaque technical infrastructure. A result of this ignorance is that individuals are handicapped in negotiating for their privacy interests. Second, the online industry, the entity with superior knowledge, generally has incentives to provide suboptimal information to guide individual decision-making about personal data use.[13] Silence works in the favor of the parties who construct «code» and utilize it in their business endeavors. The resulting societal ignorance of the terms of data processing contributes to the failure of the privacy market.

Beyond the «knowledge gap,» a final reason exists for caution about use of a market to establish privacy standards. I term this critique, the «consent fallacy.» A standard requirement for valid consent is that it

11 See generally ROBERT COOTER & THOMAS ULEN, Law and Economics 364 (2d ed. 1997) (discussing severe information asymmetries as a standard cause of market failure).

12 JAMES GLAVE, Wired News Privacy Report Card, wired.com 2 (December 22, 1998) <http://www.wired.com/news/print_version/politics/story/16963.html?wnpg=all>.

13 PHILIP AGRE has noted a significant aspect of this incentive structure. Agre observes that the relationship between data processing organizations and individuals is generally based on asymmetric knowledge. PHILIP R. AGRE, Introduction in Technology and Privacy: The New Landscape 1, 11 (PHILIP E. AGRE & MARC ROTENBERG eds., 1997). As a result, «the organization [has] the greater power to control what information about itself is released while simultaneously obscuring the nature and scope of the information it has obtained about individuals.» Id.

be both: (1) informed and (2) voluntary.[14] We have already seen that individuals are likely to lack knowledge of the technological context of data use and that parties with the necessary knowledge may be unwilling to disgorge all relevant data. As a result, consent to data processing cannot as a general matter be characterized as «informed.»[15] The «voluntary» nature of consent is also doubtful. Even when consent to an exchange of personal data is carried out in a formal manner, its voluntariness is often suspect.

Personal data use in cyberspace increasingly is structured around an empty process of consent that takes both formal and informal variants. As I have noted, some Web sites currently present screens with a consent form that must be clicked on as a condition for entering the site. Beyond this seeking of formal consent, other Web sites, such as that of the *New York Post*, contain consent boilerplate in their privacy statements that seek to create the legal fiction of informal agreement to data processing practices for all that visit the site.[16] In either manner of «consent,» formal or informal, agreement to data processing in cyberspace is likely to turn into a hollow ritual. Individuals may not bother to read a given «informed consent» screen or know where to look for a «privacy statement» before they click through or «surf» deeper into a Web site. In addition, the language on a consent screen or «privacy statement» may approve any and all use of an individual's personal information. Self-reliant consent cannot fulfill its assigned role if individuals are guided into making uninformed, non-voluntary exchanges.[17]

This analysis suggests that current conditions are not favorable for the marketplace to generate the fair information practices that this Essay has advocated. Nevertheless, once these fair information practices are in place, the market has a potentially important role. Trusted Third Parties (TTP's) can help individuals negotiate around privacy default standards. Trusted Third Parties are already emerging. In particular,

14 For a discussion of informed consent in the health care setting, see PETER H. SCHUCK, Rethinking Informed Consent, 103 Yale L.J. 899, 902-04 (1994); JOSEPH GOLDSTEIN, For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent and the Plea Bargain, 84 Yale L.J. 683, 690-94 (1975).

15 The consent is not «informed» due to the lack of disclosure about planned data use that most Americans would view as «material» to their decision to agree to the processing.

16 N.Y. Post (visited April 5, 1999)<http://www.nypost.com>.

17 See generally MARK A. LEMLEY, Beyond Preemption: The Law and Policy of Intellectual Property Licensing, 87 Cal. L. Rev. 111, 129-30 (1999) (criticizing «shrinkwrap» licensing terms that give copyright owners excessive rights).

the «infomediary» seeks to act on behalf of individuals in creating a new «information supply chain.»[18] Individuals are first to express their privacy preferences, including the personal data that they wish to reveal to these TTP's; these entities are then to locate firms that agree to accept this information and gather no more.[19]

Taken by themselves, however, infomediaries are unlikely to turn the necessary fair information practices into cyberspace's predominant norms. Infomediaries negotiating around a default of *maximum* disclosure of personal information will be incapable of shifting the customs of the Web through their practices. This transformation will be hindered by consumer ignorance and the lack of market incentives to make the majority of firms oppose their self-interest, which lies in maintaining the status quo. In the next section, I will explore in detail why industry collectively benefits if it can resist changes in current privacy norms, including that of maximum information disclosure. Here, I wish only to note that the result of this likely market equilibrium will be one-sided bargains for consumers and the marginalization of infomediaries.

This analysis suggests, however, that infomediaries will have great potential in helping individuals negotiate around a default of *minimum* disclosure. Once this default norm is established, industry will have a strong incentive to offer more in exchange for personal data and have more interest in doing business with infomediaries. In other words, infomediaries can help in the development of «privacy price discrimination.» By this term, I wish to indicate a differentiation by data processing companies among individuals with varying preferences about the use of their personal data.[20] A default norm of mini-

18 JOHN HAGEL III & JEFFREY F. RAYPORT, The Coming Battle for Customer Information, Harv. Bus. Rev. 53, 54 (1997).

19 Id. at 55-57; JOHN HAGEL III & MARC SINGER, Net Worth: Shaping Markets When Customers Make the Rules 109-33 (1999). Infomediaries make this customization of privacy possible by developing new data management software. For example, the CEO of Lumeria promises to hand millions of consumers a «superWallet» with a «super-Password» that will let them control and update personal information «including which marketers get to what parts of it, how much these firms are allowed to see, or if they can see it at all.» JAMES GLAVE, The Dawn of the Infomediary, wired.com 1 (Feb. 24, 1999) <http://www.wired.com/news/print_version/business/story/18094.html?wnpg=all>.

20 My development of a concept of «privacy price discrimination» has a close analogy in the law of intellectual property. In the context of computer software, in particular, the law has been highly attentive to price discrimination and the kinds of behavior that should be permitted among buyers and sellers of information goods. See, e.g., ProCD v. Zeidenberg, 86 F.3d 1447, 1448-49 (7th Cir. 1996); ROBERT MERGES,

mum data disclosure will thereby end a personal information subsidy to data processing companies. I will explore the idea of the information subsidy at greater length in the next section; here, I wish only to stress that ending this assistance to industry will cause a net social gain by allowing individuals to personalize their privacy levels around standards that promote democratic self-rule.

4 Industry Knows Best: Self-Regulatory Mechanisms

While self-regulation remains the favored policy alternative for privacy on the Internet, it is as improbable a candidate for success as the privacy market. Nevertheless, Vice President Gore, the Commerce Department, and the United States Government Working Group on Electronic Commerce all strongly endorse privacy protection through industry self-regulation. The online industry has found this emphasis welcome, and, in turn, is emphasizing its sensitivity to information privacy issues. In the words of the Online Privacy Alliance, a lobbying organization representing a wide range of corporations and associations, online industry is engaged in «development and use of self-regulatory initiatives that create an environment of trust and foster the protection of individuals' privacy online and in electronic commerce.»[21]

I begin my analysis of privacy self-regulation by putting it into the larger perspective of standard-setting. Apart from a sometimes significant governmental role in developing standards, companies engage in this process through either competition or cooperation.[22] During a standards competition, companies promote dueling products in an effort to control the future technological standard. An example of such a standards war is the losing battle that Sony fought in the

Comment: Of Property Rules, Coase, and Intellectual Property, 94 Colum. L. Rev. 2655, 2666-67 (1994); WILLIAM M. LANDES & RICHARD POSNER, An Economic Analysis of Copyright Law, 18 J. Legal Stud. 325, 328 (1989).

21 Online Privacy Alliance, Mission (visited March 30, 1999) <http://www.privacyalliance.com/mission/>.

22 CARL SHAPIRO & HAL R. VARIAN, Information Rules 261-96 (1999); JOSEPH FARRELL, Standarization and Intellectual Property, 30 Jurimetrics J. 35, 41 (1989).

late 1970's and the early 1980's to make the Betamax the leading format for video cassettes.[23]

In contrast, cooperative standard-setting involves negotiations between different enterprises to reach agreement on one set of issues so these entities can concentrate on competition in other areas. As two economists have observed of such collaborative standard-setting, «[The] process should be thought of as forging an agreement on the rules of play — the size of the playing field, the type of ball used, and so on.»[24] One example of a standards collaboration is the negotiation between Philips Electronics and Sony that led to the still accepted format for CD's.[25] A second example of such collaboration about standards is the current effort by Johnson & Johnson, Eastman Kodak, and Proctor & Gamble to develop uniform security-alarm tags.[26] This trio has formed a consumer products manufacturers' consortium to set out a standardized shoplifting-alarm packaging system for products sold in grocery and drug stores.[27]

Thus, industry self-regulation about privacy is a negotiation about «the rules of play» for the use of personal data. In coming to agreement about these rules, however, companies are likely to be most concerned with one question: what revenues are at stake in the negotiation about standards?[28] The development of standardized formats for CD's increased revenues for hardware manufacturers and software providers by helping convince consumers that these new formats would become widely accepted; as a result, people were more willing to bear the switching costs associated with their adoption of these products.[29] In the case of the consumers products manufacturers' consortium, a standardized anti-theft system will benefit these companies uniformly by reducing losses from shoplifting and the obstruction of brand names by retailers pasting security tags in an ad hoc fashion.[30]

Revenues are also at stake in privacy standard-setting. These revenues are tied to the collection, analysis and sale of the enormous amounts of personal data that individuals generate once online. For the current online industry, moreover, personal information largely has the quality of nonrivalrous consumption, which means that one firm's utilization of it does not leave less for any other company.[31] As a result, almost all major Internet enterprises and computer companies benefit from developing standards, including new technology, that preserve the current status quo of maximum information disclosure.

In this view, unlike the commons of England, personal information cannot be overused and should not bear legal limits that restrict the ability of companies to collect and transfer it as they see fit.[32] Scott McNealy, chairman and chief executive of Sun Microsystems, summed up this aspiration in his blunt statement, «You already have zero privacy — get over it.»[33] This is advocacy masked as description; its purpose, like that of the self-regulation movement, is to promote the financial interest of online business as it is currently configured. Yet, the way in which industry «consumes» personal data has considerable spillover.[34] In particular, promotion of the values of democratic deliberation and individual self-determination require limits on outside access to personal information to stop harms to democratic self-rule and individual self-determination.

The difficulty with self-regulation then is that within the present incentive structure, online industry will use a collaborative standard-setting process to lock-in a poor level of privacy at a societal level. At present, industry action takes precisely this route in proposals that center on two areas: (1) industry-wide privacy codes of conduct for Web sites, and (2) technology that allows individuals to express their privacy preferences in their browser. In both areas, industry plans fall far short of the fair information practices that I have advocated in this Essay.

To begin with the creation of codes of conduct, industry action has generally focused on only two of the four fair information practices that are necessary. The two practices that industry has largely ignored are the need for an effective fabric of obligations, such as data mini-

23 SHAPIRO & VARIAN, supra note 22, at 17.
24 Id. at 306.
25 Id. at 261-62.
26 TARA PARKER-POPE, Consortium to Develop Security Tags for Items Sold in Groceries, Drug Stores, Wall St. J., March 19, 1999, at B3.
27 Id.
28 SHAPIRO & VARIAN, supra note 22, at 293.
29 Id. at 262.
30 PARKER-POPE, supra note 26, at B3.
31 See generally COOTER & ULEN, supra note 11, at 40 («[C]onsumption of a public good by one person does not leave any less for any other consumer.»).
32 On the notion of the overuse of public goods, the so-called «tragedy of the commons,» see ROBERT C. ELLICKSON, Property in Land, 102 YALE L.J. 1315, 1319 (1993); GARRETT HARDIN, The Tragedy of the Commons, 162 Science 1243, 1247 (1968).
33 POLLY SPRENGER, Sun on Privacy: ‹Get Over It›, wired.com 1 (Jan. 26, 1999) <www.wired.com/news/print_version/politics/story/17538.html?wnpg=all>.
34 Spillover or «external» costs cause the individual's self-interest to diverge from social interests. COOTER & ULEN, supra note 11, at 188.

malization, and for limited procedural and substantive rights, such as rights of access and correction. As for the fair information practices that industry emphasizes, it has presented incomplete versions of these two standards and failed to convince Web sites to follow even these weak guidelines.

In place of the full range of fair information practices, industry codes of conduct concentrate on transparent processing systems and the establishment of external oversight. In industry's model of online privacy self-regulation, however, significant problems exist with the initial conception and actual expression of both standards. To begin with transparency, industry views it as fulfilled by incomplete privacy statements.[35] Problems also exist at present with compliance even with this current, stripped-down version of fair information practices. As a result, a thin caricature of transparency is emerging as a cornerstone of industry's preferred mode of self-regulation.

The oversight that industry is proposing is also incomplete and likely to be ineffective.[36] The private sector has been resolute in opposing proposals for a governmental data protection agency; instead, online industry is promoting nongovernmental «seal services» that create «trusted privacy marks» to be placed on the Web sites that make use of them. These kind of Trusted Third Parties differ from infomediaries; where the latter companies seek to stimulate development of a privacy market through development of direct relations with individual consumers, privacy seal companies offer a general branding trade-

35 In particular, the Online Privacy Alliance has emphasized the value of posting of any sort of privacy statement as a means of warding off governmental regulation. It advises Internet companies, «Government officials will be judging how successful self-regulation may be by how many companies have posted privacy policies on their web sites and how many have joined the Alliance and adopted its guidelines.» Online Privacy Alliance, Frequently Asked Questions 2 (visited October 21, 1998) <http://www.privacyalliance.com/facts/>.

36 Moreover, this entire process travels down a path already taken; in «Real Space,» that is, the real world rather than cyberspace, a strong negative example exists of a group of enterprises using the claim of self-regulation to construct a smokescreen of ineffective measures that obscures its true practices. The direct marketing industry has ardently promoted self-regulation; its trade group, the Direct Market Association (DMA), has pointed to an industry code of conduct and a Privacy Task Force as the prime fruits of this self-regulatory effort. Paul Schwartz & Joel Reidenberg, Data Privacy Law 308-309 (1996). It has devoted less publicity to poor industry compliance with this code, including violations of its regulations by at least one enterprise that belonged to the Privacy Task Force. Id. The DMA is now playing an aggressive role in promoting self-regulation in cyberspace. DMA, Welcome to Privacy Action Now! (visited April 1, 1999) <http://www.the-dma.org/pan7/main/shtml>.

mark combined with audit services for companies.[37] A Web site's posting of such a privacy logo on its home page indicates that the site has posted a privacy statement and that the designated privacy seal service will audit compliance by monitoring the companies' data-handling practices.[38] The two leading such Trusted Third Parties are Truste and BBBOnLine.[39]

This approach is promising; its current weaknesses are that the privacy seal companies: (1) are limited in their enforcement powers, and (2) have brands that are not widely recognized at present. These two shortcomings, unfortunately, magnify each other. Should these companies find a violation of a posted privacy practice, their most effective action is forbidding a site from utilizing their respective privacy seal, which individuals will hardly miss. The limited evidence available also suggests that monitoring organizations have been far from aggressive in carrying out their duties. Most privacy violations involving Web sites are brought to public attention by the media and are not followed by a privacy-branding company's decisive enforcement action or revocation of a privacy seal.[40]

Thus, significant shortcomings exist in the first element of industry self-regulation, which is the development of codes of conduct. The second element of industry self-regulation is a technological solution that seeks to allow each person to express the kind of fair information practices that she wishes. Here, the standard-setting process involves not only private corporations but the World Wide Consortium (W3C), a nonprofit institution involved in Internet self-governance.[41] The W3C is developing a Platform for Privacy Preferences (P3P), which is a software protocol for allowing an individual to check whether a Web

37 For a good introduction to the leading privacy seal service, see Truste, Frequently Asked Questions 1 (visited April 9, 1999) <http://www.truste.org/webpublishers/pub_faqs.html>.

38 Id. at 2.

39 BBBOnline began offering its services later than Truste. For information on it, see BBBOnline, The BBBOnline Privacy Program 1 (visited April 9, 1999) <http://www.bbbonline.com/businesses/privacy/index.html>.

40 For a recent incident following this pattern that involves Microsoft, one of the premier sponsors of Truste, see Jeri Clausing, Privacy Watchdog Declines to Pursue Microsoft, a Backer, New York Times on the Web, 1 (March 22, 1999) <http://nytimes.com/library/tech/99/03/cyber/articles/23privacy.htm>; Microsoft Off Trust-e's Hook, wired.com 2(March 22, 1999). <http://www.wired.com/news/print_version/chnology/story/18639.html?wnpg=all>.

41 W3C, Platform for Privacy Preferences (P3) Project (visited March 29, 1999) <http://www.w3.org/P3/Update.html>.

site's privacy practices match her wishes.[42] P3P is to create «a platform on which technical, market and social solutions for protecting privacy on the World Wide Web can be built.»[43] This technological solution follows a path similar to that of the «V-Chip,» a filtering device which Congress has mandated to be built into television sets to allow parents to restrict the kinds of programs to which their children will be exposed.[44]

P3P has great potential to assist in the customization of individual wishes for information privacy. The difficulty, as I have already noted in the context of infomediaries, is that a lock-in of a poor level of privacy is likely to occur around a norm of maximum information disclosure. The use of P3P in the context of this norm of maximum disclosure will permit Web sites to close themselves off entirely to individuals who seek the full range of fair information practices. In other words, those who view the Internet through the filter of privacy-enforcing software may end by placing most of the Web off-limits to themselves. Their Hobson's choice will be sacrificing either their privacy or their access to the Internet.

This analysis indicates that the timing of strategic moves is critical in the development of privacy norms. Technology can play an important role in constituting a multidimensional privacy territory on the Internet. Yet, the contribution of P3P technology will be most effective if made at the time when the data topography of cyberspace is first established. It is particularly troubling, therefore, that P3P's development has not only been slow, but was even stalled for awhile by a dispute about legal rights to the essential underlying intellectual property.[45] Even if P3P is finally made available, cyberspace privacy may have been permanently defined down by that time.

42 Id.

43 Joseph Reagle & Lorrie Faith Cranor, P3P in a Nutshell (visited March 29, 1999) <http://www.w3.org/P3P/nutshell.html>. See also W3C, Platform for Privacy Preferences: P3P Project (visited March 29, 1999) <http://www.w3.org/P3P>.

44 Such filtering technologies require a reduction of a universe of possible preferences to simple standards. J.M. Balkin, Media Filters, The V-Chip, and the Foundations of Broadcast Regulation, 45 Duke L.J. 1131, 1143 (1996). In the case of the V-Chip, for example, the FCC has approved a regulatory scheme in which television programs will be rated as belonging to one of seven categories, ranging from TV-Y (suitable for all Children) to TV-MA (designed to be viewed by adults and, therefore, perhaps unsuitable for children under 17). F.C.C., In the Matter of Implementation of Section 551 of the Telecommunications Act of 1996: Video Programming Ratings, FCC 98-35, CS Docket No. 97-55 (March 13, 1998). P3P is seeking to develop a similar kind of privacy language; here, one proposal is for six pre-configured preference files ranging from «Access all Web sites» to «I want to be close to anonymous.» Joseph Reagle, P3 Prototype Script (Version 3.0 final) (visited November 19, 1998) <http://www.w3.org/Talks/970612-ftc/ftc-mast.html>. Within these six files, more detailed choices will be preset, and an individual will have the possibility to fine-tune these values. Id.

5 The Law's Domain

Both the market and self-regulation have important roles to play in privacy protection on the Internet; yet, reliance on these forces alone will not create effective privacy standards for cyberspace. Fair information practices should be expressed in federal legislation; enactment of this law would be an ideal follow-up to congressional enactment in 1998 of the Children's Online Privacy Act. This legislative imposition of fair information practices for cyberspace will lead to two significant benefits: (1) the prevention of a lock-in of poor privacy standards, and (2) the creation of the preconditions for effective market and self-regulatory contributions to privacy protection.

The timing of strategic moves in the Information Age is critical, and the likely result of delay in the expression of privacy standards will be to lock-in the current privacy horror show in cyberspace. If we wait, American society may follow the path indicated by Scott Nealy and «get over» its loss of privacy on the Internet.[46] This path would be more than unfortunate; privacy rules are a critical means of consti-

45 The patent owner for a filtering technology similar to that of P3P, Intermind, is demanding «licensing fees in the millions of dollars from any company building with P3P.» Chris Oakes, Patent May Threaten E-Privacy, wired.com 1 (Nov. 11, 1998) <http://www.wired.com/news/print_version/technology/story/16180.html?wnpg=all>. A report in the trade press recently quoted one anonymous member of the P3P working group as saying that this controversy surrounding Intermind's patent «has stopped P3P dead in its tracks.» Connie Guglielmo, Will Patent Pose Privacy Problem?, Inter@ctive Week, February 1, 1999, at 36. It is, unsurprising, therefore, that the Microsoft Internet Explorer 5.0, lacks P3P. Id.Some slight positive movement regarding P3P has occured, however, with the release by Microsoft of the «Privacy Wizard.» Chris Oakes, Click Here for a Privacy Policy, wired.com 1 (April 10, 1999) <http://www.wired.com/news/print_version/technology/story/16180.html?wnpg=all>. This software program allows sites to disclose their privacy policies and to have these privacy statements become part of a P3P infrastructure. Id. The modesty of this development is due to the lack of a complete P3P infrastructure; as wired.com explains, «the cart is leading the horse.» Id. at 2.

46 Sprenger, supra note 33, at 1.

tuting both individuals and community. The promotion of cyberspace as a new arena for civic life and the maintenance of a populace capable of self-determination requires the right kind of restrictions on different kinds of access to personal information. Fair information practices, if expressed in law, will be the best first step in establishing the necessary data topography of Internet privacy. This legal expression of privacy norms will also promote democratic deliberation and individual self-determination in cyberspace.

A further benefit of a legislative expression of privacy norms, paradoxically, will be to heighten the effectiveness of the market and self-regulatory mechanisms. The Clinton Administration's policies in this area have largely encouraged a consensus in industry around norms that do not benefit society as a whole. As industry is currently configured, it benefits from standards that: promote maximum disclosure of personal data; establish a poor level of transparency; offer no effective procedural or substantive rights; and establish hollow oversight. In a similar fashion in the past, the legal system's deference to the direct marketing industry's weak code of conduct has permitted it to stave off effective regulation.

A legal expression of fair information practices would create an environmental shock to industry's privacy self-regulatory groups and its current consensus. The legislative enactment of fair information practices would prevent firms from viewing personal data as a public good; instead, companies would be forced to engage in privacy price discrimination. Already, software and other Information Age companies have become highly sophisticated at capturing revenues by customizing their products and services to charge each customer the price that she is willing to pay, and no more.[47] Such price discrimination sometimes takes place by selling to different users at different prices, by letting users choose the version of a product they wish, and by making discounts available to certain groups.[48] Compared to this effort, companies do not generally seek privacy price discrimination because the law, technology, and social practices create an information subsidy in their favor. From this perspective, a legislative enactment of fair information practices would end a socially unproductive subsidy to online industry. In addition, greater industry interest in such Trusted Third Parties as infomediaries and privacy seal organizations is likely to develop.

47 SHAPIRO & VARIAN, supra note 22, at 55-68.
48 Id.

6 Conclusion

The Internet is growing at a rate that outpaces any modern medium for communication.[49] Television took thirty-five years to reach thirty percent of households in the United States; the Internet's World Wide Web («Web») is expected to achieve this degree of market penetration a mere eight years after its popular debut.[50] Indeed, one study predicted that by the year 2000 over 100 million Americans will be «surfing» the Web on a regular basis.[51] This figure represents a seventy-five percent increase.[52] As more Americans go online, this electronic medium is of increasing significance for this country— it is the new arena for public and private life in the United States. Millions of people now seek connections with other individuals in cyberspace through activities that both track real world behavior and assume dimensions unique to this electronic setting.[53]

This essay advocates a legislative enactment of fair information practices. This legal expression of privacy norms is the best first step in promoting democratic deliberation and individual self-determination in cyberspace. It will further the attainment of cyberspace's potential as a new realm for collaboration in political and personal activities. Enactment of such a federal law would be a decisive move to shape technology so it will further – and not harm – democratic self-governance.

Bibliographical references

See footnotes.

49 See U.S. DEPT. OF COMMERCE, The Emerging Digital Economy 4 (1998) («The Internet's pace of adoption eclipses all other technologies that preceded it.»).
50 PAINEWEBBER, Converging Technologies: Investing in the Information Age for the New Millennium 9 (1998).
51 PERRY H. ROTH, Internet Industry, Value Line, March 5, 1998, at 2228.
52 Id.
53 For descriptions of some of the myriad forms of online behavior, see Reno, 117 S.Ct. 2329, 2343-45 (1997); SHERRY TURKLE, Life on the Screen 186-209 (1995).