NORM PROSELYTIZERS CREATE A PRIVACY ENTITLEMENT IN CYBERSPACE

By Steven A. Hetcher[†]

ABSTRACT

This article explores an important development in the informal regulation of online privacy. Privacy norm proselytizers have been the leading contributors toward the recognition by Internet users of a moral entitlement to privacy in cyberspace.

This article begins by examining the non-moral social meaning of the original personal data collection practices that emerged at the World Wide Web's inception in the early 1990s. Next, it analyzes methods by which privacy activists endeavored to moralize the social meaning of online data collection. It also emphasizes that other norm entrepreneurs, namely, the Federal Trade Commission and creators of new software privacy solutions, have subsequently supported an entitlement to privacy for reasons less selfless, but no less efficacious, in terms of helping to stimulate demand for increased privacy protections. The article concludes that even though a grundnorm of respect for consumer data privacy has generally emerged in American culture, American society is only at the beginning of the difficult task of incorporating this grundnorm into its social and business practices.

I. INTRODUCTION

This is not cattle.
This is a human being.
We do not spam human beings.
We respect human beings.
Respecting human beings is good business.

---

† Associate Professor of Law, Vanderbilt University School of Law. I am grateful for comment from Robert Ellickson, John Goldberg, Mark Lemley, Eric Posner, Bob Rasmussen, Randall Thomas, Bob Thompson, and Chris Yoo. I wish to thank the members of my Spring 2001 Law of Cyberspace course at Vanderbilt Law School, where many of the ideas in the article were first explored. I am especially grateful for the expert research assistance of Janet Hirt, Steve Jordan, Tatjana Stoljarova, and Angela Vitale.

-This is the code.[1]

Over the past few years, the norms governing personal data interactions between consumers and websites have changed dramatically. There is an increasing moral sensitivity regarding the commercial collection and use of personal data.[2] The social meaning has changed from a morally-neutral to a morally-charged status.[3] Consumers now perceive a general right to privacy in cyberspace that includes respectful treatment of personal data. This change arose not by accident or necessity, but from the intentional actions of actors possessing an interest in promoting online privacy. I will designate these actors as privacy norm proselytizers and privacy norm activists.[4]

---

1. Netcreations, Inc., Advertisement, INDUSTRY STANDARD, Jul. 10-17, 2000, at 150-51.

2. The connection between the collection of personal data and personal privacy is straightforward; the more personal data that websites collect, store, and use, the less privacy that data subjects have. *See* A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1465 (2000); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1283-1286 (2000). There are two broad categories of personal data: information that can be used to identify consumers (personal identifying information: including name, postal or e-mail address) or demographic and preference information (including age, gender, income level, hobbies, or interests). The latter can be used either in aggregate, non-identifying form for purposes including market analysis, or in conjunction with personal identifying information to create detailed personal profiles. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 20 (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter 1998 FTC REPORT TO CONGRESS].

3. *See, e.g.*, *The End of Privacy*, THE ECONOMIST, May 1, 1999, at 21; Rep. Asa Hutchinson and Rep. Jim Moran, *Industry Needs to Take the Lead on Protection,* ROLL CALL, Jul. 10, 2000, *available at* 2000 WL8734799; Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 182; Jared Sandberg, *Losing Your Good Name Online*, NEWSWEEK, Sept. 20, 1999, at 56 (describing the "alarming prospect" of identity theft—"the worst kind of privacy violation"); Celia Santander, *Web-Site Privacy Policies Aren't Created Equal*, WEB FIN., Dec. 11, 2000. Opinion polls show increasing public concern with respect to online privacy. *See infra* note 155.

4. Norm entrepreneurs are actors who promote the change of norms. Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909 (1996). Norm proselytizers promote norms for moral reasons which they themselves accept. Norm proselytizers, then, are a sub-category of norm entrepreneurs. Privacy activists have functioned as norm proselytizers. Robert Ellickson seeks to develop a richer vocabulary by distinguishing among a variety of specialists who supply new norms. *See* Robert Ellickson, *The Market for Social Norms*, 3 AM. LAW & ECON. REV. at 10-12 (2001). "Change agents" are actors or enforcers who are relatively early in supplying a new norm. *Id.* He distinguishes among these subcategories of change agents: self-motivated leaders, norm entrepreneurs, and opinion leaders. *Id.* The following discussion will indicate that these

Social meanings attach to social norms; one method of changing social norms is to alter their social meanings.[5] For example, changing the social meaning associated with smoking is one way to regulate cigarette smoking among teens. As long as smoking retains a cool and rebellious mystique, it will be difficult to eradicate the practice.[6] Analogously, privacy norm proselytizers are in the process of changing the social meaning associated with websites' collection and use of personal data.[7]

---

subcategories may be aptly applied to norm creation in cyberspace. In addition, I will suggest that the norm proselytizer is aptly viewed as a distinct type of change agent.

5. *See* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 951 (1995) ("Any society or social context has what I call here social meanings—the semiotic content attached to various actions, or inactions, or statuses, within a particular context."); Steven A. Hetcher, Norms (1991) (unpublished Ph.D. dissertation, University of Illinois) (on file with author) (defining a social norm as a pattern of rationally or morally governed behavior maintained in a community by acts of conformity). *But see* Sunstein, *supra* note 4, at 914 (defining social norms as "social attitudes of approval and disapproval, specifying what ought to be done and what ought not to be done"). Judge Richard Posner views law and norms theory as second-generation law and economics. *See* Richard A. Posner, *Social Norms, Social Meaning, and Economic Analysis of Law: A Comment,* 27 J. LEGAL STUD. 553 (1998). Ellickson views law and norms as representing a new paradigm within the traditional law and economic approach. *See* Robert C. Ellickson, *Law and Economics Discovers Social Norms,* 27 J. LEGAL STUD. 537 (1998). Social norms theory has been the subject of a number of important recent symposia. *See* Symposium, *The Informal Economy*, 103 YALE L. REV. 2119 (1994); Symposium, *Law, Economics, and Norms*, 144 U. PA. L. REV. 1643 (1996); Symposium, *Law and Society & Law and Economics*, 1997 WIS. L. REV. 375 (1997); Symposium, *The Legal Construction of Norms*, 86 VA. L. REV. 1577 (2000); Symposium, *The Nature and Sources, Formal and Informal, of Law*, 82 CORNELL L. REV. 947 (1997). Recent law and norms literature has included a number of significant case studies. *See, e.g.,* Lisa Bernstein, *Merchant Law in a Merchant Court: Rethinking the Code's Search for Immanent Business Norms,* 144 U. PA. L. REV. 1765 (1996); Robert Cooter & Janet T. Landa, *Personal Versus Impersonal Trade: The Size of Trading Groups and Contract Law,* INTL. REV. L. & ECON. 15 (1984); Richard H. McAdams, *Cooperation and Conflict: The Economics of Group Status Production and Race Discrimination*, 108 HARV. L. REV. 1003 (1995); Mark D. West, *Legal Rules and Social Norms in Japan's Secret World of Sumo*, 26 J. LEGAL STUD. 165 (1997). None of these case studies, however, has applied law and norms methodology in an online context.

6. *See* Lessig, *supra* note 5, at 950-52.

7. On some accounts, this process may come too late. In a now famous remark, the CEO of Sun Microsystems, Scott McNealy, advised the public, "[y]ou already have zero privacy—get over it." John Markoff, *Growing Compatibility Issue: Computers and User Privacy,* N.Y. TIMES, Mar. 3, 1999, at A5. McNealy's remark is self-serving, given that it was made at the launch of Jini software, which raised privacy concerns because it enabled all electronic devices to interconnect using an identification number. *Id.* One can imagine McNealy making a statement similar to that quoted above, albeit toned down in its rhetoric, as a defendant in a civil suit, or as a witness in a congressional hearing, with

The set of normative concepts that increasingly surround the practice in popular discourse is evidence that consumers are developing a more complex normative understanding. Notably, interactions between websites and their visitors are now framed in terms of privacy. Privacy is among the most potent normative concepts of the modern age.[8] Proponents of personal data privacy have won a substantial victory now that data is widely understood to raise concerns for a new species of privacy: informational or data privacy. Not long ago, these expanded privacy concepts did not exist in either popular discourse or the moral theory lexicon.

Privacy is generally conceptualized as a right.[9] In ordinary moral understanding, rights function differently than preferences. Our preferences do not imply the existence of desired rights. By contrast, we have rights even if we do not prefer to exercise them. This is true for many individuals regarding their right of religious expression. While they may have no desire to express their religious views, they may nevertheless place value in their right to do so. So, too, with personal data. Although many people may not desire to actively control their personal data online, they may nevertheless be inclined to support such a moral entitlement.

Increasingly, a consumer's entitlement to control his or her personal data is generally recognized.[10] Where does this growing sense of entitle-

---

the implicit message that if privacy is gone already, Sun Microsystems cannot be accused of its further degradation.

8. *See, e.g.*, A. S. Berman, *Reports of Gates' Death Greatly Exaggerated*, USA TODAY, Apr. 5, 2001, at 3D (noting that Microsoft spokesperson Beth Jordan stated, "[t]here's nothing more important to Bill [Gates] than the privacy of his family and children."); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 179 (1999) ("Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century." (quoting Marc Rotenberg)).

9. *See infra* note 69; *see also, e.g.*, Louis D. Brandeis and Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Simon G. Davies, *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 144 (Philip E. Agre & Marc Rotenberg eds., 1997) (noting a change in society's approach from privacy protection to data protection); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497-498 (1995) (arguing that a citizen's right to participate in government depends "on the ability to control the disclosure of personal information"). Some European Union Parliament and Council Directives dealing with privacy are based on a conception of personal data protection as a fundamental civil liberty interest. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

10. Paul Davidson, *Marketing Gurus Clash on Internet Privacy Rules*, USA TODAY, Apr. 27, 2001, at 1B ("'Such a system recognizes a 'subtle but important shift' in direct marketing,' says Hans Peter Brondmo, founder of Netcentives, an opt-in e-mail firm.

ment come from? It is primarily due to the efforts of privacy norm entrepreneurs proselytizing to consumers regarding their entitlement to control over personal data.[11] The word "proselytize" is appropriate because it would be unhelpfully reductionist to describe these entrepreneurs as merely fostering preferences for data privacy in the manner that Madison Avenue seeks to create preferences. Instilling a sense of moral entitlement to data privacy is fundamentally different from instilling a preference for Coke over Pepsi. Privacy norm proselytizers seek to arouse the moral consciousness of consumers *vis-à-vis* websites' collection and use of their personal data.[12]

As consumers increasingly perceive an entitlement, there is a corresponding tendency for them to feel moral outrage at websites that fail to respect data privacy. In terms of the emerging moral framework for governing online personal data, websites ought to respect the data privacy entitlements of consumers.[13] Websites that do so may earn the trust and confidence of consumers.[14] Consumers who feel that they are disrespected,

---

'Companies used to think of customer data as theirs. They're starting to realize they're really custodians, and the customer controls the information.'").

11. Matt Richtel, *When Computers Know What a Stranger Can't*, N.Y. TIMES, Mar. 12, 2000, at C9. Marc Rotenberg "believes that Web sites should make clear what information they are capturing and give users a clear option to decline to participate." *Id.*

12. Traditional economic analysis has shied away from the topic of preference formation. This is changing, however. *See* GARY S. BECKER, ACCOUNTING FOR TASTES 3 (1996) (noting in his study of individual preferences that "preferences or tastes play a crucial part in virtually all fields of study in economics . . . . [b]ut with few exceptions, economists and political scientists pay little attention to the structure of preferences"); *see also* JON ELSTER, SOUR GRAPES (1983).

13. Jeri Clausing, *Can Internet Advertisers Police Tthemselves? Washington Remains Unconvinced*, N.Y. TIMES, June 14, 2000, at C10 (reporting that Marc Rotenberg, director of the Electronic Privacy Information Center stated "Internet users should be able to have their profiles deleted upon request"); David Cohen, *Be sure you never take a cookie from strangers*, THE GUARDIAN (London), Apr. 1, 2000, at 22 ("Some of the UK's popular internet banks are eager to point out their respect for customer privacy. 'We do not passively track visitors to our website,' says Richard Thackray, UK country manager for first-e. 'Once a customer is signed up, we keep records of all communications and may use the information for special offers, but we don't trade customer information without their prior consent.'"); Rep. Edward J. Markey, *We must act soon to protect online privacy*, THE HILL, Feb. 7, 2001 ("I believe that Congress must enact meaningful privacy protections to reflect the fundamental value that the overwhelming majority of Americans place upon this core element of freedom.").

14. *See* Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1.

> That's not to say that L. L. Bean executives think that people are ready to give up their privacy. To the contrary, L. L. Bean believes that, as always, people are willing to share private information with

however, may seek to punish websites by taking their business elsewhere, reciprocating the disrespect by providing the website with false personal information,[15] or sanctioning the website through negative gossip.[16]

Commercial websites are profit-maximizing entities, and thus morality has no intrinsic relevance for them. Nevertheless, they must engage in interactions with consumers who do have complex moral psychological states. Woe be unto the website that blithely carries on as if consumers merely have a preference for data privacy in the same manner they have a preference for, say, price discounts or free gift-wrapping.[17] Thus, while

---

> those they trust, and it believes that it has its customers' trust. The company may be right. It reports that customers love the convenience. In fact, one recent caller was so charmed by the personal treatment that she thought the saleswoman recognized her voice. "That's a trusting relationship with that business," said Marc Rotenberg, executive director of the Electronic Privacy Information Center, a privacy advocacy group in Washington. Mr. Rotenberg said L. L. Bean's customers had faith that the company would not abuse the information by reselling it.

Id.

15. *See* George R. Milne, *Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue*, 19 J. PUB. POL'Y & MKTG. 16, 16 (2000). Milne succinctly summarized several studies: "When Web sites require consumers to provide information to register, many consumers provide false information. Surveys report that half the Internet users report false information about a quarter of the time." *Id.* (citation omitted). *See also* Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 664-65 (1999) (citing a Boston Consulting Group consumer study stating that "40% of Internet users have provided false information at least once when registering at a website"); Jerry Guidera, *Online Shoppers Often Lie To Guard Privacy, Survey Says*, WALL ST. J. EUROPE, Mar. 16, 2000, at 28.

16. ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 213-14 (1991).

17. *See The Internet's Chastened Child*, THE ECONOMIST, Nov. 11, 2000, at 80. Kevin O'Conner, founder of DoubleClick, lost his job due to his insensitivity to the issue of privacy:

> Consumer watchdogs were slow to grasp the implications of the Abacus deal—and of the fact that, in its wake, DoubleClick had quietly dropped from its website its pledge to keep users' data completely anonymously. But they woke up in January when the company announced that it had created profiles of 100,000 individual surfers and was planning to sell them to advertisers. The resulting outcry triggered an FTC probe into whether DoubleClick had engaged in deceptive trade practices, leading to a 25% drop in the group's shares in a single day and eventually, to a pledge that it would not sell the profiles after all. DoubleClick's subsequent promise not to integrate its own database

websites are not themselves moral, they may nevertheless need to address moral concerns to effectively interact with consumers. They may even hire a morally-oriented executive: a Chief Privacy Officer.[18]

It may appear naive to assume that consumers could have a pseudo-moral relationship with a distant, uncaring, and profit-maximizing website. In other areas, however, the law is available to create relationships that simulate moral relationships: this is the notion of the fiduciary. Ideally doctors, lawyers, and accountants would legitimately care about their clients' well-being. At the very least, their clients expect and pay for these professionals to act as though they care. The reason clients may trust their fiduciaries to take their interests to heart is that this is part of their contractual agreement. Similar relationships may potentially be achieved via informal social norms rather than formal legal structures. We may be moving into a world where this occurs with respect to the relationships between websites and their visitors. Many websites now expressly promise to respect their users' privacy in statements loaded with moral language. This moral language arguably creates consumer expectations that may subsequently be interpreted as constituting special, legal relationships.

Among the strongest privacy guarantees are those found on financial services firm websites. Citigroup states that it is "committed to the Citigroup Privacy Promise for Consumers."[19] Note that Citigroup designates its assertions as a promise. Other websites typically entitle their commitments as a privacy "statement" or "policy."[20] The risk of making such statements is having the language used adversely against the firm should litigation ensue. Citigroup likely calculated that the positive value of the moral language offset the potential risk. The Citigroup Privacy Promise

---

> fully with that of Abacus turns the acquisition, in the eyes of many, into a monumental flop.

Id.

18. *See* John Schwartz, *First Line of Defense, Chief Privacy Officers Forge Evolving Corporate Roles*, N.Y. TIMES, Feb. 12, 2001, at C1 (explaining that lawyers are good at making sure that a company complies with privacy laws "but being a chief privacy officer is a lot more than simply compliance. 'You have to have a fundamental commitment to—dare I say it?—morality.'"); *see also* David Bicknell, *Directors Face E-Laws Overload*, COMPUTER WKLY., Feb. 24, 2000, at 16 (stating that the burdens of complying with European privacy policies has led some companies to be pro-active and engage in "self-help" through "privacy specialists").

19. *See* Citigroup Privacy Promise, *at* http://www.citibank.com/privacy (last visited Sept. 4, 2001) [hereinafter Citigroup Privacy Promise].

20. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 823 (2000) (noting that a privacy policy is a document that is often accessed through a hypertext link on a homepage which spells out how it collects and uses personal information).

contains additional language that would be useful to a plaintiffs' class action attorney in arguing that a legally enforceable promise was made.[21]

The legal enforceability of privacy policies is currently an unsettled area of the law.[22] Some websites claim that users who use the website agree to the terms of the website.[23] This language may promote contractual interpretations of the privacy statement. Others expressly disavow any contractual reading of the document.[24] Even if not contractually interpreted, these promises may still have legal significance. The Federal Trade Commission ("FTC") has used its jurisdiction to regulate unfair and deceptive trade practices by prosecuting failures to comply with the terms of privacy policies.[25] Websites' representations may arguably create privacy expectations such that promiscuous uses of customer data are tortious.[26] More generally, Congress has regulated particularly sensitive categories of personal information, including medical and financial data and information collected from children.[27] The more websites treat all consumer personal data in a similar fashion under their privacy policies, the more they

---

21. The Citigroup Privacy Promise reads: "our most important asset is our customers' trust. Keeping customer information secure, and using it as our customers would want us to, is a top priority for all of us at Citigroup." Citigroup Privacy Promise, *supra* note 19. It later states: "We will continuously assess ourselves to ensure that customer privacy is respected." *Id.* In the space of a one-page privacy statement, then, this document uses the normatively-loaded terms, "promise," "trust," and "respect." *Id.*

22. Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 588 (2001).

23. *See* http://www.jcrew.com (last visited Sept. 4, 2001) ("By visiting jcrew.com you are accepting the practices described in this privacy policy.").

24. *See* http://www.weather.com (last visited Sept. 4, 2001) ("This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights.").

25. *See infra* note 31; Steven A. Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2056-59 (2000).

26. The tortious relationship between the parties is expressed in terms of unfair competition and breach of confidentiality. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1154-57 (2000).

27. Nina Bernstein, *Welfare Officials to Search Records Of Drug Treatment*, N.Y. TIMES, Sep. 25, 1999, at A1 ("Marc Rotenberg, executive director of the Electronic Privacy Information Center, a civil liberties advocacy group based in Washington, said: 'Welfare recipients are among the first to lose their privacy. But the unfortunate consequences of these tracking and matching technologies tend to make their way up the line.' A Federal law passed in the 1970's makes it a crime, with few exceptions, to disclose information about patients in drug and alcohol treatment programs without the patients' narrowly defined written consent. That consent does not allow re-disclosure for any other purposes. Experts on privacy law call the measure unique and exemplary, and contrast it to the blanket consent forms allowed in the gathering of other types of health care information."); Hafner, *supra* note 14, at G1.

invite Congress to formally treat all personal data on par with the most sensitive categories.

Why would websites expose themselves to potential liability and increased prospective regulation? In other words, what economic forces have fostered a situation where websites are the dominant suppliers of more respectful Internet privacy norms? What benefits do they receive as suppliers of these norms that have caused them to assume the costs associated with their supply? This Article addresses these questions and examines the role of privacy norm proselytizers in changing the social meaning of data collection. These changes in social meaning have increased consumer demand for privacy and, correspondingly, website supply.

This Article will first examine the original data-collection practices that emerged at the World Wide Web's inception in the early 1990s. The social meaning of these practices was non-moral. Websites benefited through the largely unrestricted collection of personal data while consumers absorbed a third-party externality in the degradation of their personal privacy.[28] These practices emerged as the first norms of online data collection. This Article will analyze the strategic relationship structures among actors that allowed these permissive norms to flourish. The persistence of these norms created a norm gap between the actual practices and the practices norm proselytizers judge to be preferable.[29]

This Article will further examine methods by which norm proselytizers endeavored to moralize the social meaning of online data collection to close this norm gap. These privacy proselytizers precipitated a norm cascade toward more respectful privacy norms.[30] Following in their wake, other norm entrepreneurs promoted the emerging moralized data norms. This Article will conclude by examining the activities of two of these new entrepreneurs—the FTC and creators of new software privacy solutions.

---

28. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998).

29. Stephen Labaton, *U.S. Is Said to Seek New Law to Bolster Privacy on Internet*, N.Y. TIMES, May 20, 2000, at A1. ("'The bottom line is that the privacy gap between the safeguards in place and the intrusions seems to be growing not narrowing . . .' said Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology.").

30. Sunstein, *supra* note 4, at 909 (stating that a norm cascade is a rapid shift in norms, perhaps as a result of fragile social conditions); *see also* Randal C. Picker, *Simple Games in a Complex World: A Generative Approach to the Adoption of Norms*, 64 U. CHI. L. REV. 1225, 1227-28 (describing the function of the law in "norm seeding," which is the idea that norms adopted by a small group of people may produce a norm cascade, such that the norm spreads throughout society and replaces old norms).

The current situation is far from ideal, as many websites have failed to adopt more respectful privacy practices. Other firms have endorsed such practices in word but not deed, either by posting deceptive privacy policies, or regularly violating the terms of their posted policies.[31] On the whole, improvements in consumer/website interactions have been realized. Through the efforts of norm proselytizers, a grundnorm of respect for consumer data privacy has generally emerged in American culture.[32] American society is only at the beginning of the difficult task of incorporating this grundnorm into its social and business practices.

II. THE NON-MORAL SOCIAL MEANING OF EARLY WEBSITE DATA COLLECTION

The social meaning of the initial website data-collection practices was morally neutral. The mainstream participants, the websites and their visitors, did not perceive moral claims as generated by the data-collection activities of websites. The original data-collection practices that emerged in the early, unrestrained Internet environment are described in section A. Section B discusses how these practices evolved into the permissive norms that characterized the early website industry. These norms strongly favored the interests of the website industry over the interests of consumers. As a result, a norm gap existed between the actual practices and those practices that leading norm proselytizers viewed as justified. Section C considers the normative characteristics of these permissive practices. Finally, section D utilizes informal game theory methods to model the strategic structures of early website practices. This analysis will demonstrate why the early norms were resistant to change through industry self-regulation, and hence why the norm gap persisted.

A. Initial Data-Collection Practices of the Nascent Website Industry

The Internet was initially developed in the 1960s by government-funded engineers working in American universities. This effort was one small part of the U.S. government's Cold War strategy.[33] In this early period, Internet use was mainly by academic researchers working in com-

---

31. For example, in bankruptcy proceedings, Toysmart.com recently moved to sell personal data it had collected pursuant to a specific privacy guarantee. *See infra* note 169.

32. A grundnorm is a basic norm. *See* John R. Carnes, *Why Should I Obey the Law*, 71 ETHICS 14, 19 (1960).

33. STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 92 (1998).

mon disciplines.[34] In Robert Ellickson's terms, these were "close-knit" groups, as the members were relatively small in number and engaged in overlapping, multiplex interactions.[35] As members in such "close knit" communities are typically able to sanction perceived inappropriate behavior, there are internal incentives to deter opportunistic behavior.[36]

This situation changed due to two developments: the invention of the World Wide Web[37] and the commercialization of cyberspace. Once the core features of the Web were in place, the Internet became easier to use

---

34. *Id.* at 99-117.

35. *See generally* ELLICKSON, *supra* note 16. These researchers might see each other at conferences; they might be former classmates, or share advisors or mentors; or they might wish to seek future employment at one another's institutions. Accordingly, there would often exist ample opportunities to sanction non-cooperative behavior, or reward cooperative behavior. Listservs such as *The Well* are of interest in this regard. *The Well* was pre-Web and non-commercial. In addition, many of its members were part of a relatively close-knit community, the Bay Area Internet *cognoscenti*. *The Well* nevertheless allowed members to interact anonymously if they wished. Predictably, serious problems arose with the community under conditions of anonymity. *See* ESTER DYSON, RELEASE 2.0 46, 217 (1998).

36. *See* ELLICKSON, *supra* note 16, at 177-79. Based on empirical studies of ranching and farming communities in Northern California, Ellickson developed the hypothesis that efficient norms will emerge in "close-knit communities." *Id.* These norms will serve as solutions to the iterated "collective-action problems" faced by the group. *Id.* at 177. The apparent implication is that website privacy norms are inefficient if they are the product of communities that are not close-knit. Thus, while these norms are indeed rapidly emerging, there is reason to fear that they may not be moving toward greater efficiency because the Internet would appear not to be close-knit. *See* Reno v. ACLU, 521 U.S. 844, 851 (1997) ("Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."); Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) ("Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet."); Dan L. Burk, *Trademark Doctrines for Global Electronic Commerce*, 49 S.C. L. REV. 695, 716 (1998) ("Notwithstanding that the Internet is and will be segmented by economic, social, and technological divisions, those divisions will not necessarily map onto the geographic, political, and economic divisions already existing offline . . . . the current technological structure of the Internet . . . ignores customary political and geographical boundaries on which much of our legal system is based."); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1276-77 (1998) (expressing skepticism that Internet norms are efficient).

37. The Web is that portion of the Internet that runs Hyper Text Transfer Protocol ("HTTP"), Transmission Control Protocol/Internet Protocol ("TCP/IP") and utilizes Uniform Resource Locators ("URLs"). *See generally* TIM BERNERS-LEE, WEAVING THE WEB (1999).

and websites proliferated.[38] As commercial websites have been the main actors in the collection and use of personal data, the commercialization of cyberspace precipitated the current concerns regarding online privacy.[39]

Early commercial websites gathered consumers' personal data either by explicitly requesting it or simply taking it. Many websites conditioned access to their websites on the provision of personal data from visitors. In other instances, consumers received discounts, coupons, or free contest entries as an inducement to provide personal information.[40] Significantly, websites deployed new technologies that vastly improved their ability to collect data from visitors. Most significant has been the development of cookies, which allow a website's server to place information about previous visits on the consumer's computer in a text file that only the server can read.[41] From the website's perspective, cookies had the distinct advantage that typical consumers were unaware that their personal data was being gathered.[42]

When using cookies, a website assigns each consumer a unique identifier,[43] so that the consumer may be recognized in subsequent visits to the

---

38. Early websites were not commercial in nature, as the National Science Foundation did not allow such activity. *See* SEGALLER, *supra* note 33, at 224-25. The Web was not available to private enterprise until the Bush Administration zoned cyberspace for commercial use. *See id.* at 297.

39. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 40.

> While American businesses have always collected some information from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns.

Id. Increasingly, however, privacy concerns have arisen regarding data collection by nonprofit sites as well. *See* Ellen Almer*, Online Therapy: An 'Arms Length Approach,* N.Y. TIMES, Apr 22, 2000, at A1.

40. Matthew L. Wald, *Pay-As-You-Go Plan For Car Insurance*, N.Y. TIMES, Dec. 22, 2000, at F1 ("'Privacy has increasingly become sort of a premium,' Mr. Rotenberg said. 'Increasingly people will be required to give up information to obtain a good deal.'").

41. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 45 n.4; Stacee Barcelata, *How Cookies Work* (Aug. 31, 2001) *at* http://www.zdnet.com/zdhelp/stories/main/0,5594,916619,00.html.

42. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 34-42 (1999).

43. Generally, a unique identifier is connected to the machine and not to a named individual. The problem is that this is a small gap to bridge. Consequently, privacy advocates have been concerned about unique identifiers even when connected to machines and not individuals. *See, e.g.*, *Oversight Hearing on Electronic Communications Privacy Policy Disclosures Before the House Committee on the Judiciary*, *Subcomm. on Courts and*

website.[44] This allows the website to obtain consumer-specific information on each subsequent return visit to its website. Websites are most interested in gathering consumer preference or interest information, as indicated by previously accessed web pages, downloaded information, or items the user previously clicked on.[45] Once firms collect personal data, they may then aggregate it or sell it to aggregating firms that maintain databases containing profiles of named individuals.[46] With this data, online companies can individually target products and services that are tailored to consumer preferences.[47] Cookie use is rising and firms are developing more sophisticated means of data gathering.[48] Personal data is quickly becoming an important commodity.[49]

Intellectual Property, 106th Cong. 78 (1999) (testimony and statement of Marc Rotenberg, Director Electronic Privacy Information Center). Recently, both Intel and Microsoft have made efforts to tie numbers to names. *See* Edward C. Baig, *Privacy: The Internet Wants Your Personal Info. What's In It for You?*, BUS. WK., Apr. 5, 1999, at 84; Don Clark & Kara Swisher, *Microsoft to Alter Windows 98 so Data About Users Won't Be Sent to Company*, WALL ST. J., Mar. 8, 1999, at B16; Robert Lemos, *The Biggest Computer Bugs of 1999!*, ZD INTERNET MAGAZINE, Dec. 23, 1999, *available at* 1999 WL 14538475 (discussing Intel's Pentium III serial number, global unique identifiers, and two Microsoft products, Office 97 and Windows 98, that attempted to match various numbers to personal information and names).

44. An industry has emerged to market a variety of software products designed to assist websites in collecting and analyzing visitor data and in providing targeted advertising. *See, e.g.*, Thomas E. Weber*, Software Lets Marketers Target Web Ads*, WALL ST. J., Apr. 21, 1997, at B1.

45. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 45-46.

46. *See* Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 COMPUTER LAW 7 (May 1999) (noting that commercial activity involving personal data is growing at rapid pace).

47. *See* Froomkin, *supra* note 2, at 1469. For example, a firm named Acxiom currently holds personal and financial information about nearly all U.S., U.K., and Australian consumers. *Id.* at 1473-74.

48. *Id.* at 1487 ("Cookies, however, are only the tip of the iceberg. Far more intrusive features can be integrated into browsers, into software downloaded from the Internet, and into viruses or Trojan horses. In the worst case, the software could be configured to record every keystroke." (citations omitted)); Free On-Line Dictionary Of Computing, *at* http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=trojan+horse (last visited Sept. 2, 2001) (defining a trojan horse as a "malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or . . . a program . . .").

49. The term "commodification" is not inherently pejorative. Whether, and to what extent, the commodification of personal data is a negative development depends on one's normative theory. For instrumentalist theories generally, and economic analysis in particular, "commodification," *per se*, has no *sui generis* moral meaning. The core idea of this type of normative framework is that all things of value may be put on a single scale. Thus, to commodify data, or anything else, is not to change its moral status. In fact, eco-

B. Normative Features of Unregulated Data-Collection Practices

The previous section provided a description of the initial data-collection practices of the website industry. This section begins the examination of identity theft, medical data exploitation, and data collection from children from a normative perspective.[50]

As a descriptive matter, people are normative beings. Not surprisingly, human practices and institutions have normative features. This is true of the emerging practices regarding the collection and use of personal data by websites. The unregulated website practices described in the previous section may be characterized in terms of the following normative propositions.[51]

Permissive Data-Collection Norms

1) Websites felt free to gather as much personal data as desirable from consumers.

2) Websites did not feel obligated to ask permission to gather personal data.

3) Websites did not feel obligated to inform consumers when their personal data was gathered.

---

nomic theorists may view commodification as an instrumental good, as commodifying data may promote efficiency by allowing this data to more easily reach the hands of those who will value it most. For some versions of deontological theory, on the other hand, personal data may not morally be made the subject of market exchanges. *See* Samuelson, *supra* note 26, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."). *See generally* Pamela S. Karlan, *Not By Money But By Virtue Won? Vote Trafficking and the Voting Rights System*, 80 VA. L. REV. 1455 (1994) (explaining rationale for public policies against vote trafficking). This type of deontological theory is not the type that is implicit in most discussions of online privacy, however. Most deontologically-oriented discussions of privacy implicitly accept the notion that under proper conditions, such as when there is informed consent, a data subject may morally alienate personal data in a market exchange. *See generally* Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace,* 73 CHI.-KENT L. REV. 1295 (1998).

50. This does not mean a critical normative perspective, however. I will not seek to provide arguments regarding what I take to constitute the correct or true moral analysis of norms of Internet privacy. Instead, I will engage in what I take to be a form of social science. Similarly, H.L.A. Hart took himself to be engaging in "descriptive sociology" in THE CONCEPT OF LAW. *See generally* H. L. A. HART, THE CONCEPT OF LAW (2d ed. 1994).

51. Websites might plausibly have thought their behavior was acceptable for a couple of reasons. First, personal data is in the public domain and so available for all to use, and second, consumers benefited from the personalized marketing possibilities available as a result of the increased commercial flow of data.

4) Websites felt free to place cookies on consumers' hard drives.

5) Websites felt free to use personal data in any manner they preferred, including selling or licensing this data to third-parties.

6) Websites did not feel obligated to monitor or regulate how these third-parties used consumer data they supplied.

7) Websites did not feel obligated to allow consumers access to their data.

8) Websites did not feel obligated to provide security for personal data in their possession.

The website industry did not highlight the fact that these norms characterized its relationship with consumers and their personal data. Websites acted in ways that established these norms because it was legal and profitable to do so.[52] These practices did not reflect the websites' desire to establish socially justified patterns of obligatory behavior.[53] Accordingly,

---

52. ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 3-4 (1994).

> A great deal of information we consider to be highly personal, and of interest to ourselves and the town gossip—our names, telephone numbers, marital status, educational accomplishments, job and credit histories, even medical, dental, and psychiatric records—is now being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. These transactions usually take place without our knowledge or consent.

Id. Commercial websites behave in this morally dubious, but commercially reasonable manner for two reasons. First, personal data is not owned and hence it is not unlawful to collect it without consent, and second, in the emerging digital economy, personal data is becoming increasingly valuable. *See* Kathryn Kranhold & Michael Moss, *Companies Are Refusing to Share Their Cookies Tracking Devices, Consumer Data Is Too Precious*, CHI. TRIB., Apr. 10, 2000, at 11 (discussing how large Fortune 500 companies are protecting online tracking devices from Internet advertising companies because consumer data is a veritable "gold mine"); *Online Privacy*, BUS. WK., Mar. 20, 2000, at 82 (comparing the stockpiles of information to an Internet gold rush). *But see* Melissa Preddy, *Metro Teenagers Take Bait, Hook Prize on the Net—They Yield on Privacy in Bid for College Cash,* DETROIT NEWS, June 15, 2000, at 1 (profiling websites that entice Internet users to give up personal information, which on the Internet is regarded as "gold dust," for money and rewards).

53. Because social justification was not a factor, it served the website industry's interests that these norms in general remained unarticulated. This highlights the fact that norms, at their core, are patterns of behavior, not rules, statements, or other linguistic entities. A norm need not be expressed in linguistic terms in order to have content, whereas a rule is by definition linguistic. A norm's content is defined in terms of its strategic structure. A norm, then, is behavior of a certain sort, which may or may not have an

the above may be characterized as constituting the permissive norms of the early website industry which created freedom and did not impose obligations or constraints on the individual website conformers.[54]

The result of the previous data-collection norms was that consumers were adversely affected in many ways. One of the most concerning activities, data collection from children, has already prompted the enactment of the Childrens' Online Privacy Protection Act ("COPPA").[55] While COPPA has reduced the amount of data collected from children, there is evidence that these activities still persist. For example, the ToySmart.com plan to sell its database containing children's personal information, contrary to its previous explicit promises, brought it under FTC scrutiny.[56] Once the FTC was involved, it discovered that this data was collected without explicit parental consent in violation of COPPA.[57] Other websites have also been recently found in violation of COPPA.[58]

Prior to COPPA, children were especially vulnerable to questionable website practices. A wide variety of detailed personal information was collected from children online through various stratagems, notably en-

---

attached linguistic component. *See* Steven Hetcher, *Norms*, *in* ENCYCLOPEDIA OF ETHICS, 909, 909-12, (Lawrence C. Becker ed., 1992) [hereinafter Hetcher, *Norms*]. When characterizing a group's norms, it is necessary to keep in mind the difference between norms and rules, as it is important to be able to look at the actual practices of groups, rather than merely going by what they express linguistically. Talk is cheap; it is conforming behavior that creates benefits for conforming groups and externalities for third parties. *See* Steven Hetcher, *Creating Safe Social Norms in a Dangerous World*, 73 S. CAL. L. REV. 1, 43 (1999) [hereinafter Hetcher, *Creating Safe Social Norms*]. Elsewhere, I adopt the term, "norm statement" or "rule" for the linguistic component of a full norm. *See* Hetcher, *supra* note 5.

54. This is noteworthy as norms theorists often write as if norms by definition express obligatory behavior *See, e.g.,* Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 587 (1998) ("Since this article focuses on obligations, my use of "norm" conforms to philosophical usage [that a norm is an obligation.]"); Eric Posner, *Law, Economics, and Inefficient Norms,* 144 U. PA. L. REV. 1697, 1699 (1996) ("A norm can be understood as a rule that distinguishes desirable and undesirable behavior and gives a third party the authority to punish a person who engages in the undesirable behavior.").

55. 15 U.S.C. §§ 6501, 6505 (Supp. 2000).

56. *See Toysmart.com's Plan To Sell Customer Data Is Challenged by FTC*, WALL ST. J., July 11, 2000, at C8.

57. *FTC Announces Settlement With Bankrupt Website, Toysmart.com Regarding Alleged Privacy Policy Violations*, FTC Release (July 21, 2000), *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm.

58. *See FTC Announces Settlements with Web Sites That Collected Children's Personal Data Without Parental Permission*, FTC Release (Apr. 19, 2001) *at* http://www.ftc.gov/opa/2001/04/girlslife.htm.

couraging children to register for contests, enroll in electronic "pen pal" programs, complete a survey, sign up for informational updates, or play a game.[59] Other websites used "imaginary" characters to request information from children, or had them sign a "guest book."[60] The FBI and Justice Department's "Innocent Images" investigation revealed that online services and bulletin boards were rapidly becoming the most effective resources used by child predators to identify and contact their victims.[61]

Another publicized harm was "identity theft."[62] Identity theft occurs when one person intentionally assumes another person's online identity. Websites themselves did not typically engage in identity theft. Rather, identity thieves availed themselves of crucial personal information conveniently available online, including an individual's social security number and mother's maiden name, as the starting point for their activities. Typically, identity thieves go on shopping sprees at the expense of their

---

59. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 4-5.

60. *Id.*

61. *See* FEDERAL TRADE COMMISSION, PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY: CONSUMER ONLINE PRIVACY at 192-93, 229 (June 12, 1997) (testimony of Charlotte Baecher, Director of Education Services, Consumers Union and Linda Hooper, FBI Agent) [hereinafter 1997 FTC WORKSHOP]; *see also Child Pornography on the Internet and the Sexual Exploitation of Children, Before the Senate Appropriation Subcommittee for the Department of Commerce, Justice, and State, the Judiciary, and Related Agencies*, 105th Cong. (Mar. 10, 1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress98/sac310.htm; *Crimes Against Children Facilitated by the Internet: Hearing Before the House Judiciary Committee, Subcommittee on Crime* (testimony of Stephen R. Wiley, Chief, FBI Violent Crime and Major Offenders Section), 105th Cong. (Nov. 7, 1997) *available at* http://www.fbi.gov/congress/children/children.htm. Further, anecdotal evidence indicates that many children surfing the Web claim to have experienced problems such as attempted password theft and inappropriate advances by adults in children's chat rooms.

62. *See, e.g.,* Sandberg, *supra* note 3, at 56. Indicating the seriousness of the problem, the FTC has recently appointed a person to handle the issue. *See Prepared Statement of the Federal Trade Commission on "Identity Theft" Before the Subcomm. on Technology, Terrorism and Gov't Info. of the Senate Committee on the Judiciary*, 105th Cong. (May 20, 1998) (statement of David Medine, Assoc. Dir. for Credit Practices, Bureau of Consumer Prot., Federal Trade Commission). A recently passed Act imposes a penalty of up to twenty-five years of imprisonment and fines for theft of personal identification with intent to commit an unlawful act. Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(b) (1994); *see* Laracuente v. Laracuente, 599 A. 2d 968 (N.J. Law Div. 1991) (showing typical social security number identity theft); Kurt M. Saunders and Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act,* 8 CORNELL J.L. & PUB. POL'Y 661, 671 (1999); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 470-474 (giving examples).

victims, but the possibilities for abuse will only grow as the functionality of the Internet expands. As a means of combating identity theft, privacy norm entrepreneurs advocate greater data security measures by websites.[63]

The use of private employee medical information in making employment-related decisions is an egregious, and rapidly expanding, data-collection practice. One-third of Fortune 500 companies reportedly use personal medical information in hiring, promotion, or termination decisions.[64] As a result, many individuals are declining to seek medical diagnosis and treatment in order to avoid creating a paper trail that their employers can then use against them (or their children or grandchildren in diagnosis of genetic disease).[65] It remains to be seen whether the medical privacy regulations proposed by the Clinton administration and recently endorsed by the Bush administration will remedy the current situation.

The vast majority of commercial websites are engaged in the unregulated, ubiquitous gathering and use of nonspecialized personal data.[66] Studies indicate that most people feel uncomfortable with commercial entities gathering their personal data, especially when this data can be sold to

---

63. *See, e.g.*, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY, May 1, 2000, *at* http://www.ftc.gov/acoas/papers/finalreport.htm [hereinafter ONLINE ACCESS AND SECURITY].

64. *See* Jane Birnbaum, *Look Into It; Here's How to Protect Your Medical Records*, CHICAGO TRIB., Nov. 23, 1999, at C1; David F. Linowles & Ray C. Spencer, *How Employers Handle Employees' Personal Information Report of a Recent Survey*, 1 EMPLOYEE RTS. & EMPLOYMENT POL'Y J. 153, 156 (1997).

65. *See Testimony Before the Subcomm. on Health of the House Committee on Ways and Means on the Subject of "Patient Confidentiality"*, 105th Cong. (Mar. 24, 1998) (testimony of Janlori Goldman, Health Privacy Project Inst. for Health Care Research and Policy, Georgetown Univ.) ("In the absence of such trust, patients will be reticent to accurately and honestly disclose personal information, or they may avoid seeking care altogether for fear of suffering negative consequences, such as embarrassment, stigma, and discrimination. Along the continuum, if doctors and other health care providers are receiving incomplete, inaccurate information from patients, the data they disclose for payment, research, public health reporting, outcomes analysis, and other purposes, will carry the same vulnerabilities."); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 22 (1997) ("[W]ide disclosure of certain kinds of information may distort individual behavior in an inefficient fashion. Fearing loss of employment and social discrimination, people will either lie to their physicians or avoid seeking care that might lead to the creation of sensitive health care or genetic information.").

66. *See Testimony Before the Senate Comm. on Commerce, Science and Transp.*, 106th Cong. (May 25, 2000) (testimony of Sheila Anthony, FTC Comm'r) *available at* http://www.ftc.gov/os/2000/05/privacyanthony.htm (last visited Aug. 7, 2001) ("The vast majority of web sites collect personal data but do not provide privacy protections.")

third parties for unrelated purposes.[67] Among the most egregious activities, the public disclosure of highly private facts, may be legally sanctioned under the common law tort of disclosure.[68] The high standards required by this doctrine will not protect against the vast majority of website data collection activities.

Julie Cohen has advocated a right to read anonymously. She provided a powerful argument that freedom of conscience implies a right to anonymously browse the Internet.[69] No such right currently exists. When a website visitor reads online and links between various websites, it is lawful for anonymous third parties to monitor and record the visitor's activities. How may individuals freely explore their sexuality or political interests with concerns about creating a perpetual electronic record that might make it difficult to enter certain professions or run for public office?

C. The Emergence of a Privacy Norm Gap

From a policy perspective, the most striking feature of the early website norms is that they were completely biased toward serving the interests of the website industry. This reflects the reality that most websites felt neither legal nor social pressure to respect the data privacy of website visitors. This indicated a gap between the existing website data collection practices and informed, alternative practices more consonant with conventional community standards.

Gaps between actual versus desirable social practices may emerge for a variety of reasons, including small group migrations or the discovery of new scientific information. Sometimes when a smaller group migrates into a larger group, some minority practices are deemed to be out of step with the morality of the majority group, and a norm gap exists between actual and desirable practice from the majority perspective.[70] In the case of ciga-

---

67. Studies indicate that consumers are particularly afraid of transfers of their personal data to unknown third parties. *See* FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 2 (July 1999) [hereinafter 1999 FTC REPORT TO CONGRESS].

68. *See, e.g.*, Eugene Volokh, *Freedom of Speech and Informational Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1055 (2000).

69. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 982-83 (1996) (arguing that digital copyright management technologies violate First Amendment Rights protecting speech and freedom of thought); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999) (claiming that the absence of privacy norms threatens democracy).

70. The much debated topic of female genital mutilation or modification is such an instance. As members of groups that engage in this practice have migrated into popula-

rette smoking, the disclosure of new scientific information about the health impacts of smoking has opened a gap between actual and desirable practices.[71]

In the past, traditional social theory casually assumed that diffuse social forces would push groups toward closing norm gaps.[72] Rational choice theorists have subsequently demonstrated that diffuse social gap-filling will not automatically occur.[73] Whether norm gaps close depends on the strategic structures of existing practices that create and maintain the gaps and new practices that might fill the gap. Norm gaps can close automatically or, more rarely, through intentional actions. Thus, norm gaps present opportunities for norm entrepreneurs. Part II will examine the privacy norm proselytizer, a special type of norm entrepreneur that has been instrumental in closing the norm gap between actual versus desirable website data-collection practices. To fully appreciate the techniques of these norm proselytizers, it is first necessary to examine the strategic structures that perpetuated the privacy norm gap.

D. Structural Impediments to Filling the Norm Gap

Several factors converged to maintain the privacy norm gap. The first is the normative quality of interactions between websites and their visitors. Significantly, typical consumers were morally insensitive to the privacy-invasive practices of websites. Consumers did not perceive themselves as being in a strategic relationship with websites. The second factor was the relationship structure among various websites. The website industry maintained a coordination game in which negative externalities could be absorbed by third-party consumers. Examining each of these factors will

---

tions that morally criticize the practice, a gap has emerged between actual practices and practices deemed justified by the mores of the broader community. *See, e.g.*, Edward Hegstrom, *Gynecologists Report Female Circumcisions; Some Immigrants Had Operation, Study Finds*, HOUSTON CHRONICLE, Dec. 27, 2000, at A19.

71. Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 404-05 (1997).

72. *See* Ellickson, *supra* note 4, at 2.

73. Sociologists sometimes refer to diffuse social forces as bringing about changes in norms. Law and norms theorists seek instead to find rational choice explanations for the emergence of new norms:

> I suggest that a new social norm arises through a process much like the market for widgets. A norm is not the product of 'diffuse social forces,' as a sociologists [*sic*] might put it, but rather of the purposive actions of discrete individuals, especially those who are particularly suited to providing the new rule and those who are particularly eager to have it adopted.

Id. at 2.

clarify why the initial privacy norm gap was unlikely to close spontaneously.

1. Unrealized Potential for Consumer/Website Strategic Interaction

In theory, consumer/website interactions may have been capable of closing the privacy norm gap. If visitors want to be treated better and websites want more customers, a market equilibrium should emerge through Coasean bargaining in which consumers receive the level of respect for which they are willing and able to bargain. Despite favorable prospects, there are two reasons why Coasean bargaining did not produce greater privacy protection for consumers. First, consumers were not typically aware of the practices of websites or the causal connections between data collection and potential resulting harms.[74] Additionally, consumers were morally insensitive to data privacy issues: they did not perceive a moral entitlement to control over their personal data.

A Coasean bargain produces welfare-maximizing outcomes only when the parties have adequate information such that their preferences are properly connected to welfare-enhancing outcomes.[75] These connections were lacking for early website users. As discussed in section A above, methods of data gathering, including cookies, often work invisibly such that visitors are unaware that the website is collecting individualized data.[76] Even when consumers' explicit provision of personal information made them aware of website data collection, they typically remained unaware that this data could then be sold or licensed to third parties for potentially objectionable uses. Among the most fundamental dangers posed by a loss of informational privacy is the danger resulting from the aggregation of separate pieces of data into consumer profiles.[77] That a consumer's data may flow downstream and be combined with data from other sources to form comprehensive profiles would not be apparent to a typical consumer.

---

74. People's preferences do not always reflect their true interests. For example, before the dangers of smoking cigarettes became widely known, an individual might have preferred to live a healthy lifestyle and preferred to smoke, due to a lack of information that created a tension in practical reason between the two preferences. So too, an individual might desire privacy and desire to travel cyberspace, without appreciating the practical tension thereby created.

75. *See generally* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

76. *See supra* text accompanying notes 42-43.

77. *See generally* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (May 2000).

Thus, a Coasean bargain would not produce an efficient outcome simply because there was no bargain in the first place. Websites took advantage of their close proximity to consumers to quietly lift personal data in the absence of any agreement.

Note that the prospect of repeat play would not place a consumer in a better position to receive more respectful treatment from websites. Cooperation may typically become a preferred strategy in repeat games. Even in the context of repeat play, cooperation did not emerge, as websites were able to hide their privacy-degrading activities from their visitors.[78] For example, an individual may not receive a job promotion due to disclosure of health information purchased by his employer through a data broker. He may fail to realize the particular circumstances that diminished his chances for promotion. Alternatively, he might be unaware of the particular causal route from his data provision to subsequent privacy invasion. For example, he may begin to receive targeting emails, and still not know whether this is the result of a visit to his doctor, the filling of a prescription online, or the fact that he browsed a medical website such as WebMD.[79] Repeat play would not affect the likelihood that consumers would benefit from cooperative behavior in either situation.[80]

---

78. Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS 311, 314 (1995); *see also The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1676-80 (1999).

79. The failure of repeat play to produce cooperative outcomes may occur in non-cyber contexts as well. For example, a rancher and a farmer may be involved in repeat play because they are neighbors and yet one party may be able to repeatedly cause injury to the other due to the secrecy of the injurious activities. Suppose, for example, that the farmer is using chemicals on her crops that are bleaching through the soil and slowly degrading the quality of the rancher's well water. Depending on the particular chemicals, the rancher may remain ignorant of the damage for some time. Even when the rancher becomes aware of the damage, she may not be in a position to know who caused it, perhaps because the farmer has changed practices, or because a number of farmers engage in similar practices and the rancher is unsure of whose chemicals caused the damage, due to the ambiguities of underground water flow. Ellickson notes that information is one of the conditions for efficient cooperative norms to emerge. *See* ELLICKSON, *supra* note 16, at 177-78.

80. Kathleen A. Linert, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687*,* 697 n.43 (1995). ("Marc Rotenberg, director of Computer Professionals for Social Responsibility in Washington, D.C., cautions against believing contentions that privacy rights and access are inherently incompatible, since that controversy is created by those that stand to gain from less legislation and more freedom of information."); *Video Service is Compiling Data on Clients*, CHATTANOOGA TIMES/CHATTANOOGA FREE PRESS, Mar. 26, 2001, at A2 (Privacy Foundation technology officer Richard Smith said he is concerned that without privacy laws, personal TV service providers are "free to do whatever they choose" with information.).

Consumers generally did not have a moral understanding of the issue

		Website: Cooperate	Website: Not Cooperate
Visitor	Cooperate	4,2	1,4
	Not Cooperate	3,1	2,3

of data collection. Accordingly, they did not perceive their personal data as entitled to special treatment by websites. Consumers did not appreciate that certain behavior by websites disrespected their right to data privacy.[81] Because consumers failed to conceptualize this relationship as moral, they failed to appreciate the strategic nature of their relationship with websites.

A relationship is strategic when each party's utility is affected, not only by its choices, but also by the choices of the other parties. The utility of website visitors is affected both by their decision to visit a particular website *and* the website's choice to engage in harmful data-collection practices. Correspondingly, the website's utilities are affected both by its choice of data-collection practices *and* by the visitor's decision to engage in repeat visits. A website and a website visitor were potentially engaged in interactions that had the following strategic structure.

Figure 1: Consumer Failure to Appreciate Potential Strategic Relationships

The northeast cell characterizes the typical situation that existed between websites and unaware consumers. The visitor, not understanding actual website practices, instinctively cooperated. The website engaged in

81. It is worth repeating that the present account takes no position regarding the objective truth, or indeed whether there is objective truth, regarding the merits of data privacy and the rest of the circle of related moral terms under discussion. The goal here is normatively sophisticated social science. This project will be most objectively undertaken if the analysis is not seen as geared toward supporting any particular substantive normative position.

permissive data-collection activities and did not cooperate. As a result, the website benefited from its highest payoff of 4 while the visitor received its lowest payoff of 1.[82]

2. Proper Coordination Equilibrium Within Website Industry Actors

This section explores the strategic relationship structures among websites that perpetuated the privacy norm gap. According to the FTC, the website industry has an overriding interest in establishing more respectful privacy norms, if only the constituent websites could coordinate their efforts to bring about a cooperative result. The FTC claimed that if the website industry was more respectful of consumer privacy, then consumers would be less fearful of the Internet and consequently more likely to engage in electronic commerce, which would benefit the website industry.[83] Under this model, the website industry's adoption of respectful privacy norms would collectively benefit it. The barrier in initiating the collective good in this model is an example of the collective action problem.

It is, however, more plausible to suppose that the benefit of increased electronic commerce is not worth the high cost that respecting privacy might impose on websites. For many websites, the most significant cost will arise simply because consumer personal data will no longer be free for their use. For small websites, the cost of developing and implementing a privacy policy may itself be significant.[84] These development costs are of marginal importance for large websites. Large or well-funded companies, however, face a much greater cost: the increased exposure to litigation resulting from making explicit representations to consumers regarding

---

82. The numbers represent the ordinal preference rankings of the players, with 1 being a player's least preferred outcome and 4 being a player's most preferred outcome. Each pair of numbers represents the payoffs to each party for each of the four possible outcomes. The left-hand number in each pair is the payoff to the row-player and the right-hand number is the payoff to the column-player.

83. 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 43.

> By providing greater access rights, businesses could increase the reliability and accuracy of data, build consumer confidence and trust, experience a public relations benefit, make better decisions based on better data, expand markets by giving consumers greater confidence in online privacy, and experience greater efficiencies if they limit information collection to only what is necessary.

ONLINE ACCESS AND SECURITY, *supra* note 63, at §2.5.1.

84. Anecdotal evidence suggests, however, that some sites avoid this cost by simply, and illegally, cutting and pasting from the privacy policies of other sites that they find on the Web. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 36 n.148.

data-collection practices.[85] Given these costs, it is plausible that most firms would prefer not to make explicit privacy guarantees on their websites even if some lessening in the expansion of electronic commerce resulted. Thus, in seeking to foster respectful privacy norms by self-regulatory means, privacy norm entrepreneurs do not face the problem of helping a diffuse industry procure a collective good.

Instead, the strategic structure of the website industry's personal data practices is a coordination game.[86] This coordination game was solved through the pervasive data collection norms examined in Part One. These are coordination norms: a practice in which each conformer receives a coordination benefit for conforming to the norm. A coordination benefit is the added benefit an actor receives for conformity, given the conformity of other participants.[87] As a simple example, if the norm in the United States is to drive on the right side of the road, then an individual conformer receives a benefit when others also conform, as she is less likely to be involved in a collision.

A coordination norm may be an equilibrium, a coordination equilibrium or a proper coordination equilibrium.[88] Equilibrium is a combination of choices in which each actor, given the choices of the other actors, has maximally benefited. No actor will regret her choice given the choices of the others. A coordination equilibrium is a combination of choices such

---

85. For example, RealNetworks recently admitted that its RealJukebox assigned a personal ID number to users and uploaded information about their listening habits to its servers. Sara Robinson, *CD Software Is Said to Gather Data On Users' Listening Habits*, N.Y. TIMES, Nov. 1, 1999, at C1. The company was subsequently slapped with a $500 million class action lawsuit for violating California's unfair business practices law. A second class action suit was filed in the Eastern District of Pennsylvania one day later. *RealNetworks is Target of Suit in California Over Privacy Issue*, N.Y. TIMES, Nov. 9, 1999, at C1. After it was reported that its RealJukebox software continually transmits personal information about its users to the company, RealNetworks publicly acknowledged that the activity was improper and issued a fix for the software. *Id.*

86. Legal norms theorists are beginning to incorporate coordination games into their analyses. *See* Hetcher, *Creating Safe Social Norms*, *supra* note 53, at 43-45 & nn.161-68; Richard H. McAdams, *A Focal Point Theory of Expressive Law*, 86 VA. L. REV. 1649, 1654 (2001).

87. *See* Hetcher, *Creating Safe Social Norms*, *supra* note 53, at 43 n.161 (1999).

88. EDNA ULLMANN-MARGALIT, THE EMERGENCE OF NORMS 81 (1977); *see* Hetcher, *Creating Safe Social Norms*, *supra* note 53, at 44. *See generally* Margaret Gilbert, *Game Theory and Convention*, 46 SYNTHESE 41 (1981). The economics literature on "network externalities" encompasses a similar but broader rational structure as not all networks with significant externalities are norms. *See generally* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects,* 86 CAL. L. REV. 479 (1998); S.J. Liebowitz & Stephen E. Margolis, *Path Dependence, Lock-In, and History*, 11 J.L. ECON. & ORG. 205 (1995).

that no one would have been better off had any single actor behaved differently. A proper coordination equilibrium is a combination of choices such that no single actor would have been as well off had any single actor behaved differently.[89]

The crucial feature of coordination norms is that actors conform to them because it is in their direct interest. Thus, once established, coordination norms tend to stay in equilibrium. This is in contrast to collective action problems in which each actor's direct interest is not to conform, but to defect or free ride. With collective action problems, conformity occurs only if the participants can incentivize cooperation due to the possibility of repeat play, a by-product of the overlapping social relationships of close-knit communities.[90] If these conditions change, the equilibrium may falter and the norm deteriorate. With coordination norms, given the conformity of others, it is in the direct interest of actors to conform to the extant practice. Thus, coordination norms are often more stable. Efficient coordination norms may also emerge in communities that are not close-knit because these norms do not require overlapping interactions to provide incentives for conformity.[91]

---

89. DAVID K. LEWIS, CONVENTION: A PHILOSOPHICAL STUDY 22 (1969). With a proper coordination equilibrium, other conformers receive a benefit when a particular actor conforms. *Id.* It is this feature that causes David Lewis to claim that "conventions" are best modeled as proper coordination equilibria. *Id.* Conventions, on Lewis' well-known account, are maintained in part by sanctions. *Id*. at 44-49. Conformers sanction one another for non-conformity because it is in the interest of others that each conform. *Id.* The sanctions are meant to ensure the conformity of others. *Id*.

90. In addition to Ellickson, Robert Cooter, Richard McAdams and Eric Posner have each developed alternative accounts of how norms may serve as solutions to iterated collective action problems. Cooter focuses on the importance of the psychological phenomenon of "internalization," whereby conformers internalize the pro-conformist attitudes necessary to maintain productive norms. *See* Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant,* 144 U. PA. L. REV. 1643, 1690-94 (1996). McAdams emphasizes the role of "esteem" sanctions, which, as he argues, solve the second-order collective action problem created by the need for group sanctions to incentivize conformity with desirable social norms. *See* McAdams, *supra* note 71, at 342 (stating that the "theory of origin and growth of norms" in which "the initial force behind norm creation is the desire individuals have for respect or prestige, that is, for the relative esteem of others"). Finally, Posner argues that cooperation in Prisoner's Dilemma games is due to the desire of putative cooperators to "signal" that they are good types rather than bad types, and thus players worthy of future cooperation from other players. *See* Eric A. Posner, S*ymbols, Signals, and Social Norms in Politics and the Law,* 27 J. LEGAL STUD. 765, 767-68 (1998). *See generally* ERIC A. POSNER, LAW AND SOCIAL NORMS (2000).

91. Hetcher, *Creating Safe Norms*, *supra* note 53, at 9.

The present concern is whether website practices are best modeled as coordination norms. The core feature of a coordination norm is that, given the conformity of others, an actor receives a coordination benefit from conforming. This condition is met in early website data-collection practices: given that most other websites are acting disrespectfully, a particular website has a direct interest in likewise disrespecting consumers. By conforming, websites obtain use of valuable personal data at less expense and effort, and avoid the worry of exposing themselves to legal liability by making explicit representations to consumers.

In addition, it is plausible that websites also prefer that the website industry generally disrespects consumer privacy. First, websites can more easily collect personal data when consumers are ignorant of website practices. Thus, all websites will be hurt when individual websites explicitly disclose their data gathering activities. The greater the public awareness, the more likely that consumers will be wary of particular websites' activities and pressure websites to alter their practices toward greater respect. Second, should litigation arise, this will facilitate dismissal of consumer claims to a reasonable expectation.[92] If most websites are collecting data at will, with no privacy safeguards in place, then the website-defendant will have a colorable defense to plaintiffs' central claims of a reasonable expectation of privacy.[93]

From this dynamic, industry insiders might be expected to discretely promote disrespectful norms through industry leader meetings, as doing so will strengthen the norm and likewise their safe harbor. This will strengthen these disrespectful website coordination norms. The original website data collection norms appear then to be proper coordination equilibria: each particular website is not as well off had either it or another website not conformed to the disrespectful privacy practices. This situation is represented in the following payoff matrix.

Figure 2: Website Industry Coordination Game

---

92. *See, e.g.*, Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 364-65 (2000) (noting that "[a]ssurances of privacy protection by e-commerce vendors and Internet service providers demonstrate that the commercial side of the Internet recognizes that respect for privacy is a significant expectation of Internet users" (footnotes omitted)).

93. *See also* Andrew B. Buxbaum and Louis A. Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (But Not Under the Bankruptcy Code)*, 8 AM. BANKR. INST. L. REV. 395, 411-12 (2000) (arguing that the appearance of privacy policies would create an expectation of privacy).

		Other Websites: Respect Privacy	Other Websites: Disrespect Privacy
Website A	Respect Privacy	2,2	1,3
	Disrespect Privacy	3,1	4,4

The matrix in Figure 2 depicts the website payoffs depending on whether websites individually, as well as the industry as a whole, participate in personal data collection practices that either respect or disrespect the privacy of consumers. Note that whether websites respect or disrespect privacy affects the payoff to a typical website, Website A. The dominating preference is to disrespect privacy: Website A prefers to disrespect privacy regardless of the activities of other websites. Thus, A's payoffs are higher in the southern, as opposed to the northern, cells. Website A receives an additional coordination benefit when other websites also disrespect privacy. Thus, the payoff for A is higher in the southeast cell as compared to the southwest cell. Website A least prefers the northeastern cell scenario where it respects privacy and other websites disrespect privacy. In this situation, there will be no noticeable increase in electronic commerce because A's activities alone will not affect consumer confidence, and yet A has lost all the benefits from the free receipt of user data.

Like A, other websites prefer to disrespect privacy, so their highest payouts come in the eastern cells. They also prefer that A likewise disrespects privacy, due to the coordination benefit of keeping consumers in the dark. Thus, the other websites receive higher payoffs in the southeast, as compared to the northeast, cell. If the other websites are respecting privacy, however, they will likely prefer that A do the same so A is not at a competitive advantage. Thus, their payoff is higher in the northwest, as compared to the southwest, cell.

The southeastern cell outcome—where all websites disrespect privacy—is a stable equilibrium. No website has an incentive to change its behavior nor get another website to change its behavior. Just the opposite, each website has an incentive to encourage other websites not to change their behavior. The implication is that the norm gap will not close under

these conditions. The harm resulting from these practices—the degradation of personal privacy—is successfully externalized onto Web-surfing consumers.[94] Some commentators conclude that the failure of informal forces to adequately handle these externalities mandates direct governmental intervention.[95]

In the discussion in Part III below, however, it will be seen that omnibus government regulation of website practices has not been required to bring about more respectful privacy norms. The FTC has been actively involved, but its role is that of a norm entrepreneur rather than a norm imperialist. The FTC has been among a number of norm entrepreneurs, each contributing to a more respectful online privacy environment. As Part III explains, the lead role was played by public-interest privacy activists functioning as norm proselytizers.

III. PRIVACY ACTIVISTS MORALIZE THE SOCIAL MEANING OF DATA COLLECTION

The following discussion explores the actors working to close the privacy norm gap. These privacy norm proselytizers have partly overcome the factors maintaining this gap that were explored in Part I. The emergence of the grundnorm of industry respect for consumer privacy by websites is the story of how privacy activists working in their capacity as norm proselytizers have successfully changed the social meaning of data collection from a predominantly non-moral to a morally-charged activity. Consumers increasingly feel entitled to respectful treatment from those who handle their precious personal data. This dramatic change in the consumer/website relationship did not emerge spontaneously but was due to the conscious efforts of privacy activists.

The section A below examines the concept of social meaning generally. Sections B and C explore methods through which privacy activists have moralized the social meaning of data collection and the dimensions of this new morality. Finally, section D examines the impact of this change in social meaning on the strategic relationship between consumers and websites.

---

94. Similarly, the possibility of externalization of the costs of an industry custom is one reason why the established "rule of custom" in tort law is that conformity to industry custom may serve as evidence of due care, but is not dispositive. *See* Hetcher, *Creating Safe Norms*, *supra* note 53, at 73.

95. *See generally* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999).

A. Social Meaning and Social Norms

Among the key insights of recent law and norms literature is the connection between norms and their social meanings. The best approach to changing a social norm may be to change its social meaning. To illustrate this, Larry Lessig discusses dueling by the aristocratic class in the Old South.[96] The dueling norm was resistant to legal prohibition, as making dueling illegal left intact its social meaning: participation was perceived as honorable, refusal as cowardly. A more promising approach was to change dueling's associated social meaning by making it illegal for duelers to hold the honorable position of public office.[97] This changed the social meaning such that potential participants were able to decline duels without losing honor due to the credible claim that the refusal was motivated by the esteemed prospect of holding public office.[98]

With other social norms, however, the affiliated social meaning may be very difficult to change. With gun possession by juvenile members of street gangs, the challenge is to shift the social meaning from one in which gang members enhance their relative status by challenging authority through handgun possession.[99] The perverse logic of the illicit handgun possession norm and its affiliated social meaning is that the greater the legal sanction against the activity, the greater the peer status for continued participation.[100]

With personal data collection, the goal of norm entrepreneurs has been to shift the social meaning from a morally neutral to a morally-loaded significance. Two differences exist between data-collection norms and norms such as gun possession and dueling, both of which uniquely complicate the privacy activists' task. In the previous examples, the norm conformers are also the primary intended beneficiaries of the proposed new norm. With data collection, however, it is website visitors who are the main group of intended beneficiaries, not the websites themselves.

A second difference is that the goal in the above examples was to reduce or eliminate behavior. With personal data collection practices, however, the goal is more complex. The purpose is not to completely eliminate

---

96. Lessig, *supra* note 5, at 968-73.

97. *Id*. at 971-72.

98. *Id*.

99. *See generally* Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349 (1997).

100. Likewise, with cigarette smoking, the challenge is to shift the social meaning away from the current situation whereby teen smoking is considered cool. The more that authorities try to control smoking, the cooler it may seem. *See* Lessig, *supra* note 5, at 1025-34.

the collection and use of personal data by websites, but rather to put this practice on firmer moral ground. Balancing websites' benefits from disrespectful collection practices and the desire not to eradicate data collection entirely, it seems especially difficult for privacy norm entrepreneurs to bring about a more respectful and nuanced result.

The next section addresses the manner by which privacy proselytizers have approached the difficult task of changing the meaning of personal data collection in cyberspace. As this section demonstrates, the logical first step was to fit the relevant practices into a broader normative framework. Privacy proselytizers were then in a position to evaluate potential demands placed on websites that respect privacy. Finally, the activists proselytized to convince the public to accept their moral position.

B. Internet Privacy Activists' Proselytizing Efforts

Privacy regulation in the United States has consisted of applying the concept of privacy to new situations that resulted from emerging technologies. Brandeis and Warren's famous article, for example, was a response to the new privacy threat posed by the invention of the camera and its subsequent use by the media.[101] The seminal Supreme Court cases, *Olmstead v. United States*[102] and *Katz v. United States*,[103] resulted from the development and use of telephone wiretapping technology by law enforcement officials.

A generation ago, the pre-Internet electronic privacy advocates highlighted the threat that government computers posed to privacy.[104] The threat arose from U.S. Government plans to use computers to construct a comprehensive personal information database on its citizens. While privacy activists continue to perceive government as a threat to personal privacy, the focus of attention has changed in recent years to the private domain. The single most significant impetus for this change has been the emergence of the Internet and the associated website industry.

When government was the perceived threat, privacy activists invoked the Fourth Amendment of the U.S. Constitution with some degree of success. When the main threat to privacy came from private entities such as

---

101. *See* Brandeis and Warren, *supra* note 9.

102. Olmstead v. United States, 277 U.S. 438 (1928).

103. Katz v. United States, 389 U.S. 347 (1967).

104. The privacy advocacy community formed in the 1960s to fight against wide-scale personal data collection and aggregation by agencies of the U.S. government, newly armed with mainframe computers. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306-08 (1989); PRISCILLA M. REGAN, LEGISLATING PRIVACY-TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 70-71 (1995).

websites and Internet companies like DoubleClick, legal claims in favor of data privacy have had little success. It has been argued that these websites violated one or more privacy torts,[105] or engaged in unfair trade practices.[106] Attorneys have proposed that when websites plant cookies on the hard drives of consumers they commit trespass to chattels.[107] On the whole, however, none of these legal arguments has provided much protection against the majority of website data practices. Privacy activists instead place great reliance on claims that website practices are immoral.

In recent years, a number of public-interest organizations have identified online privacy as an important public-policy concern. These groups include the Electronic Privacy Information Center ("EPIC"), the Electronic Frontier Foundation ("EFF"), and the Center for Democracy and Technology ("CDT"). Particular individuals, notably Marc Rotenberg and Richard Smith, have become highly visible advocates for online privacy. Rotenberg, the Director of EPIC, is the best known "inside-the-beltway" proponent of electronic privacy. Smith is a so-called "ethical hacker," who works to expose new forms of privacy invasion.[108] As online privacy has become a highly publicized topic, shapers of public opinion, such as New York Times columnist William Safire, have also recently begun to proselytize.[109]

The privacy activist community has employed several strategies to further its goals: activists have functioned as industry watchdogs, legislative proponents, and worked closely with the media. Through these activities, privacy activists have pursued the related aims of education and effecting a change in moral perspective. They have sought to educate the public, politicians, and the media regarding factual issues relating to data collection *and* have striven to change these groups' moral perspective regarding their personal data.

Activists have sought to inform the public of the causal connection between privacy and website data-collection activities because the potential harms resulting from an inability to control personal data are not readily

---

105. *See In re* Doubleclick Inc. Privacy Litigation, No. 00CIV 0641 NRB, 2001 WL 303744 (S.D.N.Y. Mar. 28, 2001).

106. *See infra* text accompanying notes 184-185.

107. *See* Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 632A PRACTICING LAW INSTITUTE 187, 217-18 (June 2001).

108. *See, e.g.*, *Privacy champion defeating Net threats one by one*, SAN DIEGO UNION-TRIBUNE, Apr. 18, 2000, at 10. Richard M. Smith is a software expert who does not fully trust his own kind. *Id.* As a result, he has launched a personal crusade to expose technology practices that threaten the privacy of millions of Internet users. *Id.*

109. Ellickson refers to "opinion leaders." *See* Ellickson, *supra* note 4, at 12-13.

apparent.[110] It is widely believed that consumers are not significantly harmed by identity theft, as fraudulent credit card billing is insured beyond a $50 deductible.[111] In fact, the real danger from identity theft is the potential for serious harm to consumer credit records.[112] The lack of education also frustrates public appreciation of the connection between private medical data and potential damage to public health. The media presented stories connecting the flow of medical information with harms that include failure to seek medical treatment for fear of an electronic trail that could later affect employment opportunities.[113]

The bare knowledge of potential consumer harm does not inherently carry any moral implication. No moral implication follows, for example, from dental-hygiene advocates informing the public of the harmful results of plaque. Thus, establishing a moral connection between website activities and consumer harms was a core goal of the privacy norm proselytiz-

---

110. *See* Lemley, *supra* note 36, at 1276. Non-consensual website interactions are:

> particularly likely when incentives are asymmetrically distributed in the community, as when buyers and sellers have their own conflicting norms. The norm that results from this conflict may represent a variety of things besides consensus: superior bargaining power on the prevailing side, collective action problems on the other side, or the use of strategic behavior.

Id. As the discussion in the main text indicates, there is an additional reason for non-consensual website interactions besides the one Lemley lists, namely ignorance on the part of visitors of the data-collection practices of websites.

111. Susan Wells, *When It's Nobody's Business But Your Own*, N.Y. TIMES, Feb. 13, 2000, at C11.

112. Hal Berghel, *Identity Theft, Social Security Numbers, and the We*b, 43 COMMUNICATIONS OF THE ACM 17, 19 (2000), *available at* http://www.acm.org/pubs/citations/journals/cacm/2000-43-2/p17-berghel ("As any victim can attest, identity theft can destroy personal credit and potentially lead to very expensive litigation that may take years, or perhaps decades, to fully correct."); Kevin G. DeMarrais, *Beware Thieves Who Steal Christmas*, THE REC., Dec. 8, 1996, at B3 ("[I]dentity thieves can establish new accounts in your name and run up big bills and debt. By the time you realize what has happened, your credit record can be in ruins and it can take months to unravel the mess."); Michael A. Gips, *Victims Describe Identity Theft*, SECURITY MANAGEMENT ONLINE, *at* http://www.securitymanagement.com/library/000901.html (last visited Aug. 3, 2001).

113. Dan Stimson, *Internet security an issue for telemedicine success*, ALBEQUERQUE TRIB., Aug. 16, 1999, at A6 ("Exposure of private medical information can affect a person's ability to acquire employment . . . ."); *President to toughen medical privacy rules*, THE SUNDAY GAZETTE MAIL (Charleston), Aug. 20, 2000, at 6B ("Public opinion polls show that Americans are increasingly concerned about privacy in general and want greater protection for medical records, in particular. Some people say they shun testing for cancer, HIV infection and other conditions because they fear discrimination in . . . employment.").

ers. Norm entrepreneurs have advocated a moral relationship of responsibility between the data practices of websites and consumers' loss of privacy and have not dismissed consumer privacy loss as a necessary casualty of the emergence of electronic commerce. This is a moral criticism that has a distinct deontological or Kantian flavor: websites are effectively charged with treating people as mere means to an end. First, consider briefly a broad survey of the steps that privacy proselytizers have taken to promote their goals.

Ethical hackers and corporate watchdogs have been highly successful in discovering dubious website practices. Among the best examples of privacy activism targeting private companies surrounded DoubleClick's acquisition of Abacus Direct. Its intention was, contrary to earlier representations, to combine the online and offline personal data from both enterprises. The advocacy community brought the plan to the attention of the media, which gave generous attention to the story. The price of DoubleClick's stock dropped precipitously as the story unfolded in the press, destroying billions of dollars of the company's market capitalization.[114] The company has subsequently been embroiled in lawsuits and subjected to a heightened level of scrutiny from privacy activists and the FTC.[115]

Another example of successful privacy activism occurred when ethical hackers discovered that Microsoft was building a tracking utility into its software and RealNetworks was tracking the online activities of its customers.[116] The media coverage of these stores typically included a quote

---

114. *See The Internet's Chastened Child*, *supra* note 17, at 80.

115. *See* Jeri Clausing, *Privacy Advocates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000, at C2; *Privacy on the Internet*, N.Y. TIMES, Feb. 22, 2000, at A22; *Marketing the DoubleClick Way*, INDUSTRY STANDARD, Mar. 13, 2000; Will Rodger, *Activists charge DoubleClick double cross*, USA TODAY.COM (June 7, 2000), *at* http://www.usatoday.com/life/cyber/tech/cth211.htm.

116. *See* David Hamilton, *The Gadfly: Privacy Cop Richard Smith is Out to Keep Companies Honest Whether Or Not They Like It*, WALL ST. J., Jul. 16, 2001 (advocacy against RealNetworks and Microsoft); *Music software 'listens in'/ Realjukebox secretly reported listeners' tastes*, NEWSDAY (New York, NY), Nov. 2, 1999, at A47 ("One of the most popular software programs for listening to music on computers is secretly sending details back to a Seattle company about customers' music preferences, including the CDs they listen to and how many songs they copy, a security expert found. The company, RealNetworks Inc., acknowledged that information from its free 'RealJukebox' software, used by more than 12 million people, is sent via the Internet to its headquarters."); *RealNetworks is target of suit*, *supra* note 85, at C1. There were also other examples involving plans to sell data to third parties by Toysmart.com and AOL. *See infra* note 169 (Toysmart.com); Marcelo Halpern and Ajay K. Mehrotra, *From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age*, 21 U. PA. J. INT'L. ECON. L. 523, 536-37 (2000) (noting the reaction of AOL users to a

from a privacy advocate regarding the threat to personal privacy posed by the technology.[117] Once under the media spotlight, these companies quickly backed away from their planned activities.[118]

In an effort to promote laws that will create greater compatibility between positive law and the personal data norms that they promote, privacy activists have engaged in legislative activities. Marc Rotenberg, for example, has repeatedly testified before Congress in support of privacy legislation.[119] Rotenberg is credited with the Digital Millennium Copyright Act provision that could serve as a loophole if the Act fosters a regime of content licensing that requires unduly invasive monitoring.[120] Privacy activists

---

potential change in AOL's privacy policy permitting personal data sales to third parties. AOL users protested strongly and AOL decided not to alter the privacy policy).

117. *See, e.g.*, Steve Pain, *Big Brother in Disguise to Play Internet-Spy*, BIRMINGHAM POST, Mar. 13, 2001, at 24 (quoting Richard Smith).

118. *Online Ad Agency Gives Up Plan To Sell Data; DoubleClick Bows To Privacy Advocates*, ST. LOUIS POST-DISPATCH, Mar. 3, 2000, at C6.

> Bowing to intense pressure from government authorities, investors and privacy advocates, Web advertising firm DoubleClick on Thursday backed off plans to amass a giant online database of people's names and Internet habits. DoubleClick's reversal was applauded immediately by several leaders of the broad backlash against Web-privacy intrusions. Weeks of legal actions and government probes into DoubleClick Inc. have placed the online company at the center of a growing clash between businesses seeking to exploit the Internet's pervasiveness and those fearful of the consequences. "This is a great step forward for Internet privacy," said Ari Schwartz of the Center for Democracy and Technology, a Washington-based group that tracks civil liberties on the Internet.

Id.

119. *See, e.g., Relaxing Limits on Export and Encryption Software: Hearing on the Security and Freedom Through Encryption Act (SAFE), H.R. 695, Before the House Judiciary Comm., Subcomm. On Courts and Intellectual Property*, 105th Cong. (Mar. 20, 1997) (testimony of Marc Rotenberg, Director, Electronic Privacy Information Center); *Computer Technology Security: Hearing on CyberAttack: The National Protection Plan and its Privacy Implications, Before the Senate Judiciary Comm., Subcomm. On Technology, Terrorism, and Government Information*, 106th Cong. (Feb. 1, 2000) (testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center); *Electronic Privacy: Hearing on HR 5018 "Electronic Communications Privacy Act of 2000," HR 4987, "Digital Privacy Act of 2000," and HR 4908, "Notice of Electronic Monitoring Act"*, 106th Cong. (Sept. 6, 2000) (testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center).

120. *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised,* 14 BERKELEY TECH. L.J. 519, 544 n.138 (1999).

were also instrumental in lobbying for the enactment of COPPA.[121] More recently, they have pushed for an extension of this regulatory framework to adults.[122]

As with their watchdog activities, privacy activists have effectively utilized their media contacts to draw public attention and support for their legislative initiatives. The activists' efforts have generally been geared toward bringing media attention to online data issues and then converting the media to their normative positions. Both these efforts appear highly successful. In the recent past, the *New York Times* has contained at least one story per week touching on issues of electronic privacy. More conservative publications such as *The Economist* and *Forbes* have also given sympathetic treatment to the activists' views.[123] Because electronic privacy is currently a leading policy concern, the media's hunger for news stories is steadily growing, making it increasingly receptive to the story tips and press releases provided by the public interest advocacy groups.

The success of first generation privacy norm proselytizers is reflected by the attention of a second generation of privacy entrepreneurs, public

---

121. *See Privacy Advocate Calls for Strict Rules from Regulator, Encourages "Just Say No" Attitude from Parents Against Web Sites That Solicit Personal Data from Kids*, BUSINESS WIRE, Apr. 20, 1999 ("Junkbusters Corp. President Jason Catlett today urged Federal regulators and parents to stand firm against marketers who want to use the Internet to extract information from the nation's children. 'From Microsoft to the 'young investor' site that asked kids to report on their parents' financial assets, Internet companies have demonstrated they cannot be trusted to respect anyone's privacy. Parents and regulators must vigorously defend our children against the electronic molestation of their identities,' Catlett said."); *Privacy, For the Sake of Children*, CAPITAL TIMES, (Madison, WI) June 30, 2000, at 1D ("The Children's Online Privacy Protection Act—or COPPA, as its usually called—went into effect on April 21, 2000. Its 'enactment marked a triumph for children's advocates, who have agitated since the mid-1990s for basic protections for the Internet's youngest users.'"); *White House Starts Privacy Push*, CHICAGO SUN-TIMES, July 31, 1998, at 31 ("'On the main privacy issues, the ones that confront the country today, the administration is still reluctant to make the hard decisions,' said Marc Rotenberg, executive director of the Electronic Privacy Information Center.").

122. *See New Serious Side to Child's Play on Web*, N.Y. TIMES, Nov. 27, 1998, at A4 ("Privacy advocates have raised different concerns about the law. Marc Rotenberg, executive director of the Electronic Privacy Information Center, a privacy advocacy group in Washington, favors online privacy protections for adults, too, and would have preferred legislation based not on parental consent, but on the idea of privacy for all."); *Protecting Kids' Privacy Online*, NEWSBYTES, Mar. 11, 1999 ("'It's a parental notification law, which has some pluses and some minuses,' says Marc Rotenberg of the Electronic Privacy Information Center. 'What we really need is a base-line privacy bill for all users of the Internet. If this bill helps us move beyond industry self-regulation, we're moving in the right direction.'").

123. *See, e.g.*, THE ECONOMIST, *supra* note 3, at 21; Penenberg, *supra* note 3, at 182.

"opinion leaders," to online privacy.[124] William Safire, columnist for the New York Times, recently authored an editorial strongly endorsing the need for online privacy.[125] Remarkably, no particular privacy-related news event motivated the editorial—the topic itself has become newsworthy. Unlike many privacy activists, Safire did not either call for a legislative solution or explicitly promote a self-regulatory approach. Rather, he addressed the issue at a deeper, more philosophical level, arguing that Internet privacy is an issue of growing concern to all "lovers of freedom."[126] As this example suggests, a second success of the first generation of norm proselytizers is that online privacy is perceived as so urgent and morally cogent that it currently transcends ideological faction.

C. The Moral Meaning of Internet Privacy: Reasonable Control Over One's Personal Data

Norm proselytizers, including those advocating privacy norms, promote norms because they morally support them. The bare fact that privacy proselytizers accept similar moral principles does not mean they agree on the application of abstract moral principles to actual circumstances. Unless they take the untenable position that privacy trumps all other concerns, even strong believers in data privacy must balance this value against other values. Thus, the privacy proselytizer who has realistic hopes of winning converts among ordinary people must develop a position supporting increased online privacy that coheres with ordinary morality.

Two factors were present in the early online environment that should have deterred privacy proselytizers from quick conclusions about greater online privacy: the suspect website behavior was legal and consumers were indifferent toward online data privacy issues.[127] Typically, seriously immoral behavior is illegal. As website data collection practices were not illegal, one implication was that websites were behaving in a morally acceptable fashion. This is not dispositive, however, because when new types of behavior arise, often there is some delay before the law reacts.

---

124. Ellickson, *supra* note 4, at 12-13. Especially influential early on were the norms developed by the Organization for Economic Cooperation and Development ("OECD"), which endorsed eight "privacy guidelines." *Id*. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, has stated that OECD's eight principles for data protection are still the "benchmark for assessing privacy policy and legislation." *Oversight Hearing on Electronic Communications Privacy Policy Disclosures, supra* note 43; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980), *at* http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

125. William Safire, *Stalking the Internet*, N.Y. TIMES, May 29, 2000, at A15.

126. *Id*.

127. *See supra* text accompanying notes 73-76.

The second factor of consumer indifference is more troublesome for the privacy proselytizer. As discussed in Part I, consumers did not appear concerned about website data collection practices when they first emerged. If the consumers themselves were indifferent, could norm proselytizers intervene without appearing as norm paternalists?[128]

Paternalism is a suspect form of activity that morally coherent norm entrepreneurs avoid, as it conflicts with the widely accepted principle of autonomy.[129] To act paternalistically is to fail to respect individuals' ability to make decisions that they believe will best serve their interests. The privacy activist must sometimes recognize that many people may not care what websites do with their personal data.[130] In fact, many individuals may favor free use of their personal data because they prefer the resulting personally-tailored marketing over privacy.[131]

The paternalist seeks to assert parental authority against the inclinations of the subjects, while the proselytizer seeks to change the moral consciousness of autonomous subjects. Impressionistic evidence indicates that norm entrepreneurs have functioned in both capacities.

It is the mark of a savvy norm entrepreneur to spot a situation that is ripe for the emergence of a new norm. A norm may sometimes receive

---

128. A norm paternalist is one who seeks to enforce norms of behavior out of paternalistic motivations despite the fact that the subjects of the potential norm would not themselves prefer the change. It is typical to discuss paternalism in a legal context. The norm proselytizer has a wider scope of interest, however, one that includes both the formal legal domain and the informal social domain. Thus, the norm paternalist would seek to exert paternalistic authority against the inclinations of the norm subjects in both the formal and informal domains.

129. *See* JOHN STUART MILL, ON LIBERTY (1859), *reprinted in* ON LIBERTY AND OTHER ESSAYS, at 14 (John Gray ed., Oxford Univ. Press 1991); Richard J. Arneson, *Mill Versus Paternalism*, 90 ETHICS 470 (1980); Jean Braucher, *Defining Unfairness: Empathy and Economic Analysis at the Federal Trade Commission*, 68 B.U. L. REV. 349, 384-87 (1988); Joel Feinberg, *Legal Paternalism*, 1 CAN. J. PHIL. 105 (1971); *cf.* Danny Scoccia, *Paternalism and Respect for Autonomy*, 100 ETHICS 318 (1990).

130. *Laws Should Define Who Owns 'Our' Data*, NEWSDAY (New York, NY), Apr. 25, 2000, at A37 ("Who cares if once-intimate details of people's lives circulate from one databank to another? What important interest or principle is threatened by that?").

131. A majority of Internet users (61%) say they would be positive toward receiving banner ads tailored to their personal interests rather than receiving random ads. This represents about 56 million adult users interested in such personalization. More than two-thirds of Internet users (68%) say they would provide personal information in order to receive tailored banner ads, if notice and opt out are provided. This represents about 63 million adult users.

Excerpt from Dr. Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want*, (Nov. 1999), *at* http://www.pandab.org/doubleclicksummary.html.

widespread yet weak social support, while the latent support for a potential replacement norm is strong. Cass Sunstein discusses the attack on apartheid in South Africa, the use of the term "liberal" as a term of opprobrium, and the current assault on affirmative action, as examples of this phenomenon.[132] Eric Posner provides a similar analysis of the norms that bolstered regimes of the former Soviet republics.[133] In Poland, the population was ripe for a new regime incorporating more democratic norms because the support for the old norms was more apparent than real.[134] Similarly, contemporary online privacy activists intuitively sensed that widely-held moral concepts would assist them in quickly shifting public views from a position of indifference to moral concern.

The task of the privacy norm proselytizer varies depending on the community. In countries with generally weak commitments to privacy values, it is more difficult to proselytize for data privacy. In the United States, however, the privacy norm activists have an easier task because there is already a strong commitment to privacy.

The goal is to extend the scope of the concept of privacy to cyberspace. This is analogous to the task of animal rights proselytizers seeking to extend moral principles applicable to humans across species to other sentient creatures. Electronic privacy advocates do not extend moral principles to new species but rather to new types of situations involving the online collection of personal data. In either case, the goal is the same: to make people see a commonality where before they saw a distinction. The privacy proselytizer's core normative assertion is that individuals have a right to data privacy—though privacy activists rarely discuss why this right should exist. Indeed, it is not the task of privacy proselytizers to establish the right as an objective moral truth. Their task is to convince others to adopt their position; effective proselytizing need not involve reasoning from first principles.

The website industry accepts the proposition that consumers have some right to data privacy.[135] This is a striking admission. One might have expected the industry to take the more aggressive position that since personal data is in the public domain, websites are as entitled to use it as are the data subjects. Instead, the typical posture of industry is to acknowledge that data subjects have some special entitlement to their personal data, de-

---

132. Sunstein, *supra* note 4, at 912.

133. *See* ERIC A. POSNER, LAW AND SOCIAL NORMS Ch. 8 (2000).

134. *Id*.

135. *See, e.g.,* Walmart.com Privacy Policy, *at* http://www.walmart.com/cservice/ca_sp_privacypolicy.gsp?NavMode=3 (last visited Aug. 13, 2001) (stating that "[y]ou have the right to control your personal information as you see fit.").

spite a dearth of legal protection. The website industry's conflict with public-interest privacy advocates is over the proper conception of privacy, how much privacy is appropriate, and which thick behavioral practices should invoke the grundnorm of privacy respect. In other words, the disagreement is not over the grundnorm, per se, but which second-order norms and which thick behavioral norms should be established to promote privacy. The website industry has predictably proffered a fairly minimalist framework of practices to promote the grundnorm.

There is no monolithic view as to what the right to data privacy encompasses.[136] On one extreme, the less personal data collected and used, the better.[137] This position may have trouble winning widespread support, however, as this appears to go against consumer preferences.[138] Many consumers seem willing to trade away personal data as long as they receive valuable consideration in return.[139] Most privacy proselytizers do not seek to minimize data collection and use, but rather to change the nature of the relationship between websites and consumers from a morally problematic to a morally acceptable situation.

Norm proselytizers espouse a number of concrete norms to support the second-order norms of data privacy respect: notice, consent, access, security, and enforcement. Least controversial is the notion that data privacy rights include a right to receive notification of the uses to which websites will put personal data. At least in its public discourse, the website industry widely accepts the requirement of notice.[140] Some notion of consent or agreement is the second most often mentioned component of data privacy rights. There is, however, deep division regarding the definition and implication of consent in the context of website data gathering.[141]

---

136. Robert MacMillan, *Congress to Air Public Concerns Over Privacy*, NEWSBYTES, Sept. 5, 2000 (privacy advocates are split with some advocating very strong privacy protections).

137. *See, e.g.,* Litman, *supra* note 2, at 1287.

138. *See* Fred O. Williams, *Area Man Wins Cybercash,* BUFFALO NEWS, Oct. 28, 2000, at C1 (noting that "consumers appear willing to exchange personal data for free prizes and cash").

139. *Websites with a personal touch*, FINANCIAL TIMES (London), Mar. 15, 1999, at 6 ("Do consumers mind being asked to part with information in order to receive personalised goods and services? Most early research would suggest that they do not, so long as they perceive a benefit, such as reading a newspaper for free or saving time.").

140. *See, e.g., Harold McGraw III Says Internet Has Sparked a Revolution on Multichannel Publishing*, BUSINESS WIRE, June 18, 2001; *see also* Schwartz, *supra* note 69, at 1688-91 (noting the concept of notice being equivalent to privacy protection seems to be capturing much of the policy debate).

141. *See* Glancy, *supra* note 92, at 370.

The concept of consent is ambiguous in distinguishing between opt-in and opt-out regimes. In an opt-out regime, personal data will automatically be collected unless a consumer specifically indicates otherwise. Industry groups such as the Online Privacy Alliance have also promoted an opt-out policy.[142] The Alliance is a coalition of more than eighty companies and trade associations and was formed in early 1998 to encourage self-regulation of data privacy.[143] In an opt-in regime, the default is that personal data will not be collected unless the consumer explicitly agrees. Privacy advocates are typically advocates of opt-in.[144]

Privacy is often defined as the right to be left alone.[145] Website respect for consumer privacy cannot mean that websites should literally leave

---

> Whether Internet users in the United States must be asked to consent to each appropriation of information about their on-line activities (opt-in) or, rather, whether Internet users have implicitly consented to general use of digitized profiles of their Internet activities so that each Internet user must expressly withdraw consent to sale of such information (opt-out), remains a very contentious privacy issue.

See generally Jeff Sovern, *Opting In, Opting Out, or no Options at All: The Fight For Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

142. *See, e.g.,* http://www.privacyalliance.org/resources/ppguidelines.shtml.

> Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use.

Id.

143. *See* 1999 FTC REPORT TO CONGRESS, *supra* note 67, at 8-9.

144. Amy Borrus, *The Stage Seems Set For Net Privacy Rules This Year*, BUSINESS WK., Mar. 5, 2001.

> Instead, privacy hawks will push for so-called "opt-in" rules that require companies to get users' prior consent before collecting or sharing personal info. Opt-in is a far higher hurdle than opt-out, which allows a company to gather data until a consumer orders it to stop. Privacy gurus hope President Bush will be their strongest ally. As a candidate, Bush said customers "should be allowed to opt in to information sharing." Says Rotenberg: "This is one campaign promise we're not going to forget."

Id.

145. THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888). With respect to privacy, the specific right articulated by Cooley was the "right to one's person." *Id.* Cooley suggested that the personal right was that of "complete immunity" from attacks and injuries." *Id.* This he characterized as the right "to be let alone." *Id.*; *see also Legislative Hearing on H.R. 3365 Drivers Privacy Protection Act of 1993 Before the United States House of Representatives Committee on the Judiciary, Subcommittee on Civil and Constitutional*

consumers alone, as consumers are the ones who visit websites. Instead, the core meaning of privacy in the context of website personal data practices is that the website should leave the visitor's data alone, except to the extent the visitor consents to her personal data being collected and used. When a consumer allows her data to be collected and used, she will have less informational privacy as a result. Note that while this collection and use would reduce privacy, it would not be an instance of the website disrespecting the visitor, because the collection and use occurred with the visitor's consent. The central moral imperative is not to minimize collection and use of personal data, but rather to gather and use a visitor's personal data in a manner that does not violate her ability to control the flow of her personal data. When a website surreptitiously collects personal data from a consumer, this bypasses her rational capacities and treats the consumer as incapable of choosing to supply her data.

In addition to notice and consent, norm proselytizers have promoted a right of access to personal data residing on the databases of websites or related entities like DoubleClick.[146] Generally, the claim is for access and the additional ability to contest or correct incorrect data.[147] The industry has generally opposed these measures, claiming that they would be unduly expensive to implement.[148] Some websites, however, have begun to make explicit offers of consumer access to data.[149]

Rights, 103rd Cong. (Feb. 3, 1994) (statement of Mary J. Culnan, Associate Professor, School of Business, Georgetown University).

146. Drew Clark, *Activists Unite To Push For Stronger Privacy Laws*, NAT'L J'S TECH. DAILY, Jan. 30, 2001.

> For the privacy advocates, the proliferation of privacy-invading technological means that Congress should pass privacy legislation rather than forcing consumers to confront privacy questions each time a new technology is introduced. "Every new service offering raises new privacy issues because Congress and the administration are reluctant to apply a new privacy standard," said Rotenberg. He praised the Edwards bill, which would require companies that make online tracking software to inform users and give them the right to access their personal data, as "probably higher up the curve in terms of good privacy legislation" than most.

Id.

147. Seventy-nine percent of American consumers rate as "absolutely essential" that customers should be afforded the opportunity of seeing their transaction records so that their accuracy can be checked and any mistakes can be corrected. Excerpt from Dr. Alan F. Westin, *The Era of Consensual Marketing is Coming*, (Dec. 1998), *at* http://www.pandab.org/1298essary/html.

148. *See* ONLINE ACCESS AND SECURITY, *supra* note 63, §2.5.1 ("For businesses this approach would lead to a substantial increase in costs, including, among others, the costs of required modifications or new design requirements placed on existing systems, new

A fourth element of the general right to data privacy is security for personal data residing in databases of commercial firms.[150] If personal data is easily accessible by hackers, the website may be causally implicated in injuring the consumer whose data is stored by the website, even if the website is not guilty of any active wrongdoing.

Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of an enforcement principle, which requires that governmental and/or self-regulatory mechanisms impose sanctions for non-compliance with fair information practices.[151] These five aspects of the general right to data privacy are accurately grouped under the notion that people have a right of reasonable control over their personal data.[152] Note that a right to reasonable control does not entail a consumer right to ownership of individual personal data.[153] If consumers own their personal

---

storage costs, new personnel costs, new legal costs and losses due to disclosure of internal practices and proprietary information . . . .").

149. *See, e.g.,* Citigroup Privacy Promise, *supra* note 19 ("We will tell our customers how and where to conveniently access their account information at http://www.citibank.com/privacy/, except when we're prohibited by law, and how to notify us about errors which we will promptly correct.").

150. Stewart Baker, *Cyberterrorism, Industrial Espionage and Crime on the Internet, Regulating Technology for Law Enforcement*, 4 TEX. REV. LAW & POL. 51, 53 (1999).

> If you are going to protect communications from cyberterrorism, if you are going to prevent people from breaking into computers and stealing valuable information, and if you are going to trust your life and your personal data to a computer, you want guarantees that the information will be kept secure. Cryptography and encryption—the ability to scramble data—are some of the building blocks of security.

Id.

151. The European Union ("EU") has recognized that self-regulation may in certain circumstances constitute "adequate" privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking "adequate" safeguards. The EU has noted, however, that non-legal rules such as industry association guidelines are relevant to the "adequacy" determination only to the extent they are complied with and that compliance levels, in turn, are directly related to the availability of sanctions and/or external verification of compliance. *See* European Commission, Directorate General XV, Working Document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?, (Jan. 14. 1998), *available at* http://www.europa.eu.int/comm/internal_market/en/media/data-prot/wpdocs/wp7en.htm.

152. The website industry views the norms proposed by the privacy proselytizers as unworkable and overly expensive to implement. Todd R. Weiss, *Bush Faces His First Privacy Challenge: Proposals from Industry, Advocates Differ*, COMPUTERWORLD, Jan. 22, 2001, at 7. The industry's response has been to promote less demanding norms.

153. Some proselytizers have advocated for ownership of one's personal data as the best means to secure the set of rights entailed by the second order right to data privacy. *See* Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-

data, they presumably can sell it. Once alienated, the consumer has no more claim to it than a piece of real property. The right to access personal data and secure data storage discussed above may be rights that are preferably inalienable.[154]

There is a logic of ordinary morality that applies by extension to the normative language of data privacy. For example, there are important differences between preferences and entitlements. Websites that mistreat personal data are not merely subverting consumer preferences but are violating consumers' perceived rights. This is morally offensive. Many consumers prefer that Amazon charge less for shipping and handling, but they do not feel morally outraged when Amazon fails to oblige because they are not entitled to this treatment. Consumers do increasingly feel entitled to the specific respectful treatment of their data.[155] One Internet entrepreneur summarized Internet firms' growing recognition of consumer feelings: "Companies used to think of customer data as theirs. They're starting to realize they're really custodians, and the customer controls the information."[156]

Consumers currently have little legal recourse, but they may nevertheless possess a moral response that is, from the website's perspective, functionally equivalent. Morally speaking, consumers will disdain disrespectful websites. They will view such websites as less reputable, trustworthy, and worthy of continued business relationships. More aggressive consumers may feel that disrespectful websites deserve to be sanctioned or otherwise reciprocally ill-treated.[157]

We are now in a better position to understand the distinct and interrelated functions of privacy proselytizers. First, proselytizers sought to educate the public about the causal connection between website data-collection activities and individual privacy. Advocates then sought to

---

65 (1999). Such a right would be in tension with the First Amendment, however. *See generally* Volokh, *supra* note 68.

154. *See, e.g.* Samuelson, *supra* note 26, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights.").

155. Opinion polls show increasing public concern with respect to online privacy. *See* Glenn R. Simpson, *E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise,* WALL ST. J., Jan. 6, 2000, at A24. A recent poll found that 92% of Internet users were uncomfortable about websites sharing personal information with other sites. *Business Week/Harris Poll: A growing threat*, BUS. WK. ONLINE, Mar. 20, 2000, *at* http://www.businessweek.com:/2000/00_12/63673010.htm?scriptframed.

156. *Sellers Try to Soothe Fears About Personal Data Safety*, USA TODAY, Apr. 27, 2001, at 2B (quoting Hans Peter Brondmo).

157. *See* sources cited *supra* note 15.

highlight that websites were morally harming the public through their activities. Activists further taught that consumers have a moral entitlement to a reasonable degree of control over their personal data. The following section will discuss a consequence of this moral connection: consumers utilize their strategic leverage over websites to further their moral rights and entitlements to privacy.

D. Data Privacy Rights Create a Strategic Interaction of Respect and Trust

An important strategic implication follows from the activities of privacy activists in creating a sense of consumer entitlement to personal data. As previously discussed, consumers did not view their relationship with websites as strategic until they perceived it as a moral relationship. But once consumers perceive websites as either respecting or disrespecting them, they will respectively trust or distrust websites. The more strongly consumers feel a data privacy entitlement, the more they will be morally affronted by instances where websites disrespect their privacy. Accordingly, they will be slower to trust websites and more inclined to punish those that fail to show respect. Retaliation may take the form of negative gossip or providing false or misleading information to the website.[158]

The notion of website visitors choosing to trust is similar to Richard McAdams's idea that actors can choose whether to esteem another party with whom they are interacting.[159] Note, however, that whereas McAdams plausibly contends that the desire for esteem is a brute preference that a rational actor might prefer for its own sake, I am not asserting that trust is something that websites would independently desire. Rather, a website would prefer to gain the trust of its visitors because this trust will be posi-

---

158. *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and Practice*, 7 J. INTELL. PROP. L. 57, 62 (1999).

> The obvious product of this distrust is that people avoid disclosing personal information by opting against online transactions and website registration. Less obvious but equally troubling for online marketers is the 'garbage in' syndrome: in two recent surveys, over forty percent of Americans who registered at websites admitted to providing false information some of the time, mainly because of privacy concerns; the figure for European registrants was over fifty-eight percent . . . . The message to marketers is clear: if you want useful and accurate data, earn it by assuring consumers that you will use it appropriately.

Id.

159. *See* McAdams, *supra* note 71, at 355-72. Similarly, Cooter's internalization account appears not to play a role as websites are commercial enterprises that are not readily susceptible to the psychological phenomenon of internalization. *See* Cooter, *supra* note 90, at 1690-94.

tively correlated with these visitors choosing to interact with the website in the future. In other words, websites hope to signal to consumers that they are desirable partners with whom to cooperate.[160] The situation becomes strategic because the website is then in the position to choose whether to respect the consumer and engender consumer trust.[161] Part of the website's choice to show respect, or not, will depend in part on its calculation of how much its choice will cause the consumer to trust the website, and how much the resultant cooperative opportunities are worth to the website.[162] The strategic structure of the situation is represented in Figures 3 and 4.

Figure 3: Large Website/Consumer Strategic Interaction

		Large Website: Privacy Policy	Large Website: No Privacy Policy
Visitor	Trust	3, 3	1, 4
	No Trust	3, 1	1, 2

Figure 4: Small Website/Consumer Strategic Interaction

Small Website: Privacy Policy	Small Website: No Privacy Policy

160. On signaling theory, see *supra* note 92. *See generally* POSNER, LAW AND SOCIAL NORMS, *supra* note 133.

161. *Gallup Poll Uncovers Opportunities to Build Consumer Confidence in 2001 by Implementing Best Practices for Online Privacy*, PR NEWSWIRE, Jan. 16, 2001.

162. Prior to the burst of the Internet bubble, the mere eventuality of future visits to the site in itself was money in the bank, as Internet companies were valued in the market in important part based on the number of "hits" the site received.

Visitor	Trust	2, 2	1, 4
	No Trust	2, 1	1, 3

Each party has two choices, each affecting the utility of the other party. Thus, each party needs to think about how its choice and the choice of the other party will affect its payoff. This means that each party considers whether they can affect the other's choice to improve his own outcome. Specifically, the website will consider whether it should attempt to foster consumer trust, and the consumer will consider whether it can influence the website's choice to provide a privacy policy.[163] Once the consumer appreciates that the website's actions will affect her outcomes, she will either withhold or bestow trust to incentivize the website to show respect.

Because of these mutually affecting choices, a greater number of websites may find it in their interest to respect privacy in order to maintain the trust of the increasingly educated, and demanding, consumer.[164] Indeed, the number of websites that show respect for privacy has continued to grow as public consciousness of the issue of online privacy has grown.[165] Note that as recently as a few years ago, only a minority of websites—the larger and better-known websites—offered privacy policies.[166] This makes sense because these websites are most likely to have overlapping, multifaceted interactions with consumers; thus making it crucial for these websites to have respectful and trustworthy reputations.

---

163. As the above discussion has indicated, there are different ways to respect privacy. A privacy policy will be used in the example as it is the most basic means.

164. *See supra* note 18 (discussing how some companies are hiring Chief Privacy Officers).

165. *See generally* 1999 FTC REPORT TO CONGRESS, *supra* note 67.

166. In the Federal Trade Commissions's 1998 study, only 14% of websites were addressing consumer privacy issues. 1998 FTC REPORT TO CONGRESS, *supra* note 2. As the consumer sense of entitlement grows, the chances of plaintiffs' lawyers prevailing in lawsuits grows. *See* Matt Fleischer, *Lawyers Eye Privacy Cases Against Many DoubleClick Rivals*, 22 NAT'L LAW J. no. 27, at A1 (Feb. 28, 2000) (noting many lawyers are now searching for the next privacy lawsuit against DoubleClick competitors, such as Engage, 24/7 Media, MatchLogic, Flycast, and L90, each collecting over 100 megabytes of clickstream data-information per day).

That websites place a premium on consumer confidence is readily indicated by the extent to which they attempt to acquire it deceptively. Many firms have deceptive privacy policies. In other words, the firm wraps itself in a cloak of respect by means of the privacy policy, and yet the actual terms of the policy are "lawyered" such that the firm does whatever it pleases with personal data.[167] The most egregious, publicly-known case occurred recently. Toysmart.com explicitly promised not to sell data: "[p]ersonal information voluntarily submitted by visitors . . . is never shared with a third party."[168] In bankruptcy, Toysmart then attempted to sell this data.[169] Despite the sense of consumer entitlement, many small websites may still prefer to avoid the expense of providing privacy policies. As illustrated in Figure 4, many small websites may still prefer the outcome of mutual non-cooperation (southeast cell) to that of mutual cooperation (northwest cell).

As a result of privacy proselytizers, a situation has emerged in which there are two types of norms. Previously, there were simply permissive norms whereby websites did whatever they wanted with personal data without regard for consumers. Now new, more respectful, norms are emerging. For simplicity's sake, the previous discussion focused solely on

---

167. *See* Schwartz, *supra* note 20, at 824.

> In light of these flaws, the true argument in favor of the Privacy Policy can only be as follows: when a Web site says something about its data processing practices—even if this statement is vague or reveals poor practice—the visitor to the site is deemed to be in agreement with these practices so long as she sticks around . . . . Thus, a site that said 'we reserve the right to do whatever we want with the information we collect' [is] deemed to have provided notice of information practices.

Id.

168. Toysmart Privacy Statement, *at* http://www.ftc.gov/os/2000/07/toyexh1.pdf.

169. *See FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, (July 21, 2000) *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm; *Judge Is Urged to Reject Toysmart.com Settlement*, WALL ST. J., Jul. 26, 2000, at B2; *Toysmart.com's Plan To Sell Customer Data Is Challenged by FTC*, *supra* note 56, at C8. In addition, Toysmart faced a lawsuit filed by TRUSTe, which contended that Toysmart was in violation of its online agreement not to sell consumer data to third parties. *See* Elinor Abreu, *TRUSTe to File Antiprivacy Brief Against Toysmart*, INDUSTRY STANDARD, June 30, 2000, *available at* http://www.thestandard.com/article/display/0,1151,16577,00.html. *See generally* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1180 (1997). This example demonstrates how non-internalized the norm is for a website. This is a difference between humans and firms. Once internalized, a human conforms to a norm in a manner that cannot be readily changed. A firm's commitments can completely change with the installation of new management.

the provision of privacy policies. But as already mentioned, there are many actions websites may undertake in order to demonstrate their respect. Although this represents significant moral progress from a privacy activist perspective, a major problem remains. New, more respectful norms are now in play, but so, too, are the old nonrespectful norms.

Part IV will demonstrate that while the privacy activists may not themselves have the resources to push for universal conformity to respectful norms, these norms have taken on a life of their own. The result is that other norm entrepreneurs find it is their interest to get involved in promoting these norms. Part IV describes how both the FTC and various private companies have come to have an interest in further promoting those more respectful data norms first proselytized by the privacy activists. Before examining these norm entrepreneurial activities, however, consider briefly one additional force that may cause websites at the margin to switch to more respectful norms as a consequence of the initial efforts of the privacy activists.

E. Causal Feedback Loop Leading Toward Pooling Equilibrium

There is an apparent causal feedback loop operating: as more respectful practices emerged, consumers have become informed about online privacy, and consequentially increasingly demanding of their privacy.[170] In a criminal law context, Dan Kahan observes a parallel phenomenon whereby a rise in crime makes social sanctions less powerful, which leads to more crime.[171] In the situation described by Kahan, the causal feedback loop leads to normative breakdown. Richard McAdams describes a similar dynamic involving social norms pertaining to wearing fur and smoking cigarettes.[172] McAdams plausibly observes that these are activities in which the more people shun the behavior, the more negative the impact felt by remaining participants in the activity. This puts greater pressure on these remaining participants to abandon the activity. Depending on the utility functions of the remaining participants, the greater pressure may induce some to abandon the activity. Through continued iterations of this causal loop, all participants may, over time, defect from the activity. Alternatively, some stalwarts may have strong preferences that continuously outweigh all pressures to defect. After a time, a new equilibrium may re-

---

170. *See* Buxbaum and Curcio, *supra* note 93, at 411-12 (arguing that the appearance of privacy policies would create an expectation of privacy).

171. *See* Dan Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem,* 67 U. CHI. L. REV. 607, 611-18 (2000).

172. *See* McAdams, *supra* note 71, at 366.

sult such that these are stable populations of conformers and nonconformers.

A parallel dynamic in website privacy practices seems to be under way. As the number of websites providing privacy policies increases, the more intense will be the perception that the remaining websites are disrespectful of consumer interests. Increasingly, websites without a policy will be outliers in their disregard for consumer privacy interests. This will likely cause an increasing number to alter their behavior, possibly leading to a tipping point where most websites begin to take privacy more seriously.[173]

Whether such a feedback loop is in operation is an important question. The previously described process is self-regulating in the sense that the impetus toward the new norms comes from informal social forces rather than formal legal methods. One criticism occasionally made of self-regulation is that while it may work to motivate many, or even most, players to act in a cooperative fashion, there will still be some players—the "bad actors,"—who fail to conform. Due to the causal feedback mechanism, there may be the potential for the "bad actors" to become cooperators. For example, this may already be occurring among the participants in the Network Advertising Initiative, an industry group formed to agree on acceptable forms of privacy protection. A commentator suggested that the 10% of advertisers who did not initially comply with the industry guidelines might be led by "centrifugal force" to go along, or risk losing both respect and business.[174]

IV. STRENGTHENING THE PRIVACY ENTITLEMENT FOR NON-MORAL REASONS

A. The FTC's Threat Model of Privacy Entrepreneurship

The FTC has recently acted to reinforce the privacy promoting efforts of the privacy activists. Privacy activists are motivated because they care

---

173. This is modeled by the critical mass phenomenon of "tipping." *See* THOMAS C. SCHELLING, MICROMOTIVES AND MACROBEHAVIOR 102-04 (1978). Tipping occurs when the success of a social practice depends on the formation of a critical mass, and enough actors sign on or sign off such that the practice succeeds or fails. If enough actors sign on, the activity is tipped in. If enough actors sign off, the practice is tipped out. Because a relatively small number of crossover actors may cause a norm to tip, social norms may shift relatively suddenly. *Id.*

174. David Stout, *Government and Internet Ad Group Reach Agreement on Data Gleaned from Web Surfers*, N.Y. TIMES, July 28, 2000, at C6.

deeply about privacy. What could motivate a federal government agency to promote more respectful online personal-data practices? Elsewhere, I have argued that public choice theory provides a plausible answer: the FTC has sought to become the leading federal agency regulating online activities as a means of extending its regulatory grasp to the fertile new domain of the Internet.[175] The FTC's role in helping to moralize the social meaning of data collection can also be understood in public choice terms as an effort to extend the agency's purview over the burgeoning website industry.

As an indirect result of privacy advocacy, Congress asked the FTC to examine online privacy issues.[176] Voters are increasingly contacting their congressional representatives and voicing concerns about online privacy.[177] These concerns have translated into increased agitation on Capitol Hill regarding online privacy. This agitation has resulted in proposed legislation and calls for FTC involvement. The FTC acts pursuant to its authority under the Federal Trade Commission Act, which mandates that the agency address "unfair" and "deceptive" trade practices.[178] Generally speaking, the FTC's hook into the privacy debate comes by means of casting website data-gathering practices as potentially unfair and deceptive.[179] In particular, the agency has borrowed the various specific privacy protection measures supported by the privacy activists and shrouded them in the

---

175. *See* Hetcher, *supra* note 25, at 2053.

176. In a series of hearings in October and November of 1995 the FTC reported to Congress on consumer protection issues, including privacy concerns. *See Prepared Statement of FTC on "Internet Privacy" Before the House Comm. on Judiciary* (Mar. 26, 1998) *at* http://www.ftc.gov/os/1998/9803/privacy.htm. Brian Krebbs, *IT Industry Council Signals Privacy-Law Advocacy,* NEWSBYTES, Feb. 2, 2001 (due to public outcry lawmakers are suggesting federal electronic privacy protections); *see also PrivacyRight, Inc. Forms Strategic Equity Partnership with Venture Factory*, PR NEWSWIRE, June 6, 2000; Rosalind C. Tritt, *Privacy: A Threat to Free Speech?*, PRESSTIME, Jan. 2001, at 27.

177. Rep. Billy Tanzan, CATO Online Privacy Workshop, Washington, D.C. (May 1999).

178. 15 U.S.C. § 45(a) (1994). The FTC prosecutes "[u]nfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce" under Section 45 of the Federal Trade Commission Act ("FTCA"). *Id.* Section 57(b) authorizes the prosecution of actions to enforce Section 45. *Id*. § 57(b). Section 57(a) permits the FTC to create rules to prohibit deceptive or unfair practice prevalent in certain industries. *Id*. § 57(a).

179. Note that the FTC's framework for regulating unfair practices does not require ownership of personal data. The fact that data subjects may have de facto control over their data is enough to generate an instance of an unfair or deceptive trade practice. This means that the agency may gain jurisdiction over website activities without a change in the intellectual property status of personal data.

rhetoric of fairness.[180] The FTC refers to standard proposed privacy measures as the fair information practice principles ("FIPPs").[181]

The FTC contends that these fair practices are best promoted through website privacy policies. In other words, websites should address the elements of notice, consent, access, security, and enforcement in the representations that they make to consumers in their privacy policy. A privacy policy that accurately and completely states the website's personal data practices would be in accordance with the principle of notice/awareness because once the consumer has notice of the website's practices, she can consent to the data exchange or exit the website. In addition, stipulations concerning access/participation to the user's personal data on file with the website can be set out in the privacy policy, as can stipulations concerning integrity/security and enforcement/redress.

Note that whereas the privacy activists promoted respect for privacy as the core moral concern, the FTC has shifted the moral focus from respect for privacy to a concern for fair practices. When websites take up the FTC's suggestion and seek to implement the FIPPs via privacy policies, the FTC's regulatory grasp is enhanced. Once websites make representations to consumers regarding their practices, the FTC has a claim to jurisdiction if the websites behave differently. From the FTC's perspective, the website has engaged in unfair and deceptive trade practices, which is directly within the FTC's jurisdiction.[182]

As a norm entrepreneur, the FTC faced a problem not confronted by the privacy activists: an unreceptive audience. As discussed in Part TwoII, privacy activists' audience is consumers. Consumers were[TENSE] naturally disposed to accepting the extension of the general right to privacy to the domain of data privacy in cyberspace and were thus generally receptive to such ideas. By contrast, the audience for the entrepreneurial efforts of the FTC were websites. Different websites had differ-

---

180. The FTC explicitly states that it takes its normative framework from the privacy policy community. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2.

181. 1999 FTC REPORT TO CONGRESS, *supra* note 67, at 3.

182. Lawsuits filed so far have involved more than simple unconsented data collection and use. *See In re* DoubleClick, Inc., Federal Trade Commission (filed Feb. 10, 2000), *at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Judnick v. DoubleClick, No. CV-421 (Marin Cty. Sup. Ct., filed Jan. 27, 2000), *at* http://www.perkinscoie.com/resource/ecomm/netcase/complaint1.pdf; Pamela Parker, *Doubleclick's Legal Troubles Deepen*, INTERNETNEWS.COM, *at* http://www.internetnews.com/bus-news/article/0,,3_299771,00.html (discussing four different cases against Doubleclick, Inc.); The Perkins Coie LLP Internet Case Digest, *at* http://www.perkinscoie.com/resource/ecomm/netcase/Cases-18.htm (summarizing other cases against Doubleclick, Inc.).

ing interests when it came to the provision of privacy protection for the online consumer. Generally, larger and more established websites had an incentive to provide privacy protections while smaller websites did not.[183] Importantly, the FTC's preference for websites to incorporate the FIPPs into online privacy policies provided no additional incentive to the smaller websites to provide such protections. The FTC addressed this impediment by creatively utilizing the unique resources available to it as a federal agency: it issued a threat to the website industry.[184]

In 1998, the FTC threatened to recommend to Congress that it enact privacy legislation if more respectful industry customs were not forthcoming through industry self-regulation. The threat was highly credible and particularly salient due to the Commission's recent success in shaping legislation to protect children's online privacy.[185] This threat was a shock to the normative equilibrium of the website industry, causing many firms to alter their behavior. Generally, the impact of the FTC's threat correlated with website size and structure. The larger and more multi-faceted a website's activities, the more likely it was that the website reacted to the FTC's threat by providing more respectful privacy practices.

Some large websites felt so threatened that they personally attempted to incentivize smaller websites into compliance with more respectful

---

183. Large sites are prominent and they would run the risk of coming under FTC scrutiny for questionable, albeit legal, trade practices, were they to fail to make a respectable effort to show respect for user privacy, as newly spelled out by the FTC, in its fair information practice principles. In contrast, small websites would plausibly having a dominating preference to not provide privacy policies. Because they are small, they will be able to fly under the FTC's radar. With the FIPPs, the FTC had merely outlined the principles that it contends are fair. It did not mandate them.

184. *See* Hetcher, *supra* note 25.

185. In 1998, after finding self-regulation of children's online privacy to be inadequate, the FTC recommended to Congress that it create legislation, which Congress quickly did, enacting the Children's Online Protection Act ("COPPA"). On October 21, 1998, the President signed COPPA into law. Children's Online Privacy Protection Act of 1998 Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L. 105-277, 112 Stat. 2681, 2681-728 (codified at 15 U.S.C. §§ 6501-6506) (Oct. 21, 1998).

> The stated goals of the Act are: (1) to enhance the parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent.

144 Cong. Rec. S12741-04 (Oct. 21, 1998) (statement of Sen. Bryan).

norms. Under this threat, the major websites are no longer indifferent to the actions of the smaller websites. The failure of these smaller websites to adopt privacy-respecting practices might lead to privacy legislation, which would adversely affect *all* websites. The large websites in particular would have the most to lose from onerous legislative requirements. Faced with this situation, large websites devised methods to bring small websites into conformity with more respectful data collection practices. Large websites threatened to withhold advertising from websites that did not demonstrate adequate respect for privacy.[186] As represented in Figure 5, this action changed the strategic structure of the relationship between large websites and small websites.

186. *See* Hetcher, *supra* note 25, at 2047.

Figure 5: Intra-Industry Strategic Threats

		Large Websites: Privacy Policy	Large Websites: No Privacy Policy
Small Website	Privacy Policy	4, 4	3, 2
	No Privacy Policy	2, 3	1, 1

The threats issued by some key large websites likely contributed toward the desired outcome, as an increasing number of small websites are now offering privacy policies. As indicated by the FTC's 1999 Report to Congress, the number of websites providing privacy policies has increased significantly. Regarding the issuance of threats by large websites, the FTC stated that "Companies like IBM, Microsoft and Disney, which have recently announced, among other things, that they will forego advertising on websites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues."[187]

Note that when large websites threaten to withhold advertising from small websites, the effectiveness of the threat does not depend on repeated interaction between the parties. Even if the small websites only interact once with Microsoft or IBM, they will typically prefer that this interaction permit advertising. In the terminology of informal game-theory, the instrumental allocation of advertising is functioning like a "selective incentive" that rewards cooperative behavior on an individual basis.[188] Selective incentives allow the party seeking to incentivize conformity to provide incentives to individuals in order to elicit their conformity. This is in contrast to the collective good itself, which by definition is a public good: when provided for one, it is provided for all, and thus is open to free riders.

---

187. *Id*.

188. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1965); Lessig, *supra* note 5, at 996.

This type of selective incentive cannot be expected to work for all small websites. Some small websites will have little prospect of receiving advertising revenue from large websites and benefit extensively from the unfettered use of personal data. These websites may continue to have a dominating preference to free ride on the growing practice of providing privacy policies. Thus, the net result of the FTC threats was still a bi-normative world in which many large websites and some small websites are respectful of privacy while other small websites are not. More recently, however, a growing number of the recalcitrant websites do appear to be conforming to more respectful privacy norms.[189] The final section will explore another important process that appears to be contributing toward this development.

B. Software Makers Promote Privacy for Profit

A new type of privacy norm entrepreneur has recently emerged. These are software vendors marketing so-called "privacy solutions."[190] Privacy solutions are software that users or websites can install to create a more privacy-respecting online environment. The following discussion provides an examination of the advertisements placed by some of these software vendors for their products in tech-oriented magazines. Looking at the text of these advertisements serves two purposes: it provides strong evidence of privacy proselytizers' success in moralizing data privacy and suggests new methods by which these moralized norms may be further entrenched.

The ultimate audience for this growing type of advertisements is often websites, as they are the direct purchasers of these products. Due to the viral nature of norms, it is also integral that these advertisements impact consumers. The more the advertisements are successful in fostering moral concern among consumers, the greater the social pressure toward increased privacy protection that will be exerted on the website industry. As the price of not providing privacy increases, the number of websites that

---

189. 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 17.

190. John Graubert & Jill Coleman, *Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet*, 25 CAN.-U.S. L.J. 275, 290 (1999) ("In the case of Internet privacy, several technologies potentially capable of protecting the online privacy of consumers are evidently already on the market or under development. Technology-based privacy solutions may eventually provide consumers with the confidence and security that they need to conduct business on the Internet on a global scale."); *see P3P: Just a Start*, ZDWIRE, Jul. 17, 2000 ("There's no disputing that privacy has emerged as a leading issue of the Internet age. A whole industry is springing up around it, with software and service providers rushing to offer the latest and greatest solution for protecting an individual's personal information and identity online.").

will have the balance favoring of respectful over nonrespectful norms will increase.

Particularly striking is the overt normative language used in the advertisements that dramatically inform consumers that they are being disrespected by many websites. For example, consider the representative advertisement by the firm, ZeroKnowledge.[191] It depicts an average Internet user, unremarkable except for the bar code emblazoned on her neck. The text consists of a small number of rhetorical statements made by a representative online consumer to the website industry: "I am not a pair of eyeballs to be captured or a consumer profile to be sold . . . . I am not a piece of your inventory . . . . I will not be bartered, traded or sold."[192] These phrases play on current website industry jargon, in which customer visits are referred to as "capturing eyeballs," and personal data is amassed into "consumer profiles."

The theme of these statements is aptly viewed in everyday Kantian terms. The consumer is demanding more respectful treatment. As portrayed, these firms equate her with her data in contravention of the Kantian maxim that actors should not treat persons merely as a means to their own ends.[193] The import of the advertisement is that typical websites currently treat people not as individuals, but instead as "inventory" that can be bar-coded and bartered, or as "eyeballs" that can be "captured."

The advertisement then contrasts these industry attitudes with the normatively acceptable position as portrayed by a representative consumer speaking rhetorically to the website industry. "I am an individual and you will respect my privacy."[194] This brief statement contains three normatively loaded words: "individuals," "respect" and "privacy."[195] The final claim is that "On the Net, I am in control."[196] This statement is, of course, aspirational, as the whole force of the advertisement is that the woman is not presently in control of her personal data. By demanding her moral

---

191. ZeroKnowledge, Inc., Advertisement, WIRED, Aug. 2000, at 5-6. ZeroKnowledge Systems lets Internet users surf the net anonymously. *See* http://www.zeroknowledge.com (last visited Sept. 4, 2001). Zero-Knowledge Systems' Freedom software uses the encryption and several different computers to mask its users' identities even from itself. *Id.* The Freedom IP overlay network opens up an anonymous route, with encryption, from server to server. *Id.*

192. *Id.*

193. IMMANUAL KANT, THE METAPHYSICS OF MORALS 187-89 (Mary Gregor trans., Cambridge University Press 1991) (1797).

194. ZeroKnowledge, Inc., Advertisement, WIRED, Aug. 2000, at 5-6.

195. *Id.*

196. *Id.*

rights when it comes to online privacy, she in effect admonishes the reader of the advertisement to do the same.

The advertisement by the company Netcreations, a provider of a permission-based email marketing system, similarly invokes an everyday Kantian theme.[197] Netcreations promotes itself as providing consumers with only the information they have asked for. As contained in this article's epigram, the advertisement features a picture frame with the following tenets set out as its "Code": "This is not Cattle. This is a human being. We do not spam human beings. We respect human beings. Respecting human beings is good business. This is the code."[198] The advertisement strives to convince the website industry that privacy-respecting practices are also good for business. As the advertisement says, "[w]hat is right is also effective."[199]

A similar effort is made by a firm named PrivaSeek.[200] In a series of advertisements, PrivaSeek promotes technology that will give consumers control over their online profiles.[201] The advertisement notes that, "[c]onsumers are becoming more savvy about protecting their personal information online."[202] PrivaSeek's product is geared toward this changing privacy environment because it promises to increase the "confidence" of customers.[203] "Confidence" is a term that is often used in the business-to-business software market that supports secure online transactions. PrivaSeek plays on websites' desire for consumers to have confidence in them, so that consumers will readily interact with websites on a repeated basis.

In conclusion, each software privacy solutions provider will likely influence privacy norms by further stoking consumer privacy concerns and the corresponding entitlement to personal data. In other words, the advertisements will further advance the shift in the social meaning of personal data collection toward a more normatively-charged interpretation.[204] Although there is no hard data, these advertisements will likely have an effect in further galvanizing public opinion in the direction of greater de-

197. Netcreations, Inc., *supra* note 1.
198. *Id.*
199. *Id.*
200. PrivaSeek, Inc., Advertisement (on file with the author).
201. *Id.*
202. *Id.*
203. *Id.*
204. The strong moral tone of these advertisements is seen by contrasting them with ads meant to alert users to security issues. Here the threatening activities are illegal and the need is to protect oneself from theft. There is no attempt to create moral outrage on the part of consumers in the text of these advertisements.

mand for more respectful website privacy practices. For websites at the margin, it may now make sense to switch to more respectful norms. Thus, while companies selling privacy solutions may lack the lobbying savvy of organizations like EPIC or the coercive power possessed by the FTC, they may nevertheless be powerful shapers of public norms regarding online privacy due to their ability to directly reach millions through their print media campaigns.

V. CONCLUSION

There have been important changes in informal online privacy regulation over the past few years; primarily the recognition of a moral entitlement to privacy in cyberspace. This Article has argued that privacy norm proselytizers are the leading contributors to this development. These activists have taken an interest in online privacy because they believe Internet users are morally entitled to, and desperately in need of, increased protection. Other norm entrepreneurs have subsequently supported an entitlement to privacy for reasons less moral, but no less efficacious in stimulating demand for increased privacy protections.

As a result of these efforts, Internet users are increasingly conscious of moral entitlements to respectful treatment by websites. The general social demand for privacy respect in cyberspace is half of a broader supply and demand model documenting the emergence of Internet privacy norms. While this Article has begun to address the response on the part of websites to the growing demand for privacy, a more detailed analysis of the supply side is necessary in order to address a puzzle that has been created by the foregoing account.

Privacy activists have not been impressed with the response by websites to the increasing demand. They allege that websites have only made reluctant and ineffectual efforts to respect users' privacy interests. The puzzle is why the substantial increase in demand for online privacy has not resulted in a corresponding increase in the supply of online privacy, as a market model would naturally suggest. This important issue should be addressed in future research on the emergence of online privacy norms.