Harvard Journal of Law & Technology
Volume 15, Number 1 Fall 2001
PAGE LAYOUT AND NUMBERING DO NOT CORRESPOND TO ORIGINAL

CHANGING THE SOCIAL MEANING OF PRIVACY IN CYBERSPACE

Steven Hetcher*

TABLE OF CONTENTS

---

* Associate Professor of Law, Vanderbilt University Law School.

> *Information privacy is a social goal, not a technological one. To achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data*.[1]

I. INTRODUCTION

The threat to personal privacy caused by the ever-expanding flow of personal data online is the most significant public policy concern spawned by the Internet. In the past few years, websites increasingly have claimed to address this concern. Privacy advocates, however, have been unimpressed with these efforts. Some commentators have claimed that the industry's new data norms are pathetic and insincere attempts to address burgeoning privacy concerns. Jessica Litman states that industry self-regulation has been an "abject failure."[2] Whether the new website norms really do increase the supply of privacy is a contentious matter that will be addressed below. It is beyond contention, however, that the website industry has responded to demands for greater online privacy with a new set of industry norms regarding the collection and use of consumer data. This Article will seek to explain what has motivated the emergence and adoption of these new norms.

This project fits within a larger supply and demand analysis of the emergence of website privacy norms. Earlier research has focused on the demand side of the equation.[3] The focus here is on the supply side. After an introduction to the rational choice approach to privacy norms, Part II will consider the role that norm proselytizers and other norm entrepreneurs have played in stimulating consumers to demand online privacy with respect to their personal data.[4] The word "proselytize" is

---

1. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1169 (2000).

2. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2000).

3. *See* Steven Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERKELEY TECH. L.J. 877 (2001) [hereinafter Hetcher, *Norm Proselytizers*]; Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000) [hereinafter Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*]. *See generally* Robert Ellickson, *The Market for Social Norms*, 3 AM. LAW & ECON. REV. 1, 2 (2001) (setting out a supply and demand model for norm emergence).

4. Norm entrepreneurs are actors who promote the change of norms. *See* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909 (1996). Norm proselytizers promote norms for moral reasons that they themselves accept. Norm proselytizers, then, are a sub-category of norm entrepreneurs. Privacy activists have

appropriate because it would be reductionist to describe these entrepreneurs as merely fostering preferences for data privacy. Privacy norm proselytizers seek to arouse the moral consciousness of consumers vis-à-vis websites' collection and use of personal data.[5]

Part III will examine the increase in the supply of privacy-related norms by websites in response to this increased demand.[6] Whether these privacy-related norms are respectful of privacy is a complex question. In the view of their critics, the vast majority of websites have yet to display any genuine regard for the privacy interests of users. If the critics are right, this raises an interesting question: Why has an increase in demand not created an increase in supply?

One possible answer is that websites think it is in their interest to simulate privacy respect rather than provide the real thing. Part IV will consider two competing accounts of why websites might think that it is sensible to simulate respect for their users' privacy. The two accounts are derived as applications of two competing theories of norms. Under one theory, norms are patterns of rationally-motivated conforming behavior.[7] Under the other theory, norms are sets of individual signaling

---

functioned as norm proselytizers. *See* Hetcher, *Norm Proselytizers*, *supra* note 3, at 907. Ellickson seeks to develop a richer vocabulary by distinguishing among a variety of specialists who supply new norms. *See* Ellickson, *supra* note 3, at 10–12. "Change agents" are actors or enforcers who are relatively early in supplying a new norm. Ellickson distinguishes among these subcategories of change agents: self-motivated leaders, norm entrepreneurs, and opinion leaders. The following discussion will indicate that some of these subcategories may be 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. Traditional economic analysis has shied away from the topic of preference formation, but this is changing. *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 . . . . But with few exceptions, economists and political scientists pay little attention to the structure of preferences."). *See generally* JON ELSTER, SOUR GRAPES (1983).

6. *See* Samuelson, *supra* note 1, at 1163 ("The more enlightened private sector firms are coming to realize that fuller adherence to privacy principles will promote consumer trust which will, in turn, promote commerce."); Shaun A. Sparks, *The Direct Marketing Model And Virtual Identity: Why The United States Should Not Create Legislative Controls On The Use Of Online Consumer Personal Data*, 18 DICK. J. INT'L L. 517, 549 (2000) ("In the practical terms of the online environment, however, consumers have the option of choice. Unlike forced commercial interactions with utility-like cable providers, consumers may interact only with those websites that are to their liking. Websites that post adequate privacy policies, and adhere to them, will earn consumer trust and consumer dollars. Online businesses are increasingly aware of that concern, and will compete in the arena of privacy service in the same manner in which they compete on terms such as price.").

7. *See* Steven Hetcher, *Creating Safe Social Norms in a Dangerous World*, 73 S. CAL. L. REV. 1, 78 (1999) [hereinafter Hetcher, *Creating Safe Social Norms*]; Steven

acts, each of which is meant to communicate that the signaler has a low discount rate and thus is a good type with whom to enter into cooperative relationships.[8] As later discussion will demonstrate, each of these conceptions of a norm provides a distinct explanation of the dubious quality of most extant website privacy norms.

Part IV will conclude with a consideration of the normative implications of the preceding analysis for privacy proponents of various stripes. Advocates for all the competing substantive views regarding online privacy will find it useful to understand what has caused websites to pay more attention to consumer privacy. With this knowledge in hand, privacy activists will be in a better position to further influence the course of website activities toward the provision of greater privacy protections. Cooperative websites will be in a better position to understand the efficacy of their past response to the privacy demands of consumers, with an eye toward adapting their response in the future. Unfortunately, websites that adopt a deceptive strategy also will benefit from this understanding. The supply-side account of Internet privacy also will be of interest from a more general, social-scientific perspective due to a dearth of case studies on the emergence of norms in an online setting.[9]

Hetcher, Norms (1991) (Ph.D. Dissertation, University of Illinois) (on file with the author) [hereinafter Hetcher, Norms].

8. *See generally* ERIC A. POSNER, LAW AND SOCIAL NORMS (2000) (articulating a signaling theory account of emergence and maintenance of social norms).

9. *See* Mark A. Lemley, *Shrinkwraps in Cyperspace*, 35 JURIMETRICS J. 311, 314 (1995) ("In addition, the rapid growth in the number of network users has worked to transform cyberspace in important respects. With its forty or fifty million users, the Internet is no longer comprised of a limited set of close-knit communities in which private ordering can be based on shared values and understanding."). Ellickson has noted the importance of case studies for the further development of the law and norms approach. *See* Robert C. Ellickson, *Law And Economics Discovers Social Norms*, 27 J. LEGAL STUD. 537 (1998). Over the past forty years, law and economics has developed on twin tracks. On the one hand, it has developed at a theoretical level. On the other hand, it has developed through the explanation of an ever-expanding set of specific social institutions and practices. In the decade-old development of law and norms theory, it has developed along theoretical and applied tracks as well. While there have been numerous notable applications of the new law and norms theory, there is room for additional application of these theoretical accounts to new situations, both to illuminate the concrete situation and to help better understand the strengths and weaknesses of the competing theories of norms. Recent law and norms literature has included a number of significant case studies. *See, e.g.*, Robert Cooter & Janet T. Landa, *Personal Versus Impersonal Trade: The Size of Trading Groups and Contract Law*, 4 INT'L REV. L. & ECON. 15 (1984); Lisa Bernstein, *Merchant Law in a Merchant Court: Rethinking the Code's Search for Immanent Business Norms*, 144 U. PA. L. REV. 1765 (1996); Richard H. McAdams, *Cooperation and Conflict: The Economics of Group Status Production and Race Discrimination*, 108 HARV. L. REV. 1003 (1995); Mark D. West, *Social Norms in Japan's Secret World of Sumo*, 26 J. LEGAL

II. CREATING DEMAND FOR ONLINE PRIVACY

A. The Rational Actor Approach to Privacy Norms

A modified version of the rational actor approach to norms will be utilized in this Article.[10] As an introduction, this first part will survey briefly two related features of the rational actor approach that will prove to be of relevance to the topic of online privacy. The first is that norms are not linguistic rules but instead are patterns of behavior.[11] The second is that norms, understood as patterns of behavior, have rational structures.[12]

Until recently, rational choice theorists did not discuss norms. Norms were thought not to be in need of explanation but, instead, were to be avoided. They were viewed as dubious theoretical constructs that were employed in the explanations of a rival camp of social theorists comprised primarily of sociologists, anthropologists, and learning theorists.[13] These rival theorists are adherents to methodological holism, whereas rational actor theorists are resolute methodological individualists.

The contention that there is an inherent tension between norms explanations and rational choice theory is misguided. One source of this confusion is due to the fact that rational choice theorists have often conceived of norms as rules, that is, as prescriptive linguistic entities that are purported to act on the mind of the hearer.[14] It was altogether

---

STUD. 165 (1997). None of these case studies, however, has applied law and norms methodology in an online context.

10. The classic legal treatment of the subject is ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991). The classic non-legal treatments are EDNA ULLMANN-MARGALIT, THE EMERGENCE OF NORMS (1977) and RUSSELL HARDIN, COLLECTIVE ACTION (1981).

11. *See* Hetcher, Norms, *supra* note 7, at 1 (defining a social norm as a pattern of rationally or morally governed behavior maintained in a community by acts of conformity); *see also* Steven Hetcher, *Norms*, *in* ENCYCLOPEDIA OF ETHICS (2d ed, forthcoming, 2002).

12. *See generally* Hetcher, *Creating Safe Social Norms*, *supra* note 7, at 23.

13. *See* James Coleman, *Norms as Social Capital*, *in* ECONOMIC IMPERIALISM: THE ECONOMIC APPROACH APPLIED OUTSIDE THE FIELD OF ECONOMICS 133, 133 (Gerald Radnitzky and Peter Bernholz, eds., 1987) ("Especially for theories based on rational choice, invoking a norm to explain behavior constitutes an almost diametrically opposed approach. The rational choice theorist sees behavior as the result of choice made by a purposive actor; the social-norm theorist sees behavior as the result of conformity to norms"). *See generally* BRIAN BARRY, SOCIOLOGISTS, ECONOMISTS, AND DEMOCRACY (1978).

14. Sunstein, for example, conceives of norms as essentially rule-like. *See* Sunstein, *supra* note 4, at 14 (defining social norms as "social attitudes of approval and disapproval,

reasonable for law and economics scholars to conceive of norms as rule-like, given that this is often how norms have been characterized in the writings of social theorists of all camps.[15] There is a systematic ambiguity, however, in the social-scientific conception of a norm, between norms understood as rules and norms understood as patterns of behavior. The latter is the more significant conception of a norm and makes the most sense of online privacy norms.[16]

Once norms are properly understood as patterns of rationally governed behavior, the apparent tension between explanations that utilize norms and methodological individualism disappears. A pattern of behavior may be instantiated in a community even though no one explicitly formulates a linguistic rule, and a pattern of behavior need not be instantiated in a community despite the fact that a linguistic rule has been articulated.[17] In other words, the existence of a rationally governed pattern of behavior is logically distinct from the existence of a linguistic rule. A pattern of behavior is made up of all the particular bits that make up the pattern. Each of these bits is susceptible to explanation in terms

---

specifying what ought to be done and what ought not to be done."); *see also* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943 (1995). The rule view leads to a false conception of norm entrepreneurs as suppliers of norms. It will be easier to see that norm entrepreneurs do not supply norms if one keeps in mind the distinction between norms as linguistic entities and norms as patterns of behavior. A norm entrepreneur can bandy about a linguistic entity easily enough but it will be quite another thing to actually bring about a change in a pattern of behavior. It is only the websites themselves, for example, that can bring about changes in behavior of a sort that would constitute more respectful website privacy norms. *See* Hetcher, Norms, *supra* note 7 (providing the example of environmentalist promoting a no-litter norm, reaching the conclusion that it is only when the group participating in the littering practice stops the behavior that the norm itself can be said to have changed).

15. *See* Hetcher, Norms, *supra* note 7, at 8 (discussion of Max Weber and his leading American disciple, Talcott Parsons, as adherents of the rule conception).

16. Social norms theory has been the subject of a number of important recent symposia. *See generally Symposium: The Informal Economy*, 103 YALE L.J. 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 Nature and Sources, Formal and Informal, of Law*, 82 CORNELL L. REV. 947 (1997); *Symposium: The Legal Construction of Norms*, 86 VA. L. REV. 1577 (2000).

17. An example of the former is the set of norms governing interactions among cousins and other distant family members vis-à-vis flirtation and other forms of low-level romantic encounters. These norms are rarely articulated but are strongly felt and followed nevertheless. An example of the latter is a linguistic rule such as, "Turn the other cheek." If this is the stated rule, but in fact members of the relevant group do not live up to the dictates of the rule, we are typically disinclined to characterize the group as following the norm whereby people turn the other cheek. In other words, people look to actual behavior, not what people say, in order to determine whether some particular norm is instantiated in a particular group. *See* Hetcher, Norms, *supra* note 7, at 16.

of the individual interests promoted by it. Accordingly, the norm as a whole may be explained in rational choice terms.

In the sociological conception, norms purport to explain behavior by providing normative reasons for people to act.[18] For example, the reason that a person might pay taxes that she might otherwise avoid is that this person accepts the social norm that says that paying one's taxes is a requirement of civic duty.[19] By contrast, rational actor theorists seek explanations of behavior that do not rely on the motivational potency of moral duties of this sort. A rational actor theorist would contend that appealing to the norm of tax compliance has no real explanatory power, as this account fails to explain why the norm of paying one's taxes would hold sway over a rational actor in the first place. In other words, the rational actor theorist seeks an explanation as to why tax compliance is in an actor's individual self-interest. Once one has an account of why paying taxes is in one's interest, there is no need for the norm in the explanation. It is explanatorily redundant. The norm just describes the set of behaviors whereby a group of individuals each separately finds the act of paying taxes to be individually rational. A norm such as the norm of paying taxes will be maintained simply because it is individually rational to conform to the norm once it is up and running.

Likewise, although part of an individual's motivation to conform may be due to the conformity of others, this does not mean that others' conformity has any normative significance to the actor. Rather, the conformity of others may simply alter the strategic situation of the actor or provide the actor with valuable information on the advisability of conformity.[20]

Thus, norms understood as patterns of rationally governed behavior do not conflict with the rational actor approach. In this Article, norms, and in particular, website privacy norms, will be understood as patterns of behavior.

Judging by the sheer volume of literature, the pattern that has proven most useful in modeling interactions of interest to social theorists of various stripes is the iterated collective action problem or Prisoner's

---

18. *See* Coleman, *supra* note 13.

19. Eric A. Posner, *Symposium: The Legal Construction of Norms: Law and Social Norms: The Case of Tax Compliance*, 86 VA. L. REV. 1781, 1818 ("Paying one's taxes might mean discharging a civic duty . . . .").

20. Hetcher, Norms, *supra* note 7, at ch. 3 (There are three fundamental types of rational norms: sanction-driven norms, coordination norms, and epistemic norms. Each represents a distinct pattern of social behavior in terms of the characteristic reasons that motivate the rational actors who conform their actions to the pattern. With sanction-driven norms, actors conform due to the threat of sanctions. With coordination norms, actors conform in order to secure coordination benefits. With epistemic norms, actors conform in order to save on information costs.).

Dilemma. Initial inquiry into website privacy norms, then, might usefully proceed by seeking to determine whether important relationships in the context of the online privacy debate may be modeled as iterated collective action problems.[21] In one view, websites increasingly are offering privacy protections to consumers despite the fact that they might legally refrain from doing so.[22] There are costs associated with offering privacy protections.[23] Thus, assuming websites to be rational, they should explain what benefit they hope to gain as an offset to this cost. One possibility is that websites are seeking to enter into repeat-play cooperative relationships with their customers that can be modeled as iterated collective action problems.[24] This explanation might make sense of the apparent sacrificial behavior of some websites; they are incurring costs in the near term, the current game, in order to thereby entreat consumers to find them desirable partners with whom to enter into longer-term interactions or repeat games.[25]

This account faces a serious limitation, however, in that it may fail to explain the behavior of many, and perhaps most, websites. A prevalent complaint among privacy advocates about current website practices is that websites are not serious about privacy.[26] If this charge is accurate, it suggests that something unusual is going on. In the usual model of cooperation, when the rational actor foregoes a short-term gain in the hopes of thereby securing a long-term gain, she really does forego the short-term gain. The implication of the critique of the privacy

---

21. *See* Steven Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97 (2000/2001).

22. *See* Self-Regulation and Privacy Online: A Report to Congress (1999) [hereinafter 1999 FTC Report to Congress], *available at* http://www.ftc.gov/os/1999/9907/ privacy99.pdf.

23. *See* Ellen Messmer, *FTC Hearings Spotlight 'Net Privacy*, NETWORK WORLD, June 16, 1997; *see also* Craig Eddy, *A Critical Analysis of Health and Human Services Proposed Health Privacy Regulations in Light of the Health Insurance Privacy Accountability Act of 1996*, 9 ANN. HEALTH L. 1, 29 (2000) (although this article deals with providing the privacy protection required by the Health Improvement and Accountability Act, the analysis of the costs of such protections can be applied to all websites).

24. *See* Hetcher, *Norm Proselytizers*, *supra* note 3, at 921–24.

25. *See id*. Websites not only desire repeat play but repeat play with users behaving in a honest manner. *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 62 (1999) ("[I]n 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.").

26. *See supra* text accompanying note 2.

activists, however, is that websites are not really foregoing the short-term gain.

One possible explanation is that websites merely seek to pretend that they are interested in respecting user privacy. There may be good reason for a website to act in this duplicitous manner. The obvious reason is that the deceptive acts may fool users, such that they mistake the pretense for reality. These users may then cooperate with the website, thinking that the website is cooperating with them. Thus, deception appears to be a highly desirable strategy; the website gains the benefits of being a cooperator without incurring the costs of being a cooperator.[27] Understanding the actions of websites, then, may require determining whether they are best understood as seeking to simulate respect in order to trick users into turning over their data. Whether websites are best understood in this manner will be the main concern of Part IV.

First, however, in order to appreciate the pressures to be more respectful of privacy that are being brought to bear on websites, it will be necessary to examine in greater detail the demand for online privacy that has been stimulated in the past few years. Before websites will seek to become cooperators, either real of feigned, there must be a demand for their cooperation. In the initial period of website development, however, there was a lack of demand for privacy on the part of consumers.[28] This situation, and how it changed through the efforts of norm proselytizers and other norm entrepreneurs, will be explored in the next part.

B. The Social Meaning of Data Collection

The norms governing personal data interactions between consumers and websites have changed dramatically in the past few years. There is an increasing moral sensitivity among consumers regarding the collection and use of their personal data by websites.[29] Consumers now

---

27. As the old saying in moral theory goes, "All the advantages of theft over honest toil."

28. Hetcher, *Norm Proselytizers*, *supra* note 3, at 899.

29. 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* Litman, *supra* note 2, at 1283–86 (2000); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1465 (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

perceive a general right to privacy in cyberspace that includes respectful treatment of their personal data. In other words, the social meaning of personal data collection has changed from a morally neutral to a morally charged status.[30] This change is due to the actions of privacy norm proselytizers and privacy norm activists who possessed an interest in promoting online privacy.

The normative concepts that increasingly surround data collection are evidence that consumers are developing a more complex understanding of these activities. Most important, interactions between websites and their visitors are increasingly framed in terms of privacy.[31] In particular, commercial data collection is widely understood to raise concerns for a new species of privacy: informational or data privacy.[32] Not long ago, these expanded privacy concepts did not exist in either popular discourse or the lexicon of normative theory.

The more consumers feel entitled to data privacy, the greater their sense of 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.[33] Websites that do so may earn the trust and confidence of

---

detailed personal profiles. FTC, *Privacy Online: A Report to Congress* (1998) [hereinafter *1998 FTC Report to Congress*], *available at* http://www.ftc.gov/ reports/privacy3/priv-23a.pdf at 20.

30. *See, e.g.*, *The End of Privacy*, THE ECONOMIST, May 1, 1999, at 21; 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"); Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 182; Celia Santander, *Web-Site Privacy Policies Aren't Created Equal*, WEB FINANCE, Dec. 11, 2000. 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 ninety-two percent of Internet users were uncomfortable about websites sharing personal information with other sites. *Business Week/Harris Poll: A Growing Threat*, BUSINESSWEEK ONLINE, Mar. 20, 2000 *at* http://www.businessweek.com/ 2000/00_12/b3673010.htm.

31. *See, e.g.*, A. S. Berman, *Reports of Gates' Death Greatly E-xaggerated*, USA TODAY, Apr. 5, 2001, at 3D (quoting Microsoft spokeswoman Beth Jordan: "There'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. 173, 179 (1999) (quoting Marc Rotenberg: "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.").

32. *See* CMA Management Nov. 1, 1999, No. 9, Vol. 73; Pg. 13, *Embrace privacy; Brief Article* ("Concern about informational privacy in the marketplace has risen . . . .").

33. *See, e.g.*, Jeri Clausing, *Can Internet Advertisers Police Themselves? Washington Remains Unconvinced*, N.Y. TIMES, June 14, 2000, at C10 ("Marc Rotenberg, director of the Electronic Privacy Information Center, said Internet users should have the choice up front about whether they want companies collecting information about them online. And they should be able to have their profiles deleted upon request."); David Cohen, *Be Sure*

consumers.[34] Consumers who feel that they are disrespected, however, may seek to punish websites by providing them with false personal information[35] or sanctioning the website through negative gossip.[36]

Social meanings attach to social norms. Accordingly, one strategy for changing social norms is to alter their social meanings. For example, Larry Lessig discusses dueling by the aristocratic class in the Old South.[37] The dueling norm was resistant to legal prohibition; 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.[38] This changed the social meaning such that potential participants were

---

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.

34. *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 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.").

35. *See* 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, which states 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., Mar. 16, 2000; 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 & MKT. 1, Apr. 1, 2000, *available at* 2000 WL 23815801 (summarizing studies that found that "[w]hen 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").

36. *See* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 213–15 (1991).

37. *See* Lessig, *The Regulation of Social Meaning*, *supra* note 14, at 1025–34.

38. *See id.* at 968–73.

able to decline duels without losing honor due to the credible claim that the refusal was motivated by the prospect of holding public office.[39]

Social meanings are sometimes very difficult to change, however. 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.[40] As Dan Kahan notes, 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.[41]

Two differences exist between data-collection norms and norms such as gun possession and dueling, both of which uniquely complicate the privacy activists' task. First, 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 not to eliminate website data use, but rather to put this use on a firmer moral ground. Because websites benefit from disrespectful collection practices and the goal is not to eradicate data collection entirely, it seems especially difficult for privacy norm entrepreneurs to bring about a more respectful and nuanced result.

A generation ago, privacy advocates highlighted the threat that the U.S. government posed to privacy.[42] The threat arose from the government's plans to use computers to construct a comprehensive database of personal information on all citizens. While privacy activists

---

39. *See generally* Harwell Wells, *The End of the Affair? Anti-Dueling Laws and Social Norms in Antebellum America*, 54 VAND. L. REV. 1805 (2001) (discussing that fact that the "social norm" about dueling, including the consensus about what a gentleman ought to do to defend his honor and the consensus about what refusing a duel would mean, had changed).

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

41. *Id.* Likewise, with cigarette smoking, the challenge is to shift the social meaning away from its current status among teenagers as cool. The more that authorities try to control smoking, the cooler it may seem. *See* Lessig, *The Regulation of Social Meaning*, *supra* note 14, at 1025–34.

42. The privacy advocacy community began to form in the 1960s to fight against large-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 (1995); John Berard, Interview on Internet Privacy Issue, CNNfn Digital Jam (Feb. 5, 2000) (transcript #00021506FN-111), *available at* 2000 WL 4704461.

continue to perceive government as a threat to personal privacy, the focus of attention has changed in recent years to the private domain. The emergence of the Internet and the associated website industry have been the leading factors precipitating this shift. When government was the perceived threat, privacy activists successfully invoked the Fourth Amendment.[43] When the main threat came from private entities, however, legal claims in favor of data privacy have had little success. It has been argued that the websites violated one or more of the privacy torts,[44] engaged in unfair trade practices, [45] or committed trespass to chattels.[46] On the whole, none of these legal arguments has provided much protection against the majority of website data practices. Instead, privacy activists place great reliance on claims that website practices are immoral.[47]

1. Norm Proselytizers Create a Privacy Entitlement

Numerous public-interest organizations have identified online privacy as an important moral 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 Richard Smith and Marc Rotenberg, have become highly visible advocates for online privacy. Smith is a so-called ethical hacker, working to expose new forms of privacy invasion.[48] Rotenberg, the Director of EPIC, is the best known inside-the-beltway proponent of electronic privacy.

Privacy activists have functioned as industry watchdogs, legislative proponents, and have worked closely with the media. Activists have attempted to educate the public, politicians, and the media regarding

---

43. *See* Hetcher, *Norm Proselytizers*, *supra* note 3, at 908.

44. *See* In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

45. *See* Hetcher, *Norm Proselytizers*, *supra* note 3, at 908.

46. *See* Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, *in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW 2001, at 187, 217–18 (PLI Pat., Copyright, Trademark, & Literary Prop. Course, Handbook Series No. 632A, 2001); *see also* In re Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497.

47. Adapting an old adage, when the law is not on your side, argue the (moral) facts. On moral facts, see Llewellyn Joseph Gibbons, *No Regulation or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475 (1997).

48. *See, e.g.*, Frank James, *Privacy Champion Defeating Net Threats One by One*, SAN DIEGO UNION-TRIB., Computer Link, Apr. 18, 2000, at 10 ("Richard M. Smith is a software expert who doesn't fully trust his own kind. So he has launched a personal crusade to expose technology practices that threaten the privacy of millions of Internet users.").

certain factual issues relating to data collection and sought 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 these connections are not as obvious as with behaviors such as drunk driving; the potential harms from an inability to control personal data are not so readily apparent.[49] For example, 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 their employment opportunities.[50]

The bare knowledge of potential consumer harm does not inherently carry any moral implications. No moral implication follows, for example, from cardiac health advocates informing the public of the dangers of cholesterol. Thus, establishing a moral connection between website activities and consumer harms was a core goal of the privacy norm proselytizers. Norm entrepreneurs have advocated a moral relationship of responsibility between the data practices of websites and consumers' loss of privacy. They have steadfastly refused to dismiss consumer privacy loss as a necessary casualty of the emergence of electronic commerce.

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

---

49. *See* Mark A. Lemley, *Symposium on the Internet and Legal Theory: The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1276 (1998) (Norms are "particularly likely" to be inefficient "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."). As the discussion in the main text indicates, the norm of non-consensual website interaction may also stem from ignorance and moral insensitivity on the part of visitors of the data-collection practices of websites.

50. *See* Dan Stimson, *Internet Security an Issue for Telemedicine Success*, ALBUQUERQUE TRIB., Aug. 16, 1999, at A6 ("Exposure of private medical information can affect a person's ability to acquire employment."); Robert Pear, *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.").

story.[51] The company has subsequently been embroiled in lawsuits and subjected to a heightened level of scrutiny from privacy activists and the FTC.[52] Hackers also discovered that Microsoft was building a tracking utility into its software and that RealNetworks was tracking the online activities of its customers.[53] Once under the media spotlight, these companies quickly backed away from their planned activities.[54]

---

51. The price of DoubleClick's stock dropped precipitously as the story unfolded in the press, destroying billions of dollars in the company's market capitalization. *See The Internet's Chastened Child*, THE ECONOMIST, Nov. 11, 2000, at 80 (describing the fall of Kevin O'Conner, founder of DoubleClick, 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 anonymous. 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 fully with that of Abacus turns the acquisition, in the eyes of many, into a monumental flop.").

52. *See* Diane Anderson & Keith Perine, *Privacy Issue Makes DoubleClick a Target*, INDUSTRY STANDARD, Feb. 3, 2000; Will Rodger, *Activists Charge DoubleClick Double Cross*, USATODAY.COM, June 7, 2000, *at* http://www.usatoday.com/life/cyber/tech/cth211.htm (last visited Oct. 15, 2001); 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.

53. *See* David P. Hamilton, *The Gadfly: Privacy Cop Richard Smith Is Out to Keep Companies Honest – Whether They Like It Or Not*, WALL ST. J., July 16, 2001, at R10 (advocacy against RealNetworks and others); *Music Software 'Listens In' / RealJukebox Secretly Reported Listeners' Tastes*, NEWSDAY (N.Y.), 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 [transmitted] via the Internet to its headquarters."); *RealNetworks Is Target of Suit in California Over Privacy Issue*, N.Y. TIMES, Nov. 9, 1999, at C16 ("[A]fter 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.").

54. David E. Kalish, *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 ad 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

Privacy activists have engaged in legislative activities in an effort to promote laws that will create greater compatibility between positive law and the personal data norms that they promote. For example, Marc Rotenberg has repeatedly testified before Congress in support of privacy legislation.[55] Privacy activists were instrumental in lobbying for the enactment of the Children's Online Privacy Protection Act

---

Technology, a Washington-based group that tracks civil liberties on the Internet."). In another example, in bankruptcy proceedings, Toysmart.com recently moved to sell personal data it had collected pursuant to a specific privacy guarantee. *See Toysmart.com's Plan to Sell Customer Data Is Challenged by FTC*, WALL ST. J., July 11, 2000, at C8; *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 (last visited Oct. 3, 2001); *Judge Is Urged to Reject Toysmart.com Settlement*, WALL ST. J., July 26, 2000, at B2. While the FTC may settle, Toysmart still faces a lawsuit filed by TRUSTe, which contends that Toysmart is 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, *at* http://www.thestandard.com/article/ 0,1902,16577,00.html (last visited Oct. 3, 2001); *see also* Marcelo Halpern & Ajay K. Mehtova, *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 that after AOL users protested strongly to a proposed change in AOL's privacy policy permitting personal data sales to third parties, AOL decided not to alter their policy); Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 S.D. L. REV. 1153, 1180 (1997).

55. *See, e.g.*, *Security and Freedom Through Encyrption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Cts. & Intellectual Prop. of the House Comm. on the Judiciary*, 105th Cong., 113–18 (1997) (statement of Marc Rotenberg, Director, EPIC); *Cyber Attacks: The National Protection Plan and Its Privacy Implications: Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the Senate Comm. on the Judiciary*, 106th Cong., 46–53 (2000) (statement of Marc Rotenberg, Executive Director, EPIC); *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987, & H.R. 4908 Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong., 65–71 (2000) (statement of Marc Rotenberg, Executive Director, EPIC). Scholars have noted Rotenberg's involvement in successfully lobbying Congress for a loophole provision in the Digital Millennium Copyright Act that could protect against a regime of content licensing that requires unduly invasive monitoring; 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); *see also The WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce*, 105th Cong., 12–18 (1998) (statement of Marc Rotenberg, Director, EPIC).

("COPPA").[56] More recently, activists have pushed for an extension of this regulatory framework to adults.[57]

Privacy activists have effectively utilized their media contacts to draw public attention and support for their legislative initiatives. Activists have generally sought to garner the media's attention and then convert the media to its normative positions. In the recent past, the *New York Times* had at least one story per week touching on issues of electronic privacy. Conservative publications such as the *Wall Street Journal* and *The Economist* have also given sympathetic treatment to the activists' views.[58] Because electronic privacy is currently a leading policy concern, the media's hunger for news stories is steadily growing, which makes it increasingly receptive to the story tips and press releases provided by the public interest advocacy groups.

The first generation of privacy norm proselytizers has led a new generation of privacy entrepreneurs and public "opinion leaders" to

---

56. See Junkbusters Urges Vigilance From FTC and Parents to Protect Children From Corporate Surveillance and Manipulation, 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."); Gwen Carleton, *Privacy, For the Sake of the Children, But Positive New Regulation Has Negative Side Effect*, CAPITAL TIMES (Madison, Wis.), June 30, 2000, at 1D ("COPPA . . . went into effect on April 21. The law's enactment marked a triumph for children's advocates, who have agitated since the mid-1990s for basic protections for the Internet's youngest users."); Ted Bridis, *White House Starts Online 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 . . . .").

57. Leslie Miller, *Children's Crusade Advocates Work Behind the Scenes to Fight the 'Powerful Forces' of Marketers Who Target Kids' Privacy In New Media*, USA TODAY, Mar. 10, 1999, at 4D ("'It's a parental notification law, which has some pluses and minuses,' says Marc Rotenberg . . . . '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.'"); Pamela Mendels, *New Serious Side to Child's Play on the Web*, N.Y. TIMES, Nov. 27, 1998, at A20 ("Privacy advocates have raised different concerns about the law. Marc Rotenberg . . . 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.").

58. *See, e.g.*, *The End of Privacy*, THE ECONOMIST, May 1, 1999, at 15; *The Surveillance Society*, THE ECONOMIST, May 1, 1999, at 21 (covering privacy degradation in online environment); Rebecca Quick, *Net Interest: Don't Expect Your Secrets to Get Kept on the Internet*, WALL ST. J., Feb. 6, 1998, at B5; Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 182.

online privacy.[59] William Safire, columnist for the New York Times, recently authored an editorial strongly endorsing the need for online privacy.[60] Safire neither called for a legislative solution nor explicitly promoted a self-regulatory approach. Rather, he argued that Internet privacy is an issue of growing concern to all "lovers of freedom."[61] This example demonstrates a second success of norm proselytizers. Due to their efforts, the call for online privacy is now perceived as so urgent and morally cogent that it transcends ideological factions.

The proselytizers' broader goal is to extend the scope of the concept of privacy to cyberspace.[62] There is no monolithic view as to what the right to data privacy encompasses.[63] On one extreme, the less that personal data is collected and used, the better.[64] This position may have trouble winning widespread support, however, as this appears to go against consumer preferences. Many consumers seem willing to trade away personal data as long as they receive valuable consideration in return.[65]

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 morally problematic to morally

---

59. *See* Ellickson, *supra* note 3, at 16. Especially influential early on were the norms developed by the Organization for Economic Cooperation and Development ("OECD"), which endorsed eight privacy guidelines. Rotenberg has stated that these eight principles for data protection are "still the benchmark for assessing privacy policy and legislation." *Electronic Communication Privacy Policy Disclosure: Hearing Before the Subcomm. on Cts. and Intellectual Prop. of the Comm. on the Judiciary*, 105th Cong., 38 (1999) (statement of Marc Rotenberg, Executive Director, EPIC); Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), *available at* http://www.oecd.org/dsti/ sti/it/secur/.

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

61. *Id*.

62. 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.

63. *See* Robert MacMillan, *Congress to Air Public Concerns Over Privacy*, NEWSBYTES, Sept. 5, 2000, *at* http://www.newsbytes.com (privacy advocates in Congress are split, with some advocating very strong privacy protections).

64. *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1283–88 (2000).

65. *See* Fred O. Williams, *Area Man Wins Cybercash*, BUFFALO NEWS, Oct. 28, 2000, at C1 ("[C]onsumers appear willing to exchange personal data for free prizes and cash . . . ."); John Walsh, *Websites with a Personal Touch*, FIN. TIMES, Mar. 15, 2001, at Mastering Information Management 4 ("Do consumers mind being asked to part with information in order to receive personalized 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.").

acceptable. To accomplish this goal, norm proselytizers espouse a number of concrete norms, most notably notice, consent, access, security, and enforcement.

Least controversial is the notion that data privacy rights include notification of the uses to which websites will put personal data. At least in public discourse, some members of the website industry accept the requirement of notice.[66]

Some notion of consent or agreement is the second most often mentioned requirement of data privacy. There is great disagreement regarding the appropriate definition of consent in the context of website data gathering.[67] In an opt-out regime, personal data will automatically be collected unless a consumer specifically acts to indicate otherwise. Industry groups such as the Online Privacy Alliance have promoted an opt-out policy as a minimum requirement for members.[68] By contrast, 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 regimes.[69]

---

66. *See, e.g., Harold McGraw III Says Internet Has Sparked a Revolution in Multichannel Publishing*, BUSINESS WIRE, Jun. 18, 2001; *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1691 (1999) (noting that much of the policy debate centers focuses on the equivalence of notice and privacy protection).

67. *See* Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 370 (2000) ("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).

68. *See, e.g.*, Online Privacy Alliance, *Guidelines for Online Privacy Policies, at* http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited Oct. 3, 2001). The Alliance is a coalition of more than eighty companies and trade associations formed in early 1998 to encourage self-regulation of data privacy.

69. *See* Amy Borrus, *The Stage Seems Set for Net Privacy Rules this Year*, BUSINESS WEEK, Mar. 5, 2001, at 51 ("[P]rivacy 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.'")

Thomas Cooley defined privacy as the right to be let alone.[70] Respect for consumer privacy online cannot mean that websites should literally leave consumers alone: 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. 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, then, is to gather and use a visitor's personal data in a manner that does not violate her ability to control the flow of such data.

In addition to notice and consent, norm proselytizers have promoted a right of access to one's personal data residing on the databases of websites.[71] In some contexts, the claim is for access and the additional ability to contest or correct inaccurate data.[72]

A fourth element of the general right to data privacy is security for personal data residing in databases of commercial firms.[73] If personal data is easily accessible to hackers or corporate affiliates, the website may be indirectly responsible for injuring the consumer whose data is

---

70. THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888). In the words of William Safire, fair information practices allow each of us "to tell the world to mind its own business." Safire, *supra* note 60.

71. *See* Drew Clark, *Activists Unite To Push For Stronger Privacy Laws*, NAT'L J. TECH. DAILY, Jan. 30, 2001 ("For the privacy advocates, the proliferation of privacy-invading technolog[y] 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.").

72. In the context of telecommunications, seventy-nine percent of American consumers rate as "absolutely essential" that customers should be afforded the opportunity of seeing their telephone transaction records so that their accuracy can be checked and any mistakes can be corrected. Alan F. Westin, *The Era of Consensual Marketing is Coming*, *at* http://www.pandab.org/1298essay.html (last visited Oct. 12, 2001).

73. *See* Stewart Baker, *Regulating Technology for Law Enforcement*, 4 TEX. REV. L. & POL'Y. 53, 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.").

stored with the website, even if the website is not guilty of any active wrongdoing.

Finally, the effectiveness of the foregoing privacy protections is dependent on the implementation of an enforcement principle, which requires sanctions for noncompliance with fair information practices.[74]

These five elements of the general right to data privacy are accurately grouped under the second-order norm that people have a right of reasonable control over their personal data.[75] Note that this norm does not entail a consumer right to ownership of individual personal data.[76] If consumers owned their personal data, they presumably could sell it. Once alienated, the consumer would have no more claim to it than a piece of sold real property. The rights discussed above may be best treated as inalienable.[77]

Consumers increasingly feel entitled to the respectful treatment of their personal data.[78] Websites increasingly recognize this sense of entitlement. One Internet entrepreneur summarized the situation in this manner: "Companies used to think of customer data as theirs. They're starting to realize they're really custodians, and the customer controls the information."[79]

---

74. 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. *See* Commission Directive 94/46/EC, 1994 O.J. (L 268) 15–21. 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.

75. The website industry views the norms proposed by the privacy proselytizers as "overkill." *See* 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. *See id.*

76. Some commentators have advocated 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, e.g.*, Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63 (1999). Such a right would be in tension with the First Amendment, however.

77. *See, e.g.*, Samuelson, *supra* note 1, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights.").

78. *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 U.S. Business Week/Harris Poll found that ninety-two percent of Internet users were uncomfortable about websites sharing personal information with other sites. *It's Time for Rules in Wonderland*, BUSINESS WEEK, Mar. 20, 2000, at 82.

79. Paul Davidson, *Marketing Gurus Clash on Internet Privacy Rules*, USA TODAY,

An important strategic implication follows from the activities of privacy activists in creating a sense of consumer entitlement to personal data. 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.

2. Norm Entrepreneurs Support Respectful Norms

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. Other norm entrepreneurs increasingly find it is in their interest to promote privacy norms. This has most conspicuously been true for the FTC and a number of firms that market privacy-related software.

Since the mid 1990s, the FTC has acted to reinforce the privacy-promoting efforts of the privacy proselytizers. Elsewhere, I have argued that public choice theory provides a plausible explanation for the agency's involvement: the FTC has sought to become the leading federal agency regulating online activities as a means of extending its regulatory grasp to the Internet.[80] 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.

The FTC acts pursuant to its authority under the Federal Trade Commission Act, which mandates that the agency address "unfair" and "deceptive" trade practices.[81] The FTC casts website data-gathering

---

Apr. 27, 2001, at 2B (quoting Hans Peter Brondmo).

80. Hetcher, *FTC as Internet Privacy Norm Entrepreneur*, *supra* note 3, at 2053. As an indirect result of privacy advocacy, Congress asked the FTC to examine online privacy issues. 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 Statements of the Fed. Trade Comm'n on "Internet Privacy" Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary* (March 26, 1998), *at* http://www.ftc.gov/os/1998/9803/privacy.htm; Brian Kreebs, *IT Industry Council Signals Privacy-Law Advocacy*, NEWSBYTES, Feb. 2, 2001 (reporting that, due to public outcry, lawmakers are suggesting federal electronic privacy protections); Rosalind C. Tritt, *Privacy: A Threat to Free Speech?*, PRESSTIME, Jan. 2001, at 27; *PrivacyRight, Inc. Forms Strategic Equity Partnership with Venture Factory*, PR NEWSWIRE, June 6, 2000.

81. 15 U.S.C. § 45(a)(1) (1994). The FTC prosecutes "[u]nfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the Federal Trade Commission Act ("FTCA"). *See id.* Section 13(b) authorizes the prosecution of actions to enforce Section 5. *See id*. § 57(b). Section 18 permits the FTC to create rules to prohibit deceptive or unfair practice prevalent in certain industries. *See id*. § 45(a)(2).

practices as potentially unfair and deceptive.[82] In particular, the agency has borrowed the various specific privacy protection measures supported by the privacy activists — notice, consent, access, security, enforcement — and has shrouded them in the rhetoric of fairness.[83]

The FTC contends that these fair information practices are best promoted through website privacy policies. A privacy policy that accurately and completely states the website's personal data practices is in accordance with the principle of notice: 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 to the user's personal data on file with the website can be set out in the privacy policy, as can stipulations concerning security and enforcement.

When websites take up the FTC's suggestion and seek to implement the fair information practices 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 are directly within the FTC's jurisdiction.

Software vendors, marketing so-called "privacy solutions," have recently emerged as a new type of privacy norm entrepreneur.[84] Privacy solutions are software that users or websites can install in order to create a more privacy-respecting online environment. While websites are typically the direct purchasers of these products, the software developers also advertise their products to consumers. The more the advertisements are successful in fostering moral concern among consumers, the greater

---

82. 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.

83. *1998 FTC Report to Congress*, *supra* note 29, at 7. The FTC explicitly states that it takes its normative framework from the governmental privacy policy community. *See id.* at 48 n.27.

84. *See* 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."); *P3P: Just a Start*, ZDWIRE, July 17, 2000, *available at* 2000 WL 18178259 ("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.").

the social pressure toward increased privacy protection that will be exerted on the website industry.

Consider the representative advertisement by the firm, Zero-Knowledge.[85] 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." 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."

As portrayed, the firm equates her with her data, in contravention of the Kantian maxim that actors should not treat persons merely as a means to their own ends. 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 to the website industry: "I am an individual and you will respect my privacy." This brief statement contains three normatively laden words: "individual," "respect," and "privacy." The final claim is that "On the Net, I am in control." This statement is 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 rights when it comes to online privacy, she admonishes the reader to do the same.

Advertisements of this sort will likely influence privacy norms by further stoking consumer privacy concerns and the corresponding entitlement to personal data. Public opinion likely will be galvanized in the direction of greater demand 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

---

85. Zero-Knowledge advertisement, *in* WIRED, Aug. 2000, at 5–6. Zero-Knowledge Systems lets Internet users surf the net anonymously. Zero-Knowledge Systems's Freedom software uses encryption and several different computers to mask its users' identities, even from itself. The Zero-Knowledge website can be found at http://www.zeroknowledge.com.

powerful shapers of public norms regarding online privacy due to their ability to directly reach millions through their print media campaigns.

III. MEETING THE DEMAND FOR ONLINE PRIVACY

In the previous part it was seen that due to the efforts of norm proselytizers and norm entrepreneurs, the demand for privacy among consumers has surged. This Part will examine the impact of this increase in demand on the level of supply. Generally, when demand for a good or service goes up, the supply will go up as well. Thus, barring special circumstances, one would expect that the increase in demand for personal data privacy online would produce an increase in supply.

All things being equal, websites that could cheaply supply privacy would be more inclined to do so, while websites for which it was more expensive would tend to provide less privacy. Some relevant factors here are the extent to which the use of personal data plays a central role in the business model of a particular website and the site's relative cost structure for collecting, storing, processing, and manipulating data.[86] In addition, websites whose customers are more demanding of privacy will be more likely to provide greater privacy protections.[87]

Despite the increase in demand for respect for online privacy, there is great controversy as to whether there has been an increase in the supply of privacy respect. The industry claims to be responsive to user demand for a heightened level of respect. Many privacy advocates, however, strongly disagree. As noted in the Introduction, Jessica

---

86. For example, despite its high profile, Amazon recently announced that it was changing its privacy policy in a manner that was less favorable to consumer privacy interests. *See Amazon Draws Fire for DVD Pricing Test*, WALL ST. J., Sept. 14, 2000. Presumably Amazon calculated that despite the possible negative impact on its reputation as a respecter of privacy, it was worth it to make the change of practice due to the important role that consumer data plays in its business model. Ebay also recently changed its policy in a consumer-unfriendly fashion. *Ebay Says It May Sell Information on Users in Event of Acquisition*, WALL ST. J., Apr. 3, 2001, at B1. One commentator remarked that what hope could there be for online privacy if even a prosperous site such as Ebay would make such a move. This comment fails to appreciate the fact, however, that Ebay is in an unusual position because of its business model, Ebay has unusually rich access to valuable data on consumer preferences and buying activities. For it to provide respect would involve an unusually large sacrifice, one that Ebay apparently does not think it is justified by the prospect of increased consumer trust.

87. For example, health-related sites and financial sites provide higher levels of privacy, which is apparently responsive to consumer demand. *See* Stephanie Olsen and Patrick Ross, *Studies Out to Debunk Privacy Legislation*, CNET News.com, May 8, 2001 *at* http://news.cnet.com/news/0-1005-200-5865212.html?tag=tp_pr (reporting that Rep. Michael Doyle, D-Penn, "said consumers seemed more concerned with financial and medical privacy than with other types . . . .").

Litman has stated that industry attempts at self-regulation have been an "abject failure."[88] Similarly, Jason Catlett of Junkbusters, a privacy advocacy firm, has remarked that, "The stated policies of most big shopping sites run the gamut from bad to atrocious."[89]

Not all commentators sympathetic to consumer privacy concerns are this critical, however. In the same symposium in which Litman made her remarks, Pamela Samuelson noted that privacy policies are getting better.[90] Are Litman and Samuelson really disagreeing, and if so, who is right? Or are both wrong and the industry right in its more upbeat assessment? This Part and Part IV will seek to come to a better understanding of these central questions in the online privacy debate. The first section below will examine the data-regarding norms that have been adopted by websites in their privacy policies. The second section will discuss the recent emergence of the Chief Privacy Officer. These efforts constitute the main response of the website industry thus far to the chorus call for online privacy. Finally, the third section will critically evaluate these efforts by websites in order to better judge the merit of the critics' charges of duplicity. Following this discussion, Part IV will examine signaling theory in order to see whether it may lend insight into website behavior.

A. The Features and Content of Current Website Privacy Policies

Website privacy policies are a recent phenomenon, having come into existence in the late 1990s. The universal feature of website privacy policies is that they are accessible as a link from the home page of many websites. Many sites also have links to the privacy policy from areas within the site, such as from internal pages that request customer data. Privacy policies range from a half-page to ten pages in length. In terms of their apparent intent and rhetorical structure, privacy policies are hybrid documents that reflect both public relations and legal concerns. On the one hand, privacy policies often have a chatty and disarming tone that clearly seems motivated by an attempt to create an air of closeness and intimacy between the site and its users. On the other hand, privacy policies are becoming more legalistic in tone.

---

88. Litman, *supra* note 2.

89. Stephanie Olsen, *Top Web Sites Compromise Consumer Privacy*, CNET News.com, Dec. 17, 1999, *at* http://news.cnet.com/news/0-1007-200-1500309.html.

90. Samuelson, *supra* note 1, at 1161 ("[T]here is some evidence that American-based commercial based Web sites provide more notice about privacy policies now than they did a year ago. Some progress also continues in implementation of the other principles . . . .").

Privacy policies typically begin with some warm and fuzzy language about the online entity's respect for its users' privacy. Typical in this regard are statements such as, "At 1-800-flowers.com, we recognize and respect the importance of maintaining the privacy of our customers and members."[91] Some of the more scrupulous sites explicitly acknowledge the privacy rights of users in their opening remarks. Wal-Mart's privacy policy states, "We believe that you have a right to know, before shopping at Walmart.com or at any other time, exactly what information we might collect from you, why we collect it and how we use it."[92] Nike's privacy policy begins, "Nike is committed to respecting the privacy rights of all visitors to our web site."[93]

In the opening statements of their privacy policies, some sites are explicit in stating that their goal is to create a relationship of confidence and trust with consumers. The Walt Disney privacy policy begins, "The Walt Disney Internet Group is committed to helping you make the most of your free time on the Internet within a trusted environment . . . . We hope that this disclosure will help increase your confidence in our sites and enhance your experience on the Internet."[94] The introduction to the Wal-Mart privacy policy states that, "The security of your personal information is very important to us. . . . We value your trust very highly, and will work to protect the security and privacy of any personal information you provide to us and will only use it as we have described in our Privacy Policy."[95] Sears.com states, "We value the trust you place in Sears, Roebuck and Co . . . . We want to ensure that you understand what information we gather about you, how we use it, and the safeguards we have in place in order to protect it."[96]

Some sites make it apparent that they judge the moral relationship between website and consumer to be a two-way street. The first paragraph of the MadonnaFanClub.com privacy policy states that the

---

91. 1-800-flowers.com Privacy statement, *at* http://www.1800flowers.com/flowers/security/index.asp (last visited Oct. 11, 2001).

92. Walmart.com Security & Privacy, *at* http://www.walmart.com/cservice/ca_securityprivacy.gsp (last visited Oct. 11, 2001). Wal-Mart has an exemplary privacy policy. Sites of old economy firms like Wal-Mart are of particular interest, as they demonstrate the penetration of the growing ethos of Internet privacy beyond the now outdated notion of the dot.com economy. The Internet was never a marketplace but rather a technology platform.

93. Niketown.com Privacy Policy, *at* http://niketown.nike.com/info/privacy.jhtml (last visited Oct. 11, 2001).

94. Disney.com Privacy Policy, *at* http://disney.go.com/legal/privacy_policy.html (last visited Oct. 11, 2001).

95. Walmart.com Security and Privacy, *supra* note 92.

96. Sears, Roebuck and Co. World Wide Web Site Customer Information and Privacy Policy, *at* http://www.sears.com (last visited Oct. 11, 2000).

site "always respects the privacy of Fan Club members and visitors to our website."[97] The last paragraph of the short document states that, "All information contained on this site is copyrighted. Your cooperation in respecting these copyrights is appreciated."[98] Here, a core normative principle is at play. Because the site holds itself out as respectful, it is appropriate — by the lights of the ordinary moral principle of reciprocity — to ask for respect in return. Privacy policies that are more legalistic in tone would be unlikely to make the same request for reciprocal treatment.

On the whole, however, privacy policies are increasingly employing more overtly legalistic formulations.[99] For example, Weather.com states, "This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights."[100] Toyota's privacy policy in part reads, "Toyota does not assume any responsibility for the accuracy, completeness or authenticity of any information contained on this site. This site and all information and materials contained herein, is provided to you "as is" without warranty of any kind."[101] Toyota further states, "Toyota shall not be responsible for any harm that you or any person may suffer as a result of a breach of confidentiality in respect to your use of this site or any information you transmitted to this site."[102] Toyota's harsh legalistic tone illustrates the tension between a privacy policy crafted as a document meant to create trust in users and a legal document meant to protect the company against potential liability. The use of more legalistic language is perhaps not surprising, given that privacy policies are starting to play a role in lawsuits.[103] If privacy-related lawsuits become more prevalent, privacy policies may become even more legalistic.[104]

---

97. Madonna Fan Club Privacy Statement, *at* http://www.madonnafanclub.com/privacy.html (last visited Oct. 11, 2000).

98. *Id.*

99. *See* Eric Roston, *How to Opt Out of Database Sharing; Who's Got Your Number?* TIME, July 2, 2001, at 46.

100. Weather.com Privacy Statement, *at* http://www.weather.com/common/home/privacy.html (last updated July 3, 2001).

101. Toyota Privacy Policy, *at* http://www.toyota.com/html/privacy/index.html (last visited Oct. 11, 2000).

102. *Id.*

103. *See* Judnick v. DoubleClick, No. CU-421 (Main Cty. Sup. Ct., filed Jan. 27, 2000).

104. Currently, the legal status of privacy policies is ambiguous. *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, J. INTERNET L., Oct. 1999, at 12. (arguing that terms in privacy policies should be treated as contractual). *But see, e.g.*, *Weather.com Privacy Statement*, *supra* note 100 ("This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights.").

In the past few years, most websites have begun to address privacy concerns to one extent or another.[105] There are a number of common practices that websites are beginning to adopt. To some extent, these practices track the fair information practice principles that are being promoted by the privacy entrepreneurs. The FTC has noted that it is not possible to specify in detail how the privacy principles should be implemented, as the meaning of the principles will vary depending on the particular activities of the site in question.[106] Indeed, the following brief survey of the terms of a number of website privacy policies will indicate just how complex and varied the personal data practices of websites are becoming. It will be necessary to examine these practices in some detail so that it will be possible in a later section to better understand the extent to which these practices are susceptible to, or indeed constituted of, either false signaling actions or acts of mimicry.[107]

1. Notice/Awareness

The provision of notice of a site's personal-data-related activities is the first of the fair practice principles. The principle of notice is a second-order principle that supports each of the other principles. It is only when a user has knowledge of the data-related activities of a website that the user can make informed decisions about how to interact with the site regarding each of the other privacy principles. At first glance, notice might seem like a straightforward requirement with which to comply. A site simply writes down a description of its data-related practices and creates a link to this text. For some sites with simple and minimal data-related practices, the provision of straightforward notice is possible. For example, the "Official Madonna Fan Club" site's privacy policy, when printed out, is only half a page long and contains

---

105. *See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Federal Trade Commission Report to Congress* 10 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (discussing the Commission's survey findings, which demonstrate continued improvement with eighty-eight percent of websites in the random sample posting at least one privacy disclosure).

106. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), *available at* http://www.ftc.gov/reports/privacy3/toc.htm.

107. Previous studies of privacy policies have provided quantitative measures of changing website practices. *See* Federal Trade Commission, *Fair Information Practices in the Electronic Marketplace*, *supra* note 105; *see also* The Georgetown Internet Privacy Policy Survey, *available at* http://msb.edu/faculty/culnanm/gippshome.html (last updated Aug. 2000). While of general interest, these studies do not lend insight as to whether these changes represent true or feigned respect for privacy.

three short paragraphs.[108] The site is able to state in a straightforward manner, "We do not sell, rent or trade your personal information with others."[109] This site uses personal data in order to process commercial transactions, such as merchandise sales and membership dues. The site claims not to use cookies or other passive means of data gathering.[110]

Notice becomes difficult to provide, however, when a site has complex data-related practices. The first layer of complexity is introduced by means of the manner in which data is collected. Users of course understand that data is being collected from them when this data is explicitly provided by them. More opaque is data collection by means of cookies and other means of so-called passive tracking of user online activities. Many sites provide definitions of arcane terms such as "cookies" and "IPO addresses," and offer explanations of their importance for privacy purposes.[111]

For many sites, how the personal data is gathered is the determining factor in whether the data becomes "personally identifiable information" or "personal information," as compared to "anonymous information." The information that people explicitly volunteer to the website such as name, address, social security number, age, etc. is personally identifiable in the sense that it can be traced back to particular individuals. By contrast, websites collect information through the use of cookies on such activities as the users' visitation to various sites. Sites typically state that this information is not personally identifiable.[112] In other words, though the sites keep records of cookie-generated information, they

---

108. Madonna Fan Club Privacy Statement, *supra* note 97.

109. *Id.*

110. *Id.*

111. *See, e.g.*, Motorola Privacy Practices, *at* http://www.motorola.com/content/0,1037,3,00.html (last visited Oct. 11, 2001) ("When you come into our site, our server attaches a small text file to your hard drive — a cookie. Your unique cookie tells us that it is you whenever you re-enter our site, so we can recall where you've previously been on our site, and what if anything, you have in your shopping cart."); Hallmark.com Privacy Policy, *available at* http://www.hallmark.com (last visited Oct. 11, 2001) ("An IP [Internet Protocol] address is a number that is assigned to your computer when you are using your browser on the Internet. The servers that serve our web site automatically identify your computer by its IP address. We do log IP addresses, but the addresses are not linked to individual customer accounts nor are they used in any other way to personally identify our customers.").

112. The Kinkos.com privacy policy states, "Also, Kinkos uses a reputable third party to collect and accumulate other anonymous data that helps us understand and analyze the Internet experience of our visitors. . . . This information may be stored in a cookie on your computer's hard drive. However, none of this information is personally identifiable and we only share this information in the aggregate, reflecting overall web site or Internet usage trends." Kinko's Security and Privacy Policy, *at* http://www.kinkos.com/privacy.html (last visited Oct. 11, 2001).

claim not to keep track of which personally identifiable person is attached to this information.

Perhaps the most significant challenge to adequate notice arises regarding the relationships that sites have with third parties. Privacy advocates and consumers are especially concerned about the fact that personal data may be transferred to these third parties.[113] Privacy policies refer to these entities as, "trustworthy third parties,"[114] "reputable third-parties,"[115] etc. The main challenge to giving effective notice is the complexity and diversity of the relationships that sites have with these third parties. The difficult issue is determining how much description is necessary in order to provide adequate notice. Some sites are moving in the direction of providing fuller descriptions of their relationships with third parties. This means, however, that their privacy policies are becoming increasingly long and complex.

2. Choice/Consent

The second of the fair information practice principles is choice/consent. The intuitive idea is that users should have some say when it comes to the use of their personal information by websites. The FTC has interpreted the norm of choice so as to include making a choice among a number of alternatives.[116] Some sites, however, treat choice in the narrowest sense so as to mean simple consent or assent. Toyota writes, "By using this site, you signify your assent to the Toyota Online Privacy Policy. If you do not agree to this policy, please do not use this site."[117] Under the heading of, "Your Consent" on its site, Nike simply states, "By using our web site, you consent to our privacy policy."[118]

Many sites, however, do offer users choices other than the option of leaving. The most common choice made available to users is whether they want to have their personal data stored with, and used, by, the site. Many sites give the user the option of removing their personal data from the site. For example, Kinkos.com states, "You can easily change any

---

113. *See* Jason Gonzalez, *Better Business Bureau Gives Nod to Lowe's*, NATIONAL HOME CENTER NEWS, May 1, 2001, at 7 ("The posted policy must also include product information, data access, site security and third party transfer information — perhaps the primary concern among consumers and privacy advocates.").

114. Barnes & Noble.com Privacy Policy, *at* http://barnesandnoble.com/help/nc_privacy_policy.asp (last revised May 3, 2001).

115. Nokia.com Privacy Policy, *at* http://www.nokia.com/privacy.html (last visited Oct. 11, 2001).

116. *See 1998 FTC Report to Congress*, *supra* note 29, at 17.

117. Toyota Privacy Policy, *supra* note 101.

118. Niketown.com Privacy Policy, *supra* note 93.

of the information you have been asked to provide by Kinko's. You can also permanently remove your information from the Kinko's database."[119]

As already mentioned, websites offer two types of consent, which are widely referred to as opt-in and opt-out.[120] With opt-out, the user must take some positive step in order to stop what would otherwise be a default process whereby her data would be available for use by the website.[121] Typically, the user cannot simply opt-out without consequence. Sites often condition access to the site or to some portion of the site on the provision of data by consumers. Thus, opting out of the provision of data entails opting out of receiving some or all of the site's services.[122] Other sites, however, simply allow consumers to opt out of at least some of the site's collection practices without adversely affecting the consumers' abilities to benefit from the site.[123]

Until recently, it has been very uncommon for websites to provide opt-in as a choice to users. A small but growing number of sites are now offering users the choice to opt-in to some or all of the site's data practices. With opt-in, personal data will not be collected or used unless the user provides her explicit permission. In particular, sites that deal with more sensitive data are beginning to offer opt-in for this data.[124]

3. Access/Participation

The third FIPP prescribes that websites provide users with access to their personal data stored with the website. This principle is often discussed in conjunction with the principle of allowing consumers to contest data stored at the site that they deem to be incorrect. It is getting increasingly common for sites to allow users to access their data. For example, microsoft.com states, "If you ever want to review or update your profile, simply visit the Profile Center and edit your personal information. We'll ask you to disclose your Microsoft Passport (e-mail

---

119. Kinko's Security and Privacy Policy, *supra* note 112.

120. *See supra* text accompanying note 67.

121. *See supra* text accompanying note 69.

122. *See* Motorola Privacy Practices, *supra* note 111 ("You also have choices with respect to cookies. By modifying your browser preferences, you have the choice to accept all cookies, to be notified when a cookie is set, or to reject all cookies. If you choose to reject all cookies you will be unable to use those services or engage in activities that require registration in order to participate.").

123. *See* jcrew.com (permitting customers to refuse cookies and decline to receive promotional emails and catalogs without limiting the customer's shopping experience).

124. Paul Davidson, *Capitol Hill Support Brews for Internet Privacy Laws*, USA TODAY, July 12, 2001, at 3B (noting that there is consensus building for requiring opt-in for more sensitive data, such as financial and medical).

address and password) so that only you can access your profile."[125] Despite opportunities for access, fewer sites offer the ability to contest data. One that does is nokia.com, which states, "Nokia will on its own initiative, or at your request, replenish, rectify or erase any incomplete, inaccurate or outdated personal data."[126]

4. Integrity/Security

A solid minority of sites now address the issue of security in their privacy policies. Under the heading of "Security" in its privacy policy, Sun Microsystems unhelpfully states merely that, "We intend to take reasonable and appropriate steps to protect the Personal Information that you share with us from unauthorized access or disclosure."[127] Many sites employ Secure Socket Layer ("SSL") technology to protect the security of credit card information as it is transmitted to the site.[128] With SSL, the website's server scrambles the data as it travels from the user's computer to the website. It is much less common, however, for sites to make remarks in their privacy policies regarding the security of the user's data as it resides on the site's server. This latter form of security is more important than protecting the data while in transit, as most significant breaches of website security have involved hackers gaining access to databases in storage on a firm's website.[129] Increasingly, websites are addressing the issue of the security of data stored by the site. Some sites are limiting the number of employees with access to

---

125. *See* Microsoft.com Statement of Privacy, *at* http://www.microsoft.com/info/privacy.htm (last updated Feb. 23, 2001).

126. Nokia.com Privacy Policy, *supra* note 115.

127. Sun Online Privacy Policy, *at* http://www.sun.com/privacy (last visited Oct. 3, 2001); *see also* Toyota Privacy Policy, *supra* note 101 ("This information, such as name, mailing address, e-mail address, type of request and possibly additional information, is collected and stored in a manner appropriate to the nature of the data by Toyota and is used to fulfill your request.").

128. *See* Motorola Privacy Practices, *supra* note 111 ("Motorola users Secure Sockets Layer (SSL) encryption technology, the highest level of security on the Internet. The SSL protocol provides server authentication, data integrity, and privacy on the Web. This security measure helps insure that no imposters, eavesdroppers, or vandals get your personal information. SSL not only encrypts your personal and financial information transmitted, including credit card information, but also verifies the identity of the server and that the original message arrives safely at its destination.").

129. Recently, a Russian hacker, Maxus, succeeded in stealing the credit card information of a large number of consumers whose data was stored on a site. Maxus attempted to extract $100,000 from the site. When they refused to pay, he posted the information for public display on the Internet. *See* Jeffrey Kluger, *Extortion on the Internet; A daring hacker tries to blackmail an e-tailer — and sparks new worries about credit-card cybertheft*, TIME, Jan. 24, 2000, at 56.

personally identifiable data as well as employing security systems to protect the data from external intruders.[130]

5. Enforcement/Redress

The fifth FIPP is that of enforcement/redress. According to this principle, the user should be provided with some means of enforcing the above principles or of receiving redress in cases of injury due to a failure to provide protective practices that instantiate the FIPPs. Websites have done very little to promote this norm.[131]

6. Stopping Data Transfers to Third Parties

It is important to note that the fair information practice principles do not prohibit data transfers by websites to third parties. The first two principles, notice/awareness and choice/consent, are essentially an informed consent requirement. They do not prescribe a particular substantive set of privacy protections but rather stipulate that whatever data-related practices a website engages in, the site should receive the informed consent of its users as to these practices (with failure to opt-out counting as a form of consent). The latter three fair information practices provide more substantive requirements of access, security and enforcement. None of these five principles, however, prohibits data transfers to third parties. Nevertheless, a small number of sites do promise that they will not sell or trade data to third parties. For example, Wal-Mart states that, "We never sell or rent your personal information to any third parties under any circumstances."[132]

---

130. For example, MTV's website, MTV.com, states, "We have taken steps to ensure that personally identifiable information collected is secure, including limiting the number of people who have physical access to its database servers, as well as electronic security systems and password protections which guard against unauthorized access." MTV.com Terms of Use & Privacy Policy, *at* http://www.mtv.com/sitewide/mtvinfo/terms.jhtml#privacy (last updated Aug. 9, 2001); *see also* Barnes & Noble.com Privacy Policy, *supra* note 114 ("To insure that your information is even more secure, once we receive your credit card information, we store it on a server that isn't accessible from the Internet."); Microsoft.com Statement of Privacy, *supra* note 125 ("[D]ata is stored in password-controlled servers with limited access.").

131. For a token effort, see barnesandnoble.com ("We're so certain that our online ordering systems are secure that we back it up with a guarantee. In the unlikely event that you are subject to fraudulent charges….we will cover the entire liability for you, up to $50, as long as the unauthorized use of your credit card resulted through no fault of your own from purchases made from Barnes & Noble.com while using our secure server.").

132. *See* Walmart.com Security and Privacy, *supra* note 92.

For sites with complex data activities — even sites with no intention to sell or trade data to third parties — it will be difficult to promise to make no data transfers whatsoever. The reason is that simple corporate efficiency may require outsourcing various data-related activities necessary to a firm's own internal usage of the data. Some firms are making a serious effort to protect the integrity of user data despite these third party transfers. Wal-Mart, for example, promises to only transfer data for specific purposes and then under contract.[133] This achieves a similar function to a complete prohibition on data transfers. Hallmark.com treats information in the site's Address book as highly confidential and states that the information will not be disclosed to third parties.[134]

B. Chief Privacy Officers

The Chief Privacy Officer ("CPO") is a new and rapidly growing position in corporate America. Estimates vary, but there are now CPOs at a growing number of firms, particularly larger firms.[135] There is a newly created organization of CPOs and a non-profit organization run by the dean of privacy advocates, Alan Westin, to train CPOs.[136] The emergence of the CPO is a practical solution to a growing problem; as technology develops, even firms that have the desire to provide privacy are finding it increasingly difficult to do so, due to the growing complexity of the task. [137]

---

133. *See id.* ("Coremetrics is contractually prohibited from using, in any manner, information obtained in the course of providing these services to Walmart.com, other than to help us provide you the best possible shopping experience on our site."); *see also* Hallmark.com, *supra* note 111 ("If you sign up to become a Hallmark.com affiliate partner, you will be directed to a third party web site who manages the affiliate process, and this third party is not allowed to use the information they collect for any other purpose.") It is not indicated, however, what leverage Hallmark would have over these unnamed third parties.

134. Hallmark.com, *supra* note 111 ("Address book information is considered highly confidential and will not be used for promotional purposes by Hallmark or disclosed to third parties.").

135. *Privacy of Customer Information: Hearing Before the Subcommittee on Commerce, Trade and Consumer Protection of the House Energy and Commerce Committee* (July 26, 2001) (statement of Harriet P. Pearson, Chief Privacy Officer, IBM Corporation).

136. Tom Kirchofer, *Net Creates 'Chief Privacy Officer,'"* BOSTON HERALD, July 17, 2000, at D21. One might think it a puzzle that the FTC has not promoted CPOs. But this would be predicted by the public choice account of the FTC. The FIPPs promote the growth of the FTC's jurisdiction. CPOs do not.

137. Perhaps the best way for a website to make consumers think it respects their privacy is really to respect their privacy. This might involve having CPOs who really

So far, most CPOs have legal backgrounds. In addition to understanding the law of privacy, however, CPOs must be able to interface with their firm's software engineers and architects in order to create technical solutions to the demands of privacy.[138] Unless someone at a firm is in a position to understand basic privacy concepts and also have knowledge of new developments at a company, there will always be the prospect that a new activity involves gathering or using data in a potentially problematic manner.

C. Spies in the House of Online Privacy

In the last two sections, we saw that websites have been active to one degree or another in the past few years in implementing various sorts of privacy-regarding practices. These activities have come about in response to the increased demands of consumers and various privacy advocates. Although these practices are privacy-regarding, it is very controversial whether they are privacy respecting or enhancing. The practices have been subject to harsh criticism from privacy advocates, who have in general claimed that the level of protection provided by websites is far too low to provide adequate respect for consumer data privacy rights.

It is perhaps to be expected that privacy advocates would be hard to satisfy in this regard. But in addition to expressing dissatisfaction with the general level of protection, privacy advocates have sharply attacked websites for acting in a duplicitous fashion by seeking to create a false impression in consumers. Nearly all the criticism has been leveled against the main form of protection to be offered so far, the privacy policy. The general drift of criticism leveled by commentators is that privacy policies are vague, unintelligible, and incomplete.[139] Readers

---

believe in privacy as a moral value. Moral perception and moral reasoning can be complex and subtle activities. Institutional response to moral complexity has best made its presence felt in the professional context in the form of professional ethicists working with Institutional Review Boards ("IRBs") in hospitals and medical research facilities. One can view the creation of the CPO as a step in a similar direction. As technology develops, the challenges for privacy promise to develop in lock-step. It is likely that it will become more complex to determine what privacy requires in particular concrete circumstances.

138. *See* Kirchofer, *supra* note 136 ("CPOs also need to be up to the technical challenge of making sure their companies' computer systems let customers look at their personal data.").

139. *See, e.g.*, Patrick Thibodeau, *FTC Official Faults Corporate Privacy Policies*, COMPUTERWORLD, May 7, 2001, ("Many corporate privacy policies are too hard to find, too long and too confusing . . . .") (paraphrasing U.S. Federal Trade Commissioner Sheila Anthony).

are naturally led to believe they are getting greater protection than they in fact are. In terms of the potential cooperative bargain between users and websites whereby trust is exchanged for respect, this criticism can be recast in terms of seeing websites as trying to get something for nothing. They are seeking to obtain trust by exchanging not privacy protection but the illusion of privacy protection.

This criticism of the emerging website privacy norms is typically painted with a broad brush, dismissing in its entirety the effort by websites to provide respect for privacy. If these critics are right in the categorical dismissal of the efforts of websites, a puzzle arises when this dismissal is considered in light of the findings of Part One. The puzzle is to explain why no supply of privacy has been forthcoming, given the increase in demand. As noted earlier, unless there are special circumstances, an increase in demand should bring about an increase in supply. If the critics are right, this has not occurred. What then are the special circumstances that occasion this outcome?

In spite of the widespread rejection of privacy policy protections by privacy advocates, or perhaps because of it, there has been little detailed examination of the particular norms that have been promoted in privacy policies in order to better evaluate whether the categorical rejection is accurate. Accordingly, further progress in understanding this important issue will necessitate closer examination from a critical perspective of the industry norms that have emerged thus far. Following is a discussion of the various aspects of privacy policies that highlights their most troubling features.

As noted earlier, the one principle that is most often addressed by websites is *notice*, so discussion may usefully begin here. All privacy policies, to one degree or another, describe the website's data practices. The question is when do such descriptions constitute adequate notice. The better websites make statements telling the user that the notice provided by the website is exhaustive of the uses to which the consumer's data will be put. The Walmart.com policy states, "We value your trust very highly, and pledge to you, our customer, that we will work to protect the security and privacy of any personal information you provide to us and that your personal information will only be used as set forth in this Policy."[140] On the other hand, more lax websites merely

---

140. Walmart.com Security & Privacy, *supra* note 92; *see also* Intel.com, *Intel Privacy Policy*, *at* http://intel.com/sites/corporate/privacy.htm (last visited Oct. 2, 2001) ("Intel is committed to user privacy in our products and services. This policy outlines our personal information handling practices. If you give us personal information, we will treat it according to this policy."); *Microsoft.com Statement of Privacy*, *supra* note 125 ("For material changes to this statement, Microsoft.com will notify you by placing prominent notice on the Web site.").

note, at most, that they will make an effort to inform users of the sites' collection and usage practices. For instance, MTVi.com says it makes, "good faith efforts to make it clear why the information is being collected and what it will be used for . . . ."[141] In the event of litigation against MTV, the firm will always be able to assert that it made a good faith effort, under the circumstances. Wal-Mart's promise is more concrete; it either is or is not the case that the user's data was used by the website in a manner not set forth in the policy.

Even for websites such as Walmart.com, which appear genuinely interested in providing fair notice, this requirement is not without difficulties. There will inevitably be some deficit in reader comprehension simply because privacy policies may present a host of new terminology and a set of descriptions of varying and complex practices. This is a familiar problem with consumer contracts, leases, disclaimers, etc. With privacy policies, however, the failure to comprehend may be more due to unfamiliar terminology and processes than to complex legal constructions, although, as noted above, privacy policies are becoming more legalistic as well.

There is no simple solution to this difficulty, which is inherent in giving notice to ordinary people of complex activities with significant legal implications. Even websites making their best effort will need to make difficult judgement calls regarding the proper level of information to provide. If the notice is too detailed, the reader may become lost or distracted, and if the notice is too pithy, the reader may not receive adequate information.[142]

Many websites appear not to make a best effort, however, or anything close to it. For example, many websites state that they reserve the right to change their data practices without prior notice. These websites typically instruct users that they should periodically consult the site's privacy policy in order to stay apprised of the site's current data policies. The obvious problem with this suggestion is that in the time between the time the user checks the policy and the time of the policy change, she will be misinformed as to the website's practices. In addition, this practice creates an incentive for websites to promise respectful treatment to users in order to lure them in, only to then change practices in midstream.[143] The deepest fear of consumers arises

---

141. *See* MTV.com Terms of Use & Privacy Policy, *supra* note 130.

142. Citibank is dealing with this problem by offering two versions of its privacy policy, the technical one and the short form. *See* Thibodeau, *supra* note 139.

143. Many sites note that they collect personal information using cookies but that this information is not connected up to personally identifiable information. For example, Kinkos.com states that, "Kinko's does not link your IP address with any information that could personally identify you." But Kinko's also states that, "Kinko's reserves the right,

regarding the use of their data by unknown third parties using their data in unknown ways.[144] People expect that their data will be used only for the purpose for which it was collected. By the lights of ordinary moral logic, this would imply that websites have a duty to adequately inform users of external uses of their data. It is thus here that websites have their greatest opportunity to either display respect, or not. It is here that websites have perhaps been most guilty of providing inadequate notice. Websites commonly note that they will deal with third parties in order to promote the interests of the users.[145] This vaguely fiduciary language is likely to be misleading, however. The warm and fuzzy phrases used by websites to describe their relationships with unnamed third parties deceptively hide the fact that most websites use language that leaves them completely open to deal with anyone in any manner that they please. There is no evidence and little reason to believe that many websites restrict their activities with third parties to those that promote their users' interests.[146] Some of the better websites are beginning to provide more detailed explanations of their dealings with third parties.[147]

The second fair information practice principle is choice/consent. This principle is connected to the first principle of notice in that when

---

at its sole discretion, to make modifications, alterations or updates to this policy at any time." Kinkos Security & Privacy, *supra* note 112. In other words, Kinkos could at any time change its policy and begin to link up cookie data with personal information. This is precisely what DoubleClick proposed to do before they changed their plans in the face of heavy criticism. *See FTC Lets DoubleClick Off the Hook On Info-Sharing Charge*, E-BUS. L. BULL., Mar. 2001 at 12.

144. *See supra* note 30.

145. *See* Amazon.com, *at* http://www.amazon.com (last visited Nov. 22, 2001).

146. Numerous sites have demonstrated a flagrant lack of discrimination in their dealings with third parties. The Electronic Frontier Foundation launched a campaign in early June 2001 against Macys.com for giving away information from its bridal registry to its business partners. Toysmart.com explicitly promised not to sell data: "Personal information voluntarily submitted by visitors . . . is never shared with a third party." Toysmart Privacy Statement, *at* http://www.ftc.gov/os/2000/07/toyexh1.pdf (last visited Oct. 2, 2001). In bankruptcy, Toysmart then attempted to sell this data. *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 (last visited Nov. 22, 2001); *Judge Is Urged to Reject Toysmart.com Settlement*, WALL ST. J., July 26, 2000, at B2; *Toysmart.com's Plan To Sell Customer Data Is Challenged by FTC*, WALL. ST. J., July 11, 2000, 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.

147. Wal-Mart, for example, describes its dealings with Coremetrics and other third parties. *See* Walmart.com Security & Privacy, *supra* note 92. Once users possess these fuller descriptions, they will be in a position to decide for themselves whether the data transfers will benefit them.

notice is inadequate, consent will be inadequate as well. One cannot consent to what one does not know about. Thus, as a matter of the normative logic of privacy policies, unless a website demonstrates a reasonable degree of respect with regard to the provision of notice, the website cannot demonstrate a reasonable degree of respect with regard to the principle of choice/consent.

As discussed previously, the crucial issue regarding the principle of choice/consent is between opt-in and opt-out.[148] The criticism of opt-out is that it puts the default in the wrong place. The reality of opt-out is that most users do not read and study privacy policies. Thus, most users will not in fact opt out. But this does not mean that they have actually consented to the data policies of the website but merely that they have not read the privacy policy. Thus, it can be argued that if websites were really respectful, they would not go about the collection and use of user data unless they had actual consent from the user.

Websites can argue with some plausibility, however, that opt-in is unduly restrictive in that most consumers do not mind having their data collected and used by websites. Thus, opt-in would place an artificially high burden on all those users who prefer receiving the benefits that various websites have to offer but who do not bother to read privacy policies. In an article discussing junk mail, Richard Posner argues that opt-out was more efficient than opt-in.[149] Similarly, the website industry might argue that it is actually doing consumers a favor to have opt-out instead of opt-in as the former policy will promote efficiency.[150] This example nicely illustrates the important point that one's view

---

148. Many websites' privacy policies are drafted in such a manner, either intentionally or negligently, such that the reader cannot discern if the operative practice is opt-in or opt-out. For example, Hallmark.com states, "We do not currently share your individual customer contact information with third parties for promotional purposes, and we will only do so in the future with your prior approval via email notification." Hallmark.com Privacy Policy, *supra* note 111. It is not clear, however, whether "prior approval" means prior explicit approval or merely the failure to opt-out when notice is provided. "[T]hird party cookies are placed by ad servers on seventy-eight percent of the sites in the Most Popular Group. Of those sites, only fifty-one percent disclose to consumers that they have allowed third party cookies to be placed (and they usually locate that disclosure at the end of the policy statement). Unless consumers are technically skilled enough to set their browser to alert them to cookies or to decline all third party cookies, the placement of third party cookies generally goes unnoticed by consumers." *Prepared Testimony of Sheila F. Anthony FTC Commissioner Before the Senate Committee on Commerce, Science and Transportation, Federal News Service*, 105th Cong., May 25, 2000 [hereinafter *2000 FTC Report to Congress*].

149. *See* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 398 (1978).

150. Opt-out is used "to improve profitability, to improve targeting efficiency and reduce unwanted mailings." *See Web ad agency purchase letting it profile users*, DAILY NEWS (NY), Jan. 27, 2000, at K7259.

regarding the proper scope of the demands of privacy respect may turn on one's higher level normative theory. If one is a consequentialist such as Posner, then respect will be — to proffer a term that may be apt despite its dated coinage — cashed out in terms of wealth maximization.[151] From a deontological perspective, however, respect will not be defined in terms of efficiency but rather independently, or as part of an interrelated set of moral concepts such as autonomy. To respect people is to treat them as autonomous beings. For adherents to everyday Kantian morality, this may entail a prohibition on using their data without explicit notice and consent, even if it may be productive of social utility, or for that matter, a particular user's utility, to do so.

Some sites arguably frustrate true consent by making choices more difficult than need be. For example, 1-800-flowers.com states, "If you prefer not to have us provide personal information collected from you to third parties . . . , please let us know by either: [e-mailing or writing them]."[152] Note that the website does not say to call despite the fact that the name of the company is 1-800-flowers. The site appears not to want to make it easy to opt-out.

The third FIPP is that users should have access to their data and the ability to remove incorrect data. As discussed earlier, a growing number of websites are allowing users some version of these features. What these websites do not typically explain, however, is that this access is nearly always only to so-called personally identifiable data, that is, to data explicitly gathered from the user. This means that the clickstream data collected on the user by means of cookies is not available to the consumer to access or remove. A website might say in its own defense that clickstream data is not personally identifiable and so there is no basis for user concern and thus no reason to provide access or the ability to remove the data. But there is always the possibility that clickstream data can be linked back to users, either by the website that collects the data or by some other website that cares to gain possession of such data.[153] Thus, while the clickstream data is not currently personally

---

151. The elder Posner, along with the younger Mill, attempts valiantly yet unsuccessfully to reconcile consequentialism and libertarianism.

152. 1-800-flowers.com Privacy Statement, *supra* note 91.

153. According to the complaint, in June 1999, DoubleClick acquired Abacus Direct Corp., a direct marketing company that maintains an enormous database of names, telephone numbers, addresses, and purchasing information on millions of people. DoubleClick has matched its 'clickstream' data with personally identifiable information gleaned from the Abacus database to form personally identifiable profiles of the Internet surfing and purchasing habits of millions of individuals. *See DoubleClick Faces Mic. Atty. Gen. Probe and Numerous Privacy Suits*, COMPUTER & ONLINE INDUS. LITIG. REP., Mar. 7, 2000, at 7.

identifiable, it may later come to be so. Thus, respectful websites might provide access to clickstream data (not to mention notice of the potential hookup of so-called anonymous data and user personal identity).

The fourth FIPP is security. As noted earlier, some websites provide SSL protection for personal data while in transit to the website. Other websites provide some protection for the data while in storage at the website, such as by encrypting the data or restricting employee access to the data. While these protections cannot hurt, nevertheless, for most websites, they in no way address the main threat to the security of user data. This threat is due to the loss of control over the data, due to voluntary alienation of the data to third parties. In addition, other sites allow third parties to collect user data but take no responsibility for the actions of these third parties.[154] It is as if websites padlock the backdoor to keep the illegal hackers out but leave the front door wide open for any third party with the means to walk in, conduct a transaction, and leave with the data in hand.

IV. DISCOUNT-RATE SIGNALING VERSUS PRIVACY DISPOSITION SIGNALING

The apparent dearth of substantive privacy protections as evidenced by the above discussion raises the question as to why the increased demand for privacy has not had the effect of bringing about a more robust supply of privacy protections on the part of websites. One possible answer is that the level of demand thus far has not been sufficiently strong to elicit greater supply. In other words, despite the best efforts of privacy norm entrepreneurs, consumer demand has simply not been sufficient to drive websites into a more aggressive posture in terms of providing more respectful practices.

While this is one possible answer, it suffers from the fault that it appears to leave unexplained the deceptive nature of the response on the part of many websites. If there is so little demand for online privacy, why go to the bother of attempting to create the impression in one's visitors that one is a website that is committed to respect for user privacy? Why not just avoid dealing with the topic all together, as any firm must do with a myriad of issues that have a marginal impact on its business model? Thus, a more satisfactory explanation of the website industry response must explain why websites bothered to respond at all.

---

154. *See, e.g.*, Kinko's Security and Privacy Policy, *supra* note 112 ("Some of Kinko's strategic partners, such as those with links on our website, also use cookies, but Kinko's is not responsible for the abuse or misuse of any information gathered through the use of cookies by such third parties.").

One type of explanation that naturally suggests itself is a signaling model. Signaling models seek to explain the manner by which words and deeds can serve a signaling function.[155] A party wishing to communicate a proposition through signaling, rather than merely asserting the proposition, uses words or deeds calculated to elicit the inference that the proposition is true.[156] For example, warranties may be used to communicate that a product is of high quality. The signal works because the sellers of the higher quality products are able to more cheaply send the signal.[157] In the warranty example, Baird, Gertner and Picker explain, "High quality sellers may be able to signal their type by selling goods with a warranty. Because their goods break down less often, these sellers can offer a warranty more cheaply than low-quality sellers."[158]

Perhaps the reason that the words and deeds of many websites appear to be motivated by the desire to deceive rather than to actually provide respect is indeed they are motivated by the desire to falsely signal privacy rather than actually provide it. The following discussion considers two competing signaling accounts, each of which may contain the resources to explain the deceptive, non-respectful actions of the bulk of websites.

A. Signaling Discount Rates

In his recent book, Eric Posner develops an important new theory of norms that sees them as essentially constituted of attempts to signal.[159] Posner argues that social norms are sets of rational acts whereby individuals seek to signal to others that they have low discount rates and hence that they would be good cooperative partners.[160] According to Posner, individuals need to signal that they value the

---

155. *See, e.g.*, DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW, ch. 4 (1994).

156. *See id.* at 123 ("[S]ignaling takes place when those who possess nonverifiable information can convey that information in the way they choose their actions.").

157. *See id*. at 124 ("Assume, for example, that buyers have no direct way of knowing whether a seller makes a high- or low-quality product. High quality sellers may be able to signal their type by selling goods with a warranty. Because their goods break down less often, these sellers can offer a warranty more cheaply than low-quality sellers.").

158. *Id.*

159. *See* POSNER, *supra* note 8.

160. Posner's book develops a "general model of nonlegal cooperation," which consists of a "signaling game in which people engage in behavioral regularities in order to show that they are desirable partners in cooperative endeavors." Posner describes behavioral irregularities used in this way to signal cooperative intent as "social norms." *Id.* at 5. As this quote indicates, Posner appears to believe that his signaling account provides a general account of social norms.

future sufficiently such that they would be willing to forego the immediate benefits of defecting in order to derive the future benefits of a sustained cooperative relationship.[161] Posner makes clear, however, that signaling is a distinct form of activity from cooperative behavior itself. He writes:

> Defection in cooperative endeavors is deterred by fear of reputational injury but the signaling behavior independently gives rise to forms of collective action that can be of great significance. People who care about future payoffs not only resist the temptation to cheat in a relationship; they signal their ability to resist the temptation by conforming to styles of dress, speech, conduct, and discrimination.[162]

As this quote indicates, on Posner's account, signaling allows actors to communicate prior to the establishment of a cooperative relationship that they have the "ability to resist the temptation" to defect in the current game. Thus, signaling is logically prior to actual rational acts of cooperation. It is signaling that may afford actors better opportunities for cooperative relationships at some later date.

Whether cooperation occurs will in part depend on the discount rates of the actors. The more one discounts the future, the less likely one is to forego the immediate one-time benefit gained from the defection in favor of the delayed benefit of future cooperation.[163] Posner refers to those with low discount rates as "good types" and those with high discount rates as "bad types."[164] This bipolar typology is, as Posner notes, a methodological convenience.[165]

---

161. *See id.* at 18–19.

162. *Id.* at 5.

163. *Id.* at 15 ("Then as long as each player cares enough about his payoffs in future rounds — that is, he has a low discount rate — he will cooperate rather than defect in each round.").

164. *Id.* at 18 ("Holding everything else equal, a good type is more likely to cooperate in a repeated prisoner's dilemma than a bad type is, because the good type cares more about the future payoffs that are lost if cooperation fails.").

165. Clearly, in reality there are not simply two types of preferences but rather a continuous set of preferences when it comes to discounting the future. *See id*. at 19. Interestingly, Posner implicitly draws a positive correlation between good and bad types in his sense of these terms and in the ordinary moral sense of these terms. He writes, "The reader should be reminded that a "good" or "bad" type is not necessarily a good or bad person; the label refers to the beliefs of those *within* the group about the hidden characteristics of others." *Id*. at 25.

To distinguish themselves from bad types, good types engage in actions that are called "signals." Signals reveal type if only the good types, and not the bad types, can afford to send them, and everyone knows this. Because a good type is a person who values future returns more than a bad type does, one signal is to incur large, observable costs prior to entering a relationship. For example, if a good type values a future payoff of ten at a ten percent discount and a bad type values the same payoff at a thirty percent discount, the good type can distinguish himself by incurring an otherwise uncompensated cost of eight.[166]

The goal, then, in searching for cooperative partners by watching signals is to find people with low discount rates. Accordingly, actors will seek to convince others that they have low discount rates. Thus, reputation plays a crucial role in Posner's account just as it does in the standard account of cooperation.[167] Signaling, according to Posner, is a means of establishing a reputation as a cooperator. He writes, "One wants a general reputation as a "cooperator," a person with a low discount rate, and one establishes that reputation both by declining to cheat in repeated games and by sending signals at every opportunity."[168] People will attempt to signal that they are good types and attempt to discern that others are good types, based on the signals that these others are sending.

On Posner's account, signals are arbitrary in the sense that any behavior could potentially come to serve as a signal as long as the behavior is observable and has an associated cost.[169] Because the signal is costly, some actors, the bad types, will be prudentially excluded from sending it. The result will be a *separating equilibrium* in which good types act in one manner and bad types act in another manner.[170] For example, a good type may be willing to incur a greater cost from giving a gift in the early period of a relationship than a bad type will.[171] The

---

166. *Id*. at 19.

167. Reputation is a key element in the standard account of cooperation in Prisoner's Dilemma games. While rational actors prefer to defect in a single-shot Prisoner's Dilemma game, they may cooperate when repeated play is possible in order to establish a reputation as cooperators such that others may feel safe in entering into cooperative relationships with them. *See* Ellickson, *supra* note 10, at 180–81.

168. *See* Posner, *supra* note 8, at 21.

169. *See id.* at 29 ("The cooperation game requires that the signal be costly, but nothing about the game dictates the form of the signal. As long as an action is both actually and apparently costly, it can serve as a signal that the sender belongs to the good type."); *id.* at 22-23 ("[S]ignals are costly and observable actions with no necessary or intrinsic connections to the beliefs that they provoke.").

170. *See id*. at 19.

171. *See id*. at 71 (discussing engagement rings as an example of signaling in courtships).

less one discounts the future benefits of the relationship, the more one is willing to spend early on in order to signal one's low discount rate to foster a cooperative relationship. Social norms, then, are simply the patterns of behavior that result as the equilibrium outcomes of various signaling games.

Posner gives a sense of the dynamism of norms. Once norms have been established, there will continue to be forces at play that push toward new norms. Bad types will often seek to *pool* with good types in order to benefit from the signal's power to make others think that the bad type is in fact a good type. But this in turn may lead to good types attempting to migrate to new norms in order to avoid the muddying of the old signal by the bad types.[172]

A possible explanation of the apparently deceptive actions of websites is suggested by Posner's signaling theory of norms. On this account, the emerging website privacy norms are best explained as attempts to signal to users that a website is a good type. Recall that for Posner, a norm is simply a pattern of behavior comprising individual signaling behaviors of the actors seeking to signal that they are good types. In the online privacy context, the relevant norms are the patterns of behavior whereby websites are addressing user privacy concerns by offering privacy policies with varying elements of notice, choice, access and security, enforcement, and instituting Chief Privacy Officers. Good types have low discount rates, that is, they do not highly discount the value of future utility in comparison to present utility. Thus, they are more likely to enter into cooperative relationships that promote future utility despite a sacrifice of present utility.

Posner's good types desire a situation in which good types participate in one practice and bad types participate in another practice, as it is only when there exists a separating equilibrium that the behavior of the good types will be able to effectively serve as a signal of their type.[173] Consider the personal data practices of websites. The equilibrium appears to vary depending on the particular norm. For the norm of disclosing data practices, it appears that instead of a separating equilibrium, there exists a pooling equilibrium in which most websites follow this norm or are inclined to do so in the future.[174] Website

---

172. *See id.* at 19–21.

173. *See id.* at 19.

174. It was earlier a separating equilibrium. According to the FTC's 1998 study, only fourteen percent of websites disclosed their information practices. *See 1999 FTC Report to Congress*, *supra* note 22, at 4. According to the FTC's 1999 study, already sisty-six posted at least one disclosure about their information practices. *Id. at* 7. The 2000 FTC Report indicated that 90% of the surveyed sites posted at least one disclosure about their information practices. *See 2000 FTC Report to Congress*, *supra* note 148, at 10.

behavior appears to be moving in this direction as well for the practice of providing choice, at least when choice is understood in a less demanding sense so as to include opt-out. Thus, a pooling equilibrium has formed for these two norms. The good types are not able to distinguish themselves from the bad types by means of the signals created by participating in these norms.[175]

Note, however, that for the norms of opt-in, security measures, access, redress, and no sales to third parties, it does appear that separating equilibria have formed whereby some websites conform to these norms while other websites do not.[176] One way to interpret these new norms is that they are attempts by good types to find signals that are more costly and not so susceptible to becoming pooling equilibria.

Websites that conform to more demanding norms are actors who are willing to expend costs in signaling at a level that is apparently not sustainable by most websites. Indeed, one conspicuous feature distinguishing these latter norms is that they are costly. For example, an opt-in policy is costly in terms of opportunity costs. The website foregoes the opportunity to gain access to data for free. The costs are more direct for providing access and ability to contest data.[177] Similarly,

---

175. To effectively carry out the false signaling strategy, one must be able to appear cooperative when in fact one is not. Note that this activity appears to be especially easy in the context of website personal data practices, due to the complex nature of these practices and the extent to which such practices are invisible to consumers. In this respect, these practices differ from exemplars of the cooperative model. For instance, one of Ellickson's main examples involves interactions between neighbors over the provision of border fences. Implicit in this example is the fact that one party's cooperation is verifiable by the other party. Each party knows whether the other party is doing its share to bring about the cooperative good because failure to cooperate will be readily apparent. With respect to online privacy, however, this is not the case. A user is not typically in a position to verify whether the notice provided by a site of its data-related practices is indeed an exhaustive account. This difficulty of verification allows room for false signaling. It may be difficult to signal that one will be a cooperative fence builder without actually building a fence, but one may signal that one is a privacy respecter without actually respecting privacy. Thus, in situations in which verification is difficult, it will be important for potential cooperators such as websites to be able to establish that they are trustworthy, as such trust may serve as a proxy for direct verification.

176. *See* Posner, *supra* note 8, at 19–20 ("Signals do not always result in a separating equilibrium. Sometimes an action that served to separate types at time 1 will, because of an exogenous shift in costs, fail to separate them at time 2. If the cost of the signal falls, bad types might join in (they "pool"), in the hope that good types will infer that they (the bad types) are in fact good; or good types will stop sending the signal, because they realize that the bad types can join in, and thus observers cannot distinguish the good from the bad on the basis of who sends the signal.").

177. "Among the questions the [2000 FTC] report raises is whether the costs of access — measured by money, convenience or privacy risks — would be too high, for businesses and consumers alike." Web Privacy Task Force Split on Need for Rules, N.Y. TIMES, May 15, 2000, at C4.

the costs of security measures are also direct and come from the cost of supplying the security.

Thus, some websites conform to norms that cost them significantly. Posner's account explains why some websites have shown an interest in providing these more costly forms of regard for consumer data. The motivation is to signal that they are good types and to signal in a manner that is not easily duplicated by bad types, thus enabling the good types to establish a separating equilibrium for each of the more costly practices.

B. Signaling a Respectful Disposition

It may not be so simple, however, to apply Posner's model to explain the response of websites to the heightened concern for consumer online privacy. There appears to be an important difference between the norms as characterized in Posner's model and the norms that arise in the context of website privacy-regarding activities. Contrary to Posner's model, some websites are not seeking to signal that they are good types; they are in fact taking steps that would be required of good types. Thus, their behavior is best understood not as signaling future cooperative acts but as actually engaging in cooperative acts. Posner's model is, in effect, always looking ahead to a future of cooperating after signaling is complete. But in fact some websites have already taken significant steps to begin cooperative relationships with users. Posner errs, then, by using signaling of discount rates as the sole explanation for norms.[178]

1. An Iterated Prisoner's Dilemma Model of User/Website Cooperation

The heart of cooperative solutions to iterated Prisoner's Dilemmas is that the parties incur short-term costs in order to engender long-term gains. Each party has the opportunity to defect in the first round of a game. Defection is the dominant strategy in a single-shot game; each party does best by defecting regardless of the choice made by the other party. However, when there is an opportunity for the parties to interact over time in a repeat game situation, it may be rational for each party to adopt a cooperative strategy in which each defers the immediate gain

178. Posner apparently intends his account of norms to be an account of all norms, that is, all norms can be explained as signaling equilibria. *See* Richard H. McAdams, *Signaling Discount Rates: Law, Norms, and Economic Methodology*, 110 YALE L.J. 625, 654 (2001) (reviewing ERIC A. POSNER, LAW AND SOCIAL NORMS (2000)) ("I think it [is] fair to read Posner as offering signaling . . . as a general account of social norms.").

from defection in order to realize long-term gains that may result from cooperation.[179]

Cooperation in a repeat game is a better description of what occurs with some websites, for they do sometimes incur significant short-term costs in order to provide privacy protections. Consumers may feel entitled to respect and will trust websites that can demonstrate that they are worthy of trust. Thus, there is the prospect for a cooperative relationship in which users and websites exchange trust for respect.

Consumers may not view their relationship with websites as strategic until they perceive 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 retaliate against those that fail to show respect.[180]

For example, when a website offers an opt-in policy, guarantees that it will not transfer data to third parties, provides access and redress, or provides heightened security, the website incurs real costs with the apparent goal of meeting consumer demand. These costs are distinct from the costs that may be incurred by websites that are only interested

---

179. This point was illustrated by Robert Axelrod's computer tournaments. *See* ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984). When a Prisoner's Dilemma game is repeated, and if the incentive to defect is no longer dominant because defection may provoke the other side into defecting in future rounds, cooperation may induce cooperation. If the parties care enough about the future, the discounted benefit from mutual cooperation in future rounds may exceed the immediate benefit from defecting. Cooperation is not the dominant strategy, however, because that strategy is easily exploited by strategies that always defect. Even conditional cooperation like the tit-for-tat strategy that won the Axelrod tournament is not dominant. But the well-established result is that repetition of the game makes cooperation possible; sustained conditional cooperation is one possible equilibrium for the repeated game.

180. Retaliation may take the form of negative gossip or providing false or misleading information to the website.

> 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.

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

in signaling a low discount rate. With Posner's signaling account, there is no cost associated with actually engaging in the cooperative relationship, as the actual cooperation is in the future. Websites that are actually incurring real costs as part of an already ongoing cooperative relationship have moved beyond merely signaling and are actually playing out the cooperative endeavor.[181]

The situation is strategic because websites are in a position to choose whether to respect the consumer and engender consumer trust. 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.[182] The strategic structure of the situation is represented in Figures 1 and 2.

Figure 1: Large Website/Consumer Interaction

		Large Website	
		Privacy Policy	No Privacy Policy
Consumer	Trust	3, 3	1, 4

181. The notion of website visitors choosing to trust websites is similar to Richard McAdams's idea that actors can choose whether to esteem another party with whom they are interacting. *See* Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV., 338, 355–72 (1997). 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, trust is not an item that websites would independently desire. Rather, a website would prefer to gain the trust of its visitors because this trust will be positively correlated with these visitors choosing to interact with the website in the future. Similarly, Robert Cooter's internalization account of norm conformity appears not to play a role as websites are commercial enterprises that are not readily susceptible to the psychological phenomenon of internalization. *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, 1693–94 (1996).

182. Prior to the bursting 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.

No Trust	4, 1	2, 2

Figure 2: Small Website/Consumer Interaction

		Small Website: Privacy Policy	Small Website: No Privacy Policy
Consumer	Trust	2, 2	1, 4
	No Trust	4, 1	3, 3

Each party has two choices, each affecting the utility of the other party.[183] Each party must consider how its choice and the choice of the other party will affect its payoff. This means that each party will consider whether it 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.[184]

Because of these strategically interactive 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. As recently as a few years ago, only a minority of websites — the larger and better-known ones — offered privacy

183. 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.

184. 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.

policies.[185] 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. The number of websites that show respect for privacy has continued to grow, however, as public consciousness of online privacy has grown.[186]

Despite the growing sense of consumer entitlement, many small websites may still prefer to avoid the expense of providing privacy policies. As illustrated in Figure 2, many small websites may still prefer the outcome of mutual non-cooperation (southeast cell) to that of mutual cooperation (northwest cell).

2. Mimicking Respect for User Privacy

Although Posner's signaling model fails to account for the genuinely cooperative behavior taking place between some websites and their users, an alternative signaling model may be appropriate. As noted earlier, warranties are a standard example of a signal. In the case of online privacy, privacy policies may serve a parallel role to warranties. If the analogy is to work, there must be some parallel to the nonverifiable information the seller possesses about the good that is protected by the warranty. In the privacy context, however, it is not necessarily or typically the case that one purchases a product from the website one visits. This may be true in some circumstances such as if one purchases a book from Amazon and Amazon collects data pursuant to this transaction, but most website visits do not result in a transaction. The privacy relationship between websites and users, then, is not inherently part of any transaction between these parties. A better analogy may be drawn between the online experience and the experience of customers while in the store of a seller. For example, a customer may be surreptitiously monitored while trying on apparel in the dressing room of a store.[187]

---

185. In the Federal Trade Commission's 1998 study, only fourteen percent of websites were addressing consumer privacy issues. *1998 FTC Report to Congress*, *supra* note 29, at 27. As consumer sense of entitlement grows, the chances of plaintiffs' lawyers prevailing in lawsuits grows. *See* Matt Fleischer, *Click Here for More Web Suits: Lawyers Eye Privacy Cases Against Many DoubleClick Rivals*, NAT'L LAW J., Feb. 28, 2000, at A1 (noting many lawyers are now searching for the next privacy lawsuit against DoubleClick competitors, such as Engage, 24/7 Media, MatchLogic, Flycast, and L90).

186. *See 1999 FTC Report to Congress*, *supra* note 22, at 6–7.

187. People v. Moreno, 135 Cal. Rptr. 340 (Cal. App. Dep't Super. Ct. 1976) (examining whether the actions of a security guard violate a customer's privacy when the guard observes the customer through the slits of the dressing room door).

The nonverifiable information that the website has and the user does not is the website's 'privacy disposition,' in other words, the level of its commitment to respecting consumer privacy and its competence to fulfill this commitment. While such dispositions of a firm may be less sticky than the dispositions of persons, what matters is not that such dispositions are immutable but that they are relatively stable.[188] Walmart.com's disposition to be concerned for user privacy is stable in the sense that Wal-Mart, the parent corporation, will continue to have an important interest in its reputation with its customers.[189] This disposition is not readily knowable to the website's users, however. Accordingly, there is the possibility that the privacy policy may be used to signal that this website has good privacy dispositions. [190]

The reason warranties work as signals is because firms with high-quality products can provide warranties more cheaply than firms with low-quality products. Is the same true for privacy policies? In other words, will websites with more respectful privacy dispositions be able to offer privacy policies more cheaply? The answer appears to be yes, at least some of the time.

One can imagine two websites that each offer the same fairly rigorous privacy policy. Imagine further that one of these websites, call it Wal-Mart, has more respectful privacy dispositions than another website, call it Toysmart. Wal-Mart will be able to live up to the policy's commitments more cheaply than Toysmart. The implication is that websites that have more respectful dispositions such as Wal-Mart will be able to provide privacy policies more cheaply than websites such as Toysmart that have less respectful dispositions.

One might expect, then, that the Wal-Marts of cyberspace would offer privacy policies while the Toysmarts of cyberspace would not.[191] This is not what has happened however. Instead, privacy policies have become ubiquitous. The reason appears to be that the less respectful websites do not duplicate the signal with exactitude but rather mimic it with an inferior substitute, yet one that is not readily discernable as

---

188. *See generally* ROBERT H. FRANK, PASSIONS WITHIN REASON: THE STRATEGIC ROLE OF THE EMOTIONS (1988).

189. This is not to say that Wal-Mart's disposition is immutable. Wal-Mart.com could be spun off, have a name change, and re-emerge as a more aggressive data gatherer and user.

190. Some people claim to be indifferent to the use of their personal data by websites. They say things like, "I have nothing to hide" or "I like the idea because it will lead to more personalized marketing." Even a user who does not care about whether her data is used by websites might still rationally prefer to be dealing with a website that took privacy seriously because such a site would be signaling that it was interested in long-term relationships generally.

191. BAIRD ET AL., *supra* note 155.

inferior by the typical user. As was seen in Part III, many websites use deceptive language to create an impression in users that they are being accorded a higher level of respect than is in fact the case. To the average consumer, these privacy policies are not readily distinguishable from the privacy policies of the more genuinely respectful websites such as Wal-Mart.

This attempt by some websites to offer privacy policies that superficially mimic the better privacy policies but are inferior in their details therefore, is a plausible explanation for privacy policies that are characterized by privacy activists as deceptive.

C. Normative Implications

Part III is an account of a complex regulatory system comprising informal social processes and legal rules. It is important that those interested in privacy, from whatever normative perspective, have the best possible understanding of the detailed workings of this system. Like it or not, this is the system currently in place. The task of any advocate is to evaluate this system in terms of the goals of privacy. Is this system the best system for promoting online privacy according to the goals of each particular advocate? If the answer is no, then what would a better system be? A better system must build on what is currently there, seeking to improve or replace some features while perhaps simply fine-tuning others.

As a matter of moral logic, one cannot derive a normative conclusion from factual premises without the addition of a normative premise. Thus, raising the question of normative implications immediately raises the further question: normative implications for whom and based on what normative premises? The supply and demand model of the emergence of website privacy norms implies not categorical but rather hypothetical imperatives that will depend on the particular normative premises that are combined with the positive analysis. In the interest of maintaining the objectivity of the positive analysis, no normative premises will be given priority here.

Of the actors who bring different normative premises to the table, two broad categories may be distinguished: those who are publicly interested and those who are privately interested. Those who are publicly interested are the privacy norm activists. Those who are privately interested but who may nevertheless act in a manner that promotes the public interest for instrumental reasons are the other norm entrepreneurs, namely, the FTC and software firms as well as the websites.

Within the group of actors with intrinsically publicly interested motivations, there may be principled disagreement. Different actors have different moral conceptions of privacy. It will matter, for example, whether one is a privacy deontologist or a privacy consequentialist. When privacy concerns conflict with efficiency concerns, deontologists will be willing to trade off welfare in order to reduce the amount of disrespect for privacy while consequentialists will not. Even among deontologists, there will be divergent normative positions. Some privacy advocates want to reduce the flow of personal data as a normative goal in itself. Other advocates have what can be characterized as an autonomy-based conception of privacy regulation. Reducing the amount of data flow is not a goal per se. What matters is that all transmission of personal data respects the autonomy of the participating parties. On this view, while one may indeed have dramatically less privacy if one lives in a glass house, this is not a problem as long as one autonomously chooses to live in a glass house. There is, however, common ground among the various normative positions. In fact, there is a growing consensus that online privacy should be promoted. This is the hypothetical imperative that will be taken as operative in the following brief analysis of the normative implications of the positive account. In other words, what are the normative implications of the positive account, given the general hypothetical imperative that respect for consumers' online privacy should be promoted? The normative implications fall into two broad categories, implications for the demand side and implications for the supply side.

On the demand side, the goal will be to maintain and increase the level of demand by consumers for more respectful treatment of their data by websites and third parties. This is the demand that creates an incentive for suppliers of privacy, websites, to reflect on whether it is in their interest to supply greater privacy. On the demand side, we saw that norm entrepreneurs and particularly norm proselytizers have done a good job to stimulate the emergence of a sense of entitlement in consumers to a reasonable level of control over their personal data. As the above discussion indicated, there are now a large number of websites that are beginning to incur real costs in order to enter into cooperative relationships with users. The more demand for respectful treatment, the more websites at the margin will find it in their interest to begin making cooperative gestures. Generally, then, the normative implication on the demand side would appear to be simply that there should be an effort to continue to stimulate demand for online privacy.

On the supply side, one might initially suppose that if indeed demand is increased, as prescribed above, then supply should naturally

take care of itself, rising to meet the higher level of demand. As the foregoing discussion has made clear, however, such an assumption may not hold true. The efforts of those websites that want to be more respectful will be hampered by the existence of websites with inferior privacy dispositions that mimic the websites with higher-quality privacy dispositions.

For privacy activists, then, the general task on the supply side is to reduce the incidence of false signaling in the hope that this will increase genuinely cooperative behavior. Websites with cooperative dispositions need to find a way to signal exclusively. To achieve this, the signal must be costly so that the websites with inferior dispositions cannot send it. This raises the question as to whether there are norms that make it easier for cooperative websites to distinguish themselves. For example, if opt-in became a more dominant norm, this might make it easier for good types to distinguish themselves. It would force many websites to either adopt an opt-in practice be in the vanguard of respectfulness or else live with the consequences of being seen as less respectful.

Consider a second example. Earlier discussion indicated why it may not be possible to have a norm that prohibit transfers to third parties under any circumstances. This seems like it is not a possible norm because even websites with no core interest in transferring data for profit-based reasons may sometimes need to do so in order to better perform the site's functions. This has caused some sites to note explicitly that they only transfer data for this purpose. This is indeed a norm that bad sites cannot easily mimic.[192]

Clearly, then, there may be room for creative solutions to the problem of how cooperative websites can distinguish themselves from bad sites. Note that while false signaling may be bad, it need not deter good types from conforming to cooperative norms. Even though bad websites promise notice and consent but do not deliver, it may still be rational for good types to perform these actions, as they are part of cooperating.[193]

---

192. TRUSTe was supposed to be a way for sites to certify that they were legitimate in their respect for privacy. TRUSTe has had limited success. It has been criticized for being too lax in its standards. Note that while TRUSTe as a firm has been heavily criticized, there has been support for the general plan of the firm. *See* Edmund Sanders, *The Cutting Edge: Focus on Technology; Web Privacy Programs are Scrutinized; Government May Interfere as Self-Regulation Falters*, L.A. TIMES, Dec. 11, 2000, at C1 (criticizing TRUSTe); Robert MacMillan, *TRUSTe Will Develop Privacy Symbols, Lables Guide*, NEWSBYTES, June 19, 2001 (supporting TRUSTe).

193. *See* BAIRD ET AL., *supra* note 155, at 124 (noting that there may be other reasons for taking an action in addition to its signaling function).

One might think that making it easier for websites with high-quality privacy dispositions to signal will not make any difference since people do not read privacy policies. Even though privacy policies are just a click away, users may rarely read them. Any discussion of normative implications must account for the fact that people do not read privacy policies.[194]

Websites, however, can develop reputations for respecting privacy. Consider Wal-Mart. Even though most people will not read their privacy policy, Wal-Mart still has an incentive to make the policy statement a respectful one. Doing so is a central means for Wal-Mart to foster a reputation as respectful of privacy. Privacy activists may have a significant influence in the general reputations of large firms such as Wal-Mart, and these activists are better informed about Wal-Mart's privacy practices.

A general lesson, then, is that privacy proselytizers should seek to publicize the reputations of websites. Privacy proselytizers may help to channel website activity into more defined forms in order to further aid in public comprehension of website reputations. Posner provides an interesting account of marriage laws that lends insight into how more defined forms can be advantageous. He notes that whereas in contract law, generally the parties are allowed almost complete freedom to determine the terms of the deal, this is not true for marriage contracts, which are highly specified by the government.[195] Posner argues that this promotes the emergence of uniform social norms surrounding marriage. A similar observation may be made about the role of the FIPPs. Privacy entrepreneurs have engaged in an effort to channel the privacy-regarding practices of websites into a small number of specific forms. Reduction to these specific forms may have an effect of making it easier to signal.[196] For example, privacy proselytizers may be able to more effectively promote the norm of consent through the articulation of the categories of opt-in and opt-out. The fact that there are precise names for these activities and that a number of websites are engaged in them allows consumers to attach a fairly precise meaning to these behaviors.

Although an increasing number of websites may find it in their interest to be respectful, many sites continue to provide false signals of their willingness to cooperate. These are the bad actors that perhaps

---

194. It is probably not realistic to think that consumers will start to read privacy policies on a larger scale.

195. POSNER, *supra* note 8, at 79.

196. Note that there is anecdotal evidence that many websites, small websites in particular, derive their privacy policies by cutting and pasting from the privacy policies they find on the Web. This form of copyright violation may serve the useful but unintended purpose of furthering the uniformity of privacy norms.

only a statute will deter. This does not mean, however, that self-regulation has been an abject failure. One can acknowledge that a growing number of websites are acting in a more respectful fashion and yet believe that, on the whole, the amount of disrespect is too high to tolerate. On the other hand, one might conclude that some amount of false signaling is a tolerable cost to bear given the set of alternatives and their associated costs.