University of Richmond Law Review

Volume 36 | Issue 2 Article 2

2002

Cyberian Signals

Steven A. Hetcher

COMMENTARIES

CYBERIAN SIGNALS

*Steven A. Hetcher**

INTRODUCTION

In *Law and Social Norms*,[1] Eric Posner offers an original and important theory of the emergence of norms. According to Posner, norms are collections of signals. He develops his signaling account in a variety of contexts, including criminal law, family law, political participation, and racial discrimination. This article extends Posner's theory to cyberspace, a domain of social organization not touched on in Posner's book. In particular, I will test Posner's theory by examining how well it explains the emergence of Web site privacy norms.[2] Part One will examine signaling theory. Part Two will explore privacy norms in some detail, and Part

* Associate Professor of Law, Vanderbilt University School of Law. I wish to thank Robert Rasmussen for taking the time on numerous occasions to discuss signaling theory and other issues that undergird the analysis in this article. I am grateful for the expert research assistance of Janet Hirt and Angela Vitale.

1. ERIC A. POSNER, LAW AND SOCIAL NORMS (2000).

2. There is some reason to doubt that effective norms will form in cyberspace. *See* Mark A. Lemley, *Shrinkwraps in Cyperspace*, 35 JURIMETRICS J. 311, 313–14 (1995) ("Informal social norms worked fairly well when the Internet community was small and relatively insular. . . . The addition of fifteen million new users to the Internet in the last decade may have made private ordering impossible, except in a few specialized corners of cyberspace."). There are a number of competing accounts of norms. One means of evaluating the merits of these accounts is to see how they handle particular concrete occasions in which norms have emerged. 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, 551 (1998).

Three then will apply signaling theory to privacy norms.[3] The conclusion states that these new norms are not best understood as collections of signals.

I. SIGNALING DISCOUNT RATES

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.[4] According to Posner, individuals need to signal that they value the future sufficiently such that they would be willing to forgo the immediate benefits of defecting in order to derive the future benefits of a sustained cooperative relationship.[5] Posner makes clear, however, that signaling is an activity distinct from cooperative behavior itself.[6] 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 to cheat by conforming to styles of dress, speech, conduct, and discrimination.[7]

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.[8] Thus, signaling logically occurs prior to actual rational acts of cooperation. It is signaling that

---

3. Robert Ellickson's path-breaking book on law and norms devotes the first six chapters to a detailed sociological survey of the norms of Shasta County, California, before turning to a theoretical analysis. *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991).

4. POSNER, *supra* note 1, at 5. 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." *Id.* Posner describes behavioral regularities used in this way to signal cooperative intent as "social norms." *Id.* As this quote indicates, Posner appears to believe that his signaling account provides a general account of social norms.

5. *Id.* at 18–19.

6. *Id.* at 5.

7. *Id.*

8. *Id.*

may afford actors better opportunities for cooperative relationships at some later date.[9]

Whether cooperation occurs depends in part on the discount rates of the actors.[10] The more one discounts the future, the less likely one is to forgo the immediate one-time benefit gained from defection in favor of the delayed benefit of future cooperation.[11] Posner refers to those with low discount rates as "good types" and those with high discount rates as "bad types."[12]

> 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 10 at a 10 percent discount and a bad type values the same payoff at a 30 percent discount, the good type can distinguish himself by incurring an otherwise uncompensated cost of 8 . . . .[13]

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.[14] Thus, reputation plays a crucial role in Posner's account, just as it does in the standard account of cooperation.[15] Signaling,

---

9. *See id.*

10. *See id.* at 14–15.

11. *See 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.").

12. *See 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."). The bipolar typology is, as Posner notes, a methodological convenience. *Id.* at 19. 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. *Id.* 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.

13. *Id.* at 19.

14. *Id.*

15. *Id.* at 12–13. Reputation is a key element in the standard account of cooperation in prisoner's dilemma ("PD") games. While rational actors prefer to defect in a single-shot PD 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 3, at 180–81.

according to Posner, is a means of establishing a reputation as a cooperator.[16] He writes: "One wants a general reputation as a 'co-operator,' 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."[17] Individuals attempt to signal that they are good types and attempt to discern that others are good types, judging by the signals they are sending.[18]

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.[19] Because the signal is costly, some actors—the bad types—will sometimes be prudentially excluded from sending it.[20] The result will be a *separating equilibrium* in which good types act in one manner and bad types act in another.[21] For example, a good type may be more willing to incur a greater cost from giving a gift in the early period of a relationship than a bad type.[22] The 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.[23] Social norms, then, are simply the patterns of behavior that result as the equilibrium outcomes of various signaling games.

According to Posner, norms have dynamic properties as well.[24] Once norms have been established, there will continue to be forces at play pushing 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.[25] However, this in turn may lead to good types attempting

16. POSNER, *supra* note 1, at 21.

17. *Id.*

18. *Id.*

19. *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."); *see also id.* at 22–23 ("[S]ignals are costly and observable actions with no necessary or intrinsic connections to the beliefs that they provoke.").

20. *Id.* at 19.

21. *Id.*

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

23. *Id.*

24. *Id.* at 21.

25. Posner explains that

> [s]ignals do not always result in a separating equilibrium. Sometimes an ac-

to migrate to new norms in order to avoid the muddying of the old signal by the bad types.[26] With Posner's signaling theory in mind, consider next the following descriptive account of the emergence of Web site privacy norms.

II. THE EMERGENCE OF ONLINE PRIVACY NORMS

A. *Creating Demand for Online Privacy*

The norms governing personal data interactions between consumers and Web sites have changed dramatically in the past few years. Increasingly, there is a moral sensitivity among consumers regarding the collection and use of their personal data by Web sites.[27] Consumers now perceive a general right to privacy in cyberspace that includes respectful treatment of their personal data. Web sites increasingly recognize this sense of entitlement. One Internet entrepreneur summarized the situation as follows: "'Companies used to think of customer data as theirs. They're starting to realize they're really custodians, and the customer controls the information.'"[28] In other words, the social meaning of personal data collection has changed from a morally neutral to a morally charged status.[29] This change is due to the actions of pri-

---

> tion 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.

Id. at 19–20.

26. *Id.* at 19–21.

27. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1465 (2000). The connection between the collection of personal data and personal privacy is straightforward; the more personal data that Web sites collect, store, and use, the less privacy that data subjects have. There are two broad categories of personal data: (1) information that can be used to identify consumers ("personal identifying information," including name and postal or e-mail address); and (2) demographic and preference information (including age, gender, income level, hobbies, and interests). FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 20 (June 1998) [hereinafter FTC 1998 PRIVACY REPORT], *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf; Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1283–86 (2000).

28. Paul Davidson, *Marketing Gurus Clash on Internet Privacy Rules*, USA TODAY, Apr. 27, 2001, at 1B (quoting Hans Peter Brondmo).

29. *See, e.g.*, *The End of Privacy*, THE ECONOMIST, May 1, 1999, at 21; Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 182–83; Jared Sandberg, *Losing*

vacy norm proselytizers and other norm entrepreneurs who possessed an interest in promoting online privacy.[30]

The normative debate that increasingly surrounds data collection practices is evidence that consumers are developing a more complex understanding of Web site activities. Most important, interactions between Web sites and their visitors are framed in terms of privacy.[31] In particular, commercial data collection is widely understood to raise concerns for a new species of privacy: informational privacy 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 Web sites that fail to respect this entitlement. In terms of the emerging moral discourse for governing online personal data, Web sites *ought* to respect the data privacy entitlements of consumers.[33] Web sites that do so may earn

---

Your Good Name Online, NEWSWEEK, Sept. 20, 1999, at 56; Celia Santander, *Web-Site Privacy Policies Aren't Created Equal*, WEB FIN., Dec. 11, 2000. Opinion polls show increasing public concern with respect to online privacy. *See* Glenn R. Simpson, *E-Commerce Firms Sort 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 Web sites sharing personal information with other sites. *Business Week/Harris Poll: A Growing Threat*, BUS. WK. ONLINE (Mar. 20, 2000), *at* http://www.businessweek.com/2000/00_12/b3673010.htm.

30. *See* Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERKELEY TECH. L.J. 877, 880 (2001). "Norm proselytizers promote norms for moral reasons that they themselves accept." *Id.* at 935 n.4. Norm proselytizers, then, are a sub-category of norm entrepreneurs. Norm entrepreneurs are actors who promote normative change. *See* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909 (1996). *See generally* Robert C. Ellickson, *The Market for Social Norms*, 3 AM. L. & ECON. REV. 1, 15 (2000).

31. Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 179 (1999) ("'Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century.'" (quoting Marc Rotenberg)).

32. *See* Diane McDougall, *Embrace Privacy*, CMA MGMT., Nov. 1, 1999, at 13 ("Concern about informational privacy in the marketplace has risen . . . .").

33. *See* 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."); Edward J. Markey, *We Must Act Soon to Protect Online Privacy*, THE HILL, Feb. 7, 2001.

> 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 informa-

the *trust* and *confidence* of consumers, while Web sites that do not may be subject to informal sanctioning by consumers.[34]

Privacy proselytizers have acted as industry watchdogs and legislative proponents.[35] They were instrumental in lobbying for

---

tion for special offers, but we don't trade customer information without their prior consent."

David Cohen, *Be Sure You Never Take a Cookie from Strangers*, THE GUARDIAN (London), Apr. 1, 2000, at 22.

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

> 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.

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) (citation omitted).

> 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.

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

35. Ethical hackers and corporate watchdogs have been highly successful in discovering dubious Web site practices. Among the best examples of privacy activism targeting private companies surrounded DoubleClick's acquisition of Abacus Direct. Its intention was, contrary to earlier representations, to combine the online and offline personal data from both enterprises. The advocacy community brought the plan to the attention of the media, which gave generous attention to the story. The price of DoubleClick's stock dropped precipitously as the story unfolded in the press, destroying billions of dollars in the company's market capitalization. The company has subsequently been embroiled in lawsuits and subjected to a heightened level of scrutiny from privacy activists and the FTC. *See* Jeri Clausing, *Privacy Advocates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000, at C2; *Privacy on the Internet*, N.Y. TIMES, Feb. 22, 2000, at A22; Diane Anderson & Keith Perine, *Privacy Issue Makes DoubleClick a Target*, INDUSTRY STANDARD, *at* http://www.thestandard.com/article/0,1902,9480,00.html (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; *see also Junkbusters Urges Vigilance from FTC and Parents to Protect Children from Corporate Surveillance and Manipulation*, BUS. WIRE, Apr. 20, 1999:

the enactment of the Children's Online Privacy Protection Act ("COPPA").[36] More recently, they have pushed for an extension of this regulatory framework to adults.[37]

Privacy proselytizers have attempted to educate the public and the media about the dangers of emerging data collection practices. They have also sought to change these groups' moral perspective regarding personal data by citing a relationship of responsibility between the data practices of Web sites and consumers' loss of privacy. Privacy proselytizers have steadfastly refused to dismiss consumer privacy loss as a necessary casualty of the emergence of electronic commerce.

Proponents of privacy espouse a number of concrete norms, most notably *notice*, *consent*, *access*, *security*, and *enforcement*. At least in public discourse, some members of the Web site industry accept the requirement of notice. The second most often mentioned requirement of data privacy is some form of consent. There is great disagreement, however, regarding the appropriate defini-

---

> 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.

Id.; 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); *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); *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Courts & Intellectual Prop. of the House Comm. on the Judiciary*, 105th Cong. 113–18 (1997) (statement of Marc Rotenberg, Executive Director, EPIC).

36. Gwen Carleton, *Privacy, for the Sake of the Children*, 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.").

37. *See* 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."); 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 some minuses,' says Marc Rotenberg . . . . 'What we really need is a base-line privacy bill for all users of the Internet.'").

tion of consent in the context of Web site data gathering.[38] In an opt-out regime, personal data will automatically be collected unless a consumer specifically acts to indicate otherwise.[39] Industry groups such as the Online Privacy Alliance have promoted an opt-out policy as a minimum requirement for members.[40] By contrast, in an opt-in regime, the default is that personal data will not be collected unless the consumer explicitly agrees.[41] Privacy advocates are typically advocates of an opt-in policy.[42]

Thomas Cooley defined privacy as the right to be let alone.[43] Respect for consumer privacy online cannot mean that Web sites should literally leave consumers alone: consumers are the ones who visit Web sites. Instead, the core meaning of privacy in the context of Web site personal data practices is that the Web site should leave the visitor's data alone, except to the extent the visitor consents to her personal data being collected and used. When

---

38. 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.

Id. 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).

39. *See* Amy Borrus, *The Stage Seems Set for Net Privacy Rules This Year*, BUS. WK., Mar. 5, 2001, at 51 ("Opt-in is a far higher hurdle than opt-out, which allows a company to gather data until a consumer orders it to stop.").

40. *See* Online Privacy Alliance, *Guidelines for Online Privacy Policies*, *at* http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited Mar. 21, 2002). The Alliance is a coalition of more than eighty companies and trade associations formed in early 1998 to encourage self-regulation of data privacy.

41. Borrus, *supra* note 39, at 51.

42. Some are hopeful that President Bush will push for "opt-in" rules.

> [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."

Id.

43. *See* THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888). Fair information practices allow each of us to tell the world to mind its own business. *See* William Safire, *Stalking the Internet*, N.Y. TIMES, May 29, 2000, at A15. *See generally* Kutz v. United States, 389 U.S. 347 (1967).

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 Web site disrespecting the visitor because the collection and use occurred with the visitor's consent.[44] 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 Web sites.[45] A fourth element of the general right to data privacy is *security* for personal data residing in databases of commercial firms.[46] If personal data is easily accessible to hackers or corporate affiliates, the Web site may be indirectly responsible for injuring the consumer whose data is stored with the Web site, even if the Web site is not itself guilty of any active wrongdoing. Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of an *enforcement* principle, which requires sanctions for noncompliance with fair information practices.

---

44. *See* John Walsh, *Websites with a Personal Touch*, FIN. TIMES, Mar. 15, 2001, at 6 ("Do consumers mind being asked to part with information in order to receive personalised goods and services? Most early research would suggest that they do not, so long as they perceive a benefit, such as reading a newspaper for free or saving time."); Fred O. Williams, *Area Man Wins Cybercash*, BUFFALO NEWS, Oct. 28, 2000, at 11C ("[C]onsumers appear willing to exchange personal data for free prizes and cash . . . .").

45. Consumer security remains high on the list of privacy advocates.

> 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.

Drew Clark, *Activists Unite to Push for Stronger Privacy Laws*, NAT'L J. TECH. DAILY, *at* http://nationaljournal.com/pubs/techdaily (Jan. 30, 2001).

46. *See* Stewart Baker, *Regulating Technology for Law Enforcement*, 4 TEX. REV. L. & POL. 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.

Id.

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. Note that this norm does not entail a consumer right to ownership of individual personal data.[47] If consumers owned their personal data, presumably they 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 best be treated as inalienable.[48]

An important implication follows from the activities of privacy proselytizers in creating a sense of consumer entitlement to personal data. The more strongly consumers feel about a data privacy entitlement, the more they will be morally affronted by instances where Web sites infringe upon their privacy. Accordingly, they will be slower to trust Web sites and more inclined to punish those that fail to respect consumer privacy.

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 Federal Trade Commission ("FTC") and a number of firms that market privacy-related software.[49]

Since the mid-1990s, the FTC has reinforced the privacy-promoting efforts of the privacy proselytizers.[50] The FTC acts pursuant to its authority under the Federal Trade Commission Act,[51] which mandates that the agency address "unfair" and "deceptive" trade practices.[52] The FTC casts Web site data-gathering

47. 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.

48. *See, e.g.*, Samuelson, *supra* note 34, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights.").

49. *See generally* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

50. *Id.*

51. 15 U.S.C. §§ 41–58 (2000).

52. *Id.* § 45(a)(1). The FTC prosecutes "[u]nfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce." *Id.* The FTC has the authority to file suits for violations of section 45(a)(1). *See id.* § 57(a). The FTC is "empowered and directed" to create rules to prohibit deceptive or unfair practice prevalent in certain indus-

practices as potentially unfair and deceptive.[53] In particular, the agency has borrowed the various specific privacy protection measures supported by the privacy activists—notice, consent, access, security, enforcement—and shrouded them in the rhetoric of fairness.[54] When Web sites adopt the FTC's suggestion and seek to implement the fair information practices via privacy policies, the FTC's regulatory grasp is enhanced.[55] Furthermore, once Web sites make representations to consumers regarding their practices, the FTC has a claim to jurisdiction if the Web sites behave differently.[56]

Software vendors, marketing so-called privacy solutions, have recently emerged as a new type of privacy norm entrepreneur.[57] Privacy solutions are software that users or Web sites can install in order to create a more privacy-respecting online environment. While Web sites are typically the direct purchasers of these products, software developers also advertise their products to consumers. As more advertisements foster moral concern among consumers, greater social pressure toward increased privacy

---

tries. *Id.* § 45(a)(2).

53. 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 Web site activities without a change in the intellectual property status of personal data.

54. FTC 1998 PRIVACY REPORT, *supra* note 27, at 7. The FTC explicitly states that it takes its normative framework from the privacy policy community. *Id.* at 48 n.27.

55. *See* Hetcher, *supra* note 49, at 2057.

56. The FTC's role in helping to moralize the social meaning of data collection can be understood in public choice terms as an effort to extend the agency's purview over the burgeoning Web site industry. 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. *Id.* at 2053.

57. *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); *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.").

> 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.

Graubert & Coleman, *supra*, at 290.

protection will be exerted on the Web site industry.[58] 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 further galvanized in the direction of greater demand for more respectful Web site privacy practices. For Web sites at the margin, it may now make sense to switch to more respectful norms.

B. *Meeting the Demand for Online Privacy*

The previous section analyzed a surge in the demand for privacy among consumers due to the efforts of norm proselytizers and norm entrepreneurs. This section will examine the impact of this increase in demand on the level of supply. Generally, when demand for a good or service increases, the supply increases 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, Web sites that can cheaply supply privacy will be more inclined to do so, while Web sites for which it is more expensive would tend to provide less privacy.[59] In addition, Web sites whose customers are

58. *See, e.g.*, Zeroknowledge, Advertisement, WIRED, Aug. 2000, at 5–6. The ad 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 Web site industry: "I AM NOT A PIECE OF YOUR INVENTORY. I am not a pair of eyeballs to be captured or a consumer profile to be sold. . . . I will not be bartered, traded or sold." *Id.* These phrases play on current Web site industry jargon, in which customer visits are referred to as "capturing eyeballs," and personal data is amassed into "consumer profiles." The import of the advertisement is that typical Web sites currently treat people not as individuals, but instead as "inventory" that can be barcoded 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 Web site industry: "I am an individual and you will respect my privacy." *Id.* The final claim is that "On the Net I am in control." *Id.* By demanding her moral rights when it comes to online privacy, the woman in the ad admonishes the reader to do the same.

59. Some relevant factors include the extent to which the use of personal data plays a central role in the business model of a particular Web site and the site's relative cost structure for collecting, storing, processing, and manipulating data. 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. *Amazon Draws Fire for DVD Pricing Test, Privacy Policy Change*, WALL ST. J., Sept. 14, 2000, at B4. 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 Ac-*

more demanding of privacy will be more likely to provide greater privacy protections.[60]

Despite the increase in demand for respect, there is great controversy as to whether there has been an increase in the respect of privacy. The industry claims to be responsive to consumer concern for privacy.[61] Many privacy advocates, however, strongly disagree. Jessica Litman has stated that industry attempts at self-regulation have been an "abject failure."[62] Similarly, Jason Catlett of Junkbusters, a privacy advocacy organization, has remarked that, "'[t]he stated policies of most big shopping sites run the gamut from bad to atrocious.'"[63] However, not all commentators sympathetic to consumer privacy concerns are this critical. In the same symposium in which Litman made her remarks, Pamela Samuelson noted that privacy policies are improving.[64]

The following discussion examines the data-regarding norms that have been adopted by Web sites in their privacy policies. Next, I will critically evaluate these efforts by Web sites in order to better judge the merit of the critic's charges of duplicity. Following this discussion, Part Three will examine whether Posner's theory lends insight into this response on the part of Web sites.

1. The Features and Content of Current Web Site Privacy Policies

Web site privacy policies are a recent phenomenon, having

---

quisition, WALL ST. J., Apr. 3, 2001, at B7.

60. For example, health-related sites and financial sites appear to provide higher levels of privacy. This appears to be responsive to consumer demand. *See* Stephanie Olsen & 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 (reporting that Rep. Michael Doyle, D-Penn., "said consumers seemed more concerned with financial and medical privacy than with other types").

61. *See* Sandeep Junnarkar, *FTC Faces Suit for Access to Privacy Complaints*, CNET NEWS.COM (Oct. 12, 1999), *at* http://news.com.com/news/2100-1001-231268.html. "A large part of the privacy debate in the last couple of years has centered around industry claims that there are adequate systems in place to deal with privacy problems." *Id.* (quoting David Sobel, General Counsel of the Electronic Privacy Information Center ("EPIC")).

62. Litman, *supra* note 27, at 1287.

63. Stefanie Olsen, *Top Web Sites Compromise Consumer Privacy*, CNET NEWS.COM (Dec. 17, 1999), *at* http://news.cnet.com/news/2100-1017-234631.html.

64. Samuelson, *supra* note 34, at 1161. "[T]here is some evidence that American-based commercial 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 . . . ." *Id.*

emerged in the late 1990s. The universal feature of these privacy policies is that they are accessible as a link from the home page of many Web sites. Many sites also have links to their 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 friendly, reassuring tone that seems motivated by an attempt to create an air of intimacy between the site and its users. On the other hand, privacy policies increasingly are adopting a legalistic tone.

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, "[a]t 1-800-FLOWERS.COM, we recognize and respect the importance of maintaining the privacy of our customers and members . . . ."[65] Some of the more scrupulous sites explicitly acknowledge the privacy rights of users in their opening remarks. Wal-Mart's privacy policy states, "[w]e 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."[66] Nike's privacy policy begins, "Nike is committed to respecting the privacy rights of Web site visitors."[67]

Some sites state that their goal is to create a relationship of confidence and trust with consumers. The Walt Disney privacy policy begins, "[t]he 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."[68] The introduction to the Wal-Mart

65. About 1-800-FLOWERS.COM: Your Privacy, *at* http://www.1800flowers.com/flowers/security/index.asp (last visited Apr. 4, 2002).

66. Walmart.com Privacy Policy, *at* http://www.walmart.com/cservice/ca_sp_privacypolicy.gsp (last visited Apr. 4, 2002). 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.

67. Nike's Online Privacy Policy, *at* http://niketown.nike.com/info/privacy.jhtml?item=privacy (last visited Apr. 4, 2002).

68. Disney Online Privacy Policy, *at* http://disney.go.com/legal/privacy_policy.html (last visited Apr. 4, 2002).

privacy policy states that "[t]he security of your personal information is very important to us. . . . 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 [Privacy] Policy."[69] Sears.com states, "[w]e 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."[70]

On the whole, however, privacy policies are increasingly employing more overtly legalistic formulations.[71] 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."[72] The Toyota privacy policy in part reads, "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."[73] Toyota's harsh legalistic tone illustrates the tension between a privacy policy crafted as a document meant to create trust in users, and as a legalistic 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.[74] If privacy-related lawsuits become more prevalent, the language of privacy policies may become even more legalistic.[75]

---

69. Walmart.com Privacy Policy, *supra* note 66.

70. Sears, Roebuck and Co. World Wide Web Site Customer Information Privacy Policy, *at* http://www.sears.com (last visited Apr. 4, 2002).

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

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

73. Toyota.com Privacy Policy, *at* http://www.toyota.com/html/privacy/index.html (last visited Apr. 4, 2002). The Privacy Policy also states that "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." *Id.*

74. *See, e.g.*, Judnick v. DoubleClick, No. JC-4120 (Marin Cty. (Cal.) Super. Ct., filed May 5, 2000).

75. 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

In the past few years, most Web sites have begun to address privacy concerns to some extent.[76] Web sites are beginning to adopt a number of common practices. These practices track the norms that are being promoted by the privacy proselytizers discussed in the previous section. The following brief survey of the key elements of a number of Web site privacy policies indicates just how complex and varied the personal data practices of Web sites are becoming.[77] It will be necessary to examine these practices in some detail to better understand the extent to which such practices are susceptible to, or indeed constituted of, false signaling actions, as Posner's theory may suggest.[78]

The provision of notice of a site's personal-data-related activities is the first of the fair practice principles.[79] The principle of notice is a second-order principle that supports each of the other principles, as it is only when a user has knowledge of the data-related activities of a Web site 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 seems 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 privacy policy, when printed out, is only half a page long and contains three short paragraphs.[80] The site is able to state straightforwardly, "[w]e do not sell, rent or trade your personal information with

---

contractual). *But see, e.g.*, Weather.com Privacy Statement, *supra* note 72 ("This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights.").

76. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A FEDERAL TRADE COMMISSION REPORT TO CONGRESS 10 (2000) [hereinafter FTC 2000 PRIVACY REPORT] (discussing that the Commission's survey findings demonstrate continued improvement with eighty-eight percent of Web sites in the random sample posting at least one privacy disclosure), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Apr. 4, 2002).

77. *See* FTC 1998 PRIVACY REPORT, *supra* note 27.

78. Previous studies of privacy policies have provided quantitative measures of changing Web site practices. *See* FTC 2000 PRIVACY REPORT, *supra* note 78; *see also* The Georgetown Internet Privacy Policy Study, *available at* http://msb.edu/faculty/culnanm/gipps home.html (last modified Aug. 11, 2000). While of general interest, these studies do not lend insight as to whether these changes represent true or feigned respect for privacy.

79. FTC 1998 PRIVACY REPORT, *supra* note 27, at 7.

80. Madonna Fan Club Privacy Statement, *at* http://www.madonnafanclub.com/privacy.html (last modified Mar. 11, 2002).

others."[81] This site claims it only uses personal data in order to process commercial transactions, such as merchandise sales and membership dues. The site also claims not to use cookies or other passive means of data gathering.[82]

The problem is that the data-related practices of Web sites are becoming increasingly complex, and this makes notice a more difficult matter. The first layer of complexity is introduced by means of the manner in which data is collected. Users understand that data is being collected from them when the data is explicitly provided by them. More opaque is data collection by means of cookies and other ways of so-called "passive" tracking of user online activities.[83]

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 Web site such as their name, address, social security number, age, etc., is personally identifiable in the sense that it can be traced back to particular individuals. By contrast, Web sites 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.[84] In

---

81. *See id.*

82. *See id.*

83. Many sites provide definitions of arcane terms such as "cookies" and "IPO addresses," and explanations of their importance for privacy purposes. Motorola's Web site, for example, states as follows:

> 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's 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.

Motorola.com Privacy Practices, *at* http://www.motorola.com/content/0,1037,3,00.html (last visited Apr. 4, 2002). Hallmark's site provides another example:

> 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.

Hallmark.com Privacy Policy, *at* http://www.hallmark.com (last visited Apr. 4, 2002).

84. The Kinko's Security and 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 identi-

other words, although sites keep records of cookie-generated information, they claim not to keep track of which 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.[85] Privacy policies refer to these entities as "trustworthy third parties"[86] or "reputable third-parties,"[87] 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.

The second of the privacy norms is choice/consent.[88] The intuitive idea is that users should have some say when it comes to the use of their personal information by Web sites. The FTC has interpreted the norm of choice so as to include making a choice among a number of alternatives.[89] Some sites, however, treat choice in the narrowest sense so as to mean simple consent or assent. Toyota writes, "[b]y 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."[90] Under the heading of "[y]our

---

fiable 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/global_assets/docs/privacy.php (last visited Apr. 4, 2002).

85. *See* Jason Gonzalez, *Better Business Bureau Gives Nod to Lowe's*, NAT'L 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.").

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

87. *See* Nokia.com Privacy Policy, *at* http://www.nokia.com/privacy.html (last updated Jan. 2, 2002).

88. *See* FTC 1998 REPORT TO CONGRESS, *supra* note 27, at 8.

89. *See id.* at 8–9.

90. Toyota.com Privacy Policy, *supra* note 73.

Consent" on its site, Nike simply states, "[b]y using our Web site, you consent to our privacy policy."[91]

Many sites, however, offer users choices other than the option of leaving. The most common choice made available to users is whether they want to have the site store and use their personal data. Many sites give the user the option of removing their personal data from the site. For example, Kinkos.com states, "[y]ou can easily change any of the information you have been asked to provide by Kinko's. You can also permanently remove your information from the Kinko's database."[92]

As already mentioned, Web sites offer two types of consent that are commonly referred to as opt-in and opt-out.[93] With opt-out, the user must take some positive step in order to stop what would otherwise be a default process whereby his or her data would be available for use by the Web site.[94] 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 that the consumer supply data. Thus, opting out of the provision entails opting out of receiving some or all of the site's services.[95] 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.[96] Until recently, it has been uncommon for Web sites 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. In particular, sites that deal with more sensitive data are beginning to offer users the choice to opt-in for this data.[97]

---

91. Nike's Online Privacy Policy, *supra* note 67.

92. Kinko's Security and Privacy Policy, *supra* note 84.

93. *See supra* notes 40–42 and accompanying text.

94. *See supra* note 42.

95. *See* Motorola.com Privacy Practices, *supra* note 83.

> 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 the placement of cookies.

Id.

96. *See* J.Crew.com Privacy, *at* http://www.jcrew.com/help.sniplets/privacynew.jhtml (last modified Nov. 20, 2000) (permitting customers to refuse cookies and to decline receiving promotional emails and catalogs without limiting the customer's shopping experience).

97. *See* Paul Davidson, *Capitol Hill Support Brews for Internet Privacy Laws*, USA

The third privacy norm prescribes that Web sites provide users with access to their personal data stored with the Web site.[98] 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's Web site states, "[i]f 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 address and password) so that only you can access your profile."[99] Despite opportunities for access, fewer sites offer the ability to contest data. One site that does is Nokia.com, which states that "Nokia will on its own initiative, or at your request, replenish, rectify or erase any incomplete, inaccurate or outdated personal data."[100]

A solid minority of sites now address the issue of security in their privacy policies.[101] Many sites employ Secure Socket Layer ("SSL") technology to protect the security of credit card information as it is transmitted to the site.[102] With SSL, the Web site's server scrambles the data as it travels from the user's computer to the Web site. 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 Web site security have involved hackers gaining access to databases.[103] Increasingly, Web

---

TODAY, July 12, 2001, at 3B (arguing that there is consensus building for requiring opt-in for more sensitive data, such as financial and medical).

98. *See* FTC 1998 PRIVACY REPORT, *supra* note 27, at 9.

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

100. *See* Nokia.com Privacy Policy, *supra* note 87.

101. FTC 1998 PRIVACY REPORT, *supra* note 27, at 10.

102. *See* Motorola.com Privacy Practices, *supra* note 83.

> Motorola uses 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 ensure 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.

Id.

103. 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

sites are addressing the issue of the security of data stored by the site. Some sites are limiting the number of employees with access to personally identifiable data, as well as employing security systems to protect the data from external intruders.[104]

The fifth privacy norm is that of enforcement/redress.[105] 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 Web site's failure to provide protective practices.[106] Web sites have done very little to promote this norm.[107]

2. Critique of Web Site Privacy Policies

As the previous discussion indicated, Web sites have been active to one degree or another in the past few years in implementing various sorts of privacy practices. These activities have emerged in response to increased demands of consumers and various privacy advocates. Although these practices regard privacy, it is debatable whether they actually respect or enhance privacy. The practices have been subject to harsh criticism from privacy advocates, who have in general claimed that the level of

---

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*, TIME, Jan. 24, 2000, at 56.

104. For example, MTV's Web site, MTV.com, states, "[w]e 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 (last updated Aug. 9, 2001) ("To ensure 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."). *See also* Barnes & Noble.com Privacy Policy, *supra* note 86; Microsoft.com Statement of Privacy, *supra* note 99 ("[D]ata is stored in password-controlled servers with limited access.").

105. FTC 1998 PRIVACY REPORT, *supra* note 27, at 10–11.

106. *Id.*

107. For a token effort, Barnes & Noble.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.

Barnes & Noble.com Privacy Policy, *supra* note 86.

protection provided by Web sites is far too low to provide adequate respect for consumer data privacy rights.[108]

In addition to expressing dissatisfaction with the general level of protection, privacy advocates have sharply attacked Web sites for acting in a duplicitous fashion by seeking to create a false impression in consumers.[109] 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.[110] Readers are naturally led to believe they are getting greater protection than they in fact are.

This criticism of emerging Web site privacy norms is typically painted with a broad brush, dismissing in its entirety efforts by Web sites to provide respect for privacy. If these critics are right in the categorical dismissal of the efforts of Web sites, a puzzle arises when this dismissal is considered in light of the above discussion. 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. A discussion of the various aspects of privacy policies that highlight their most troubling features follows.

---

108. *See, e.g.*, Mark E. Budnitz, *Consumer Privacy in Electronic Commerce: As the Millenium Approached, Minnesota Attacked, Regulators Refrained, and Congress Compromised*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 821, 823 (2000).

109. *Id.* at 824–25.

110. *See, e.g.*, Patrick Thibodeau, *FTC Official Faults Corporate Privacy Policies*, COMPUTERWORLD, May 7, 2001, at 12 ("Many corporate privacy policies are too hard to find, too long and too confusing . . . .") (paraphrasing U.S. Federal Trade Commissioner Sheila Anthony).

As noted earlier, the one principle that is most often addressed by Web sites is notice, so discussion may usefully begin here.[111] All privacy policies, to one degree or another, describe the Web site's data practices, but when do such descriptions constitute adequate notice? The better Web sites make statements telling the user that the notice provided by the Web site is exhaustive of the uses to which the consumer's data will be put. The Walmart.com policy states, "[w]e 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."[112] On the other hand, more lax Web sites merely note, at most, that they will make an effort to inform users of the sites' collection and usage practices. For instance, MTV.com says it makes "good faith efforts to make it clear why the information is being collected and what it will be used for."[113] In the event of litigation against MTV, the firm will always be able to assert that it made a good faith effort given the circumstances. Wal-Mart's promise is more concrete; it either is, or is not, the case that the user's data is used by the Web site in a manner set forth in the policy.[114]

Even for Web sites such as Walmart.com that 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 due more to unfamiliar terminology and processes than to complex legal constructions, although, as noted above, privacy policies are becoming more legalistic as well.

---

111. *See supra* notes 37–42 and accompanying text.

112. Walmart.com Privacy Policy, *supra* note 66; *see also* Intel.com Privacy Policy, *at* http://www.intel.com/sites/corporate/privacy.htm (last visited Mar. 21, 2002) (stating that "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 99 ("For material changes to this statement, Microsoft.com will notify you by placing prominent notice on the Web site.").

113. *See* MTV.com Terms of Use and Privacy Policy, *supra* note 104.

114. *See* Walmart.com Privacy Policy, *supra* note 66.

There is no neat solution to this difficulty, which is inherent in giving notice to ordinary people of complex activities with significant legal implications. Even Web sites making their best effort will need to make difficult judgment 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.[115]

Many Web sites appear not to make a best effort, however, or anything close to it. For example, many Web sites state that they reserve the right to change their data practices without prior notice.[116] These Web sites 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.[117] The obvious problem with this suggestion is that in the time between when the user checks the policy and the time of the policy change, she will be misinformed as to the Web site's practices. In addition, this practice creates an incentive for Web sites to promise respectful treatment to users in order to lure them in, only to then change practices in midstream.[118]

The deepest fear for consumers involves the use of their data by unknown third parties using their data in unknown ways.[119] People expect that their data will be used only for the purpose for which it is collected. By the lights of ordinary moral logic, this would imply that Web sites have a duty to adequately inform users of external uses of their data. It is thus here that Web sites have their greatest opportunity to either display respect or not. However, it is in this area that Web sites are perhaps most guilty

---

115. *See* Thibodeau, *supra* note 110, at 12 (describing how Citibank is dealing with this problem by offering two versions of its privacy policy, the technical one and the short form).

116. *See, e.g.*, MTV.com Terms of Use and Privacy Policy, *supra* note 104.

117. *Id.*

118. 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." Kinko's Security & Privacy Policy, *supra* note 84. But the Web site also states that "Kinko's reserves the right, at its sole discretion, to make modifications, alterations or updates to this Privacy Policy at any time." *Id.* In other words, Kinko's 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*, 2 E-BUS. L. BULL. (Andrews Publ'ns, Inc.) No. 5, at 12 (Mar. 2001).

119. *See* Gonzalez, *supra* note 85, at 7.

of providing inadequate notice. Web sites commonly note that they will deal with third parties in order to promote the interests of users.[120] This vague fiduciary language is likely to be misleading, however. The warm and fuzzy labels and phrases used by Web sites to describe their relationships with unnamed third parties deceptively hide the fact that most Web sites 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 Web sites restrict their activities with third parties to only those that promote their users' interests.[121] Some of the better Web sites are beginning to provide more detailed explanations of their dealings with third parties.[122]

The second privacy norm is choice and consent. This principle is connected to the first principle of notice in that when 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 Web site demonstrates a reasonable degree of respect with regard to the provision of notice, the Web site cannot demonstrate a reasonable degree of respect with regard to the principle of choice/consent.

---

120. *See, e.g.*, Amazon.com Privacy Notice, *at* http://www.amazon.com (last visited Mar. 21, 2002).

121. 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 disclaiming information from its bridal registry to its business partners. *See* Electronic Frontier Foundation, *Electronic Frontier Foundation Action Alert: Contact Macy's Now! Tell Them to Respect Your Privacy* (June 5, 2001), *at* http://www.eff.org/Privacy/Marketing/20010612_eff_macys_alert.html. Toysmart.com explicitly promised not to sell data: "[p]ersonal information voluntarily submitted by visitors . . . is never shared with a third party." Toysmart.com Privacy Statement, *at* http://www.ftc.gov/os/2000/07/toyexh1.pdf (last visited Mar. 21, 2002). In bankruptcy, Toysmart then attempted to sell this data. *See 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; Press Release, 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. 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 generally* 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.

122. Wal-Mart, for example, describes its dealings with Coremetrics and other third parties. *See* Walmart.com Privacy Policy, *supra* note 66. Once users possess these fuller descriptions, they will be in a position to decide for themselves whether the data transfers are for their benefit.

As discussed previously, the crucial issue regarding the principle of choice/consent is between opt-in and opt-out.[123] 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 Web site, but merely that they have not read the privacy policy. Thus, it can be argued that if Web sites were truly respectful, they would not collect and use consumer data unless they had actual consent.

Web sites 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 Web sites. Thus, opt-in would create an artificially high burden on all those users who prefer receiving the benefits that various Web sites have to offer but who do not bother to read privacy policies. In an article discussing junk mail, Richard Posner argued that opt-out was more efficient than opt-in.[124] Similarly, the Web site industry might argue that it is actually doing consumers a favor to have opt-out instead of opt-in because the former policy will promote efficiency.

Some sites arguably frustrate true consent by making choices more difficult than they need be. For example, 1-800-FLOWERS.COM states, "[i]f 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]."[125] Note that the Web site 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 privacy norm is that users should both have access to their data and the ability to remove incorrect data. As discussed earlier, a growing number of Web sites are allowing users some

123. Many Web sites' privacy policies are drafted in such a manner, either intentionally or negligently, that the reader cannot discern if the operative practice is opt-in or opt-out. For example, Hallmark.com states: "[w]e do not currently share your 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 83. It is not clear, however, whether "prior approval" means prior explicit approval or merely the failure to opt-out when notice is provided.

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

125. About 1-800-FLOWERS.COM: Your Privacy, *supra* note 65.

version of these features.[126] What these Web sites do not typically explain, however, is that this access is usually only to so-called personally identifiable data—data explicitly gathered from the user. This means that the clickstream data collected about the user by means of cookies is not available to the consumer to access or remove. A Web site might say in its own defense that clickstream data is not personally identifiable, and consequently 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 Web site that collects the data or from some other Web site that gains possession of such data.[127] Thus, while the clickstream data is not currently personally identifiable, it may be in the future. Respectful Web sites might therefore provide access to clickstream data not to mention notice of the potential combination of so-called anonymous data with user's personal identity.

The fourth privacy norm is security. As noted earlier, some Web sites provide SSL protection for personal data while in transit to the Web site.[128] Other Web sites provide some protection for the data while in storage at the Web site, such as by encrypting the data or restricting employee access to the data.[129] While these protections are beneficial, most Web sites do not address the main threat to the security of user data: the loss of control over the data due to voluntary alienation 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.[130] It is as if Web sites padlock the backdoor to keep the illegal hackers out but leave the front door wide open for any third party with the means

126. *See* discussion *supra* notes 37–42 and accompanying text.

127. *See DoubleClick Faces Mich. Atty. Gen. Probe and Numerous Privacy Suits*, COMPUTER & ONLINE INDUS. LITIG. REP., Mar. 7, 2000, at 7. For instance, 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. *Id.* 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. *Id.*

128. *See supra* text accompanying note 102.

129. *See, e.g.*, Microsoft.com Statement of Privacy, *supra* note 99.

130. *See, e.g.*, Kinko's Security and Privacy Policy, *supra* note 84 ("Some of Kinko's strategic partners, such as those with links on our Web site, 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.").

to walk in, conduct a transaction, and leave with the data in hand.

In sum, the above examination demonstrates that thus far Web sites have talked the talk of data privacy but have not adequately walked the walk. With this detailed look at Web site privacy norms in mind, it is now possible to fully consider whether Posner's theory provides the best explanation for norms emergence.

III. SIGNALING VERSUS COOPERATION ACCOUNTS OF WEB SITE PRIVACY NORMS

The relative dearth of substantive privacy protections provided by the Web site industry raises the question of why the increased demand for privacy has not resulted in a more robust supply of privacy protections on the part of Web sites. 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 proselytizers, consumer demand has simply not been sufficient to drive Web sites 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 Web sites. If there is so little demand for online privacy, why go to the bother of attempting to create the impression that a Web site is committed to respect user privacy? Why not just avoid dealing with the topic altogether, as any firm must do with a myriad of issues that have a marginal impact on its business? Thus, a more satisfactory explanation of the Web site industry response must explain why Web sites bother to respond in a deceptive manner.

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.[131] A party wishing to communicate a proposition through signaling, rather than merely asserting the proposition, will use words or deeds calculated to elicit the inference that the proposition is true.[132]

131. *See generally* DOUGLAS G. BAIRD, ROBERT H. GERTNER, & RANDAL C. PICKER, GAME THEORY AND THE LAW 123–24 (1994).

132. *See id.* at 123 ("Signaling takes place when those who possess nonverifiable infor-

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.[133] 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."[134]

Perhaps the reason that the words and deeds of many Web sites appear to be motivated by the desire to deceive, rather than to provide respect, is that Web sites are motivated by the desire to falsely signal privacy rather than provide it. The first section below will apply Posner's general signaling account to Web site data norms. The next section will critique this account.

A. *Signaling Theory Applied to Privacy Norms*

A possible explanation of the apparently deceptive actions of Web sites is suggested by Posner's signaling theory of norms.[135] Recall that for Posner, a norm is simply a pattern of behavior comprising individual signaling behaviors of actors seeking to signal that they are good types.[136] On this account, emerging Web site privacy norms are best explained as attempts to signal to users that the participating Web sites are good types. Web sites that are 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.

The relevant norms are the patterns of behavior whereby Web sites are addressing user privacy concerns by offering privacy policies with varying elements of notice, choice, access, security, and enforcement. Good types desire a situation in which they are able to establish a separating equilibrium and serve as the only participant in these practices. However, the situation appears to

---

mation can convey that information in the way they choose their actions.").

133. *Id.* at 124.

134. *Id.*

135. *See* POSNER, *supra* note 1, at 18–22.

136. *Id.* at 19.

vary depending on the particular norm. For the norm of providing notice of data-related practices, it appears that instead of a separating equilibrium, there exists a pooling equilibrium in which most Web sites follow this norm or are inclined to do so in the future.[137] Web site behavior appears to be moving in this direction 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 or is quickly forming for these two norms. Consequently, the good types are not able to distinguish themselves from the bad types by means of the signals created by participating in these norms.[138]

Note, however, that for the norms of opt-in, security measures, and access, it does appear that separating equilibria have formed, whereby some Web sites conform to these norms while other Web sites do not. 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. Web sites that conform to more demanding norms display a willingness to expend costs in signaling at a level that is apparently not sustainable by most Web sites. 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

137. A separating equilibrium previously existed. According to the FTC's 1998 study, only fourteen percent of Web sites disclosed their information practices. *See* FTC 1998 PRIVACY REPORT, *supra* note 27, at 27. However, in 1999 the Georgetown Internet Privacy Policy Survey Report indicated that sixty-one percent of Web sites posted at least one disclosure about their information practices. *See* FTC 2000 PRIVACY REPORT, *supra* note 76, at 10. The 2000 FTC Report indicated that eighty-eight percent of the surveyed sites posted at least one disclosure about their information practices. *See id.*

138. 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 Web site 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. *See* ELLICKSON, *supra* note 3, at 65–81; *see also* POSNER, *supra* note 1, at 173. Implicit in this example is the fact that one party's cooperation is verifiable by the other party. ELLICKSON, *supra* note 3, at 65–81. 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. *Id.* 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.

Web site forgoes the opportunity to gain access to data for free. The costs are more direct for providing access and ability to contest data.[139] Similarly, the costs of security measures also are direct and come from the cost of supplying the security.[140]

Thus, some Web sites conform to norms that cost them significantly. Posner's account provides a possible explanation as to why these sites have shown an interest in providing more costly forms of regard for consumer data. The motivation is to signal that they are good types in a manner that is not easily duplicated by bad types, thereby enabling the good types to establish a separating equilibrium for 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 Web sites to the heightened concern for consumer online privacy. There appears to be an important difference between norms as characterized in Posner's model and the norms that arise in the context of Web site privacy-regarding activities.

Contrary to the suggestion of Posner's model, many Web sites are not best characterized as 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 a discount rate conducive to future cooperative acts, but as actually engaging in cooperative acts. Posner's model is, in effect, always looking ahead to a future of cooperation after the signaling is

---

139. "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.

140. *See* FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY, FINAL REPORT 19 (2000) ("Security—and the resulting protection for personal data—can be set at almost any level depending on the costs one is willing to incur, not only in dollars but in inconvenience for users and administrators of the system."), *available at* http://www.ftc.gov/acoas/papers/finalreport.htm (May 15, 2000); *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) (discussing the privacy protection required by the Health Improvement and Accountability Act, whereby the analysis of the costs of such protections can be applied to all Web sites). *See generally* Ellen Messmer, *FTC Hearings Spotlight 'Net Privacy,'* NETWORK WORLD, June 16, 1997, at 6.

complete. But in fact some Web sites 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.[141] Online privacy norms constitute an important example in which norms are not collections of actions intended to signal discount rates, but rather collections of actions intended either to provide respect to consumers in the hope of garnering their trust, or to simulate respect also in the hope of garnering consumer trust.

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

As already noted, Web sites are increasingly offering privacy protections to consumers despite the fact that they might legally refrain from doing so.[142] There are costs associated with offering privacy protections.[143] Thus, assuming Web sites to be rational, an explanation is necessary as to what benefit they hope to gain as an offset to this cost. One possibility is the signaling account explored above.[144] Another possibility is that Web sites are seeking to enter into repeat-play cooperative relationships with their customers that can be modeled as iterated prisoner's dilemmas.[145] This explanation would make sense of the genuinely sacrificial behavior of some Web sites; 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.[146] 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

---

141. 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 POSNER, *supra* note 1) ("I think it [is] fair to read Posner as offering signaling . . . as a general account of social norms.").

142. *See supra* Part II.B.

143. *See supra* notes 139–40.

144. *See supra* Part I.

145. Hetcher, *supra* note 30, at 921–24.

146. *Id.*

a cooperative strategy in which each defers the immediate gain from defection in order to realize long-term gains that may result from cooperation.[147]

This account faces a serious limitation, however, in that it may fail to explain the behavior of many and perhaps most Web sites. As discussed above, a prevalent complaint among privacy advocates about current Web site practices is that Web sites are not serious about privacy.[148] In terms of the potential cooperative bargain between users and Web sites whereby trust is exchanged for respect, this criticism can be recast in terms of seeing Web sites as trying to get something for nothing. They are seeking to obtain trust not by exchanging privacy protection, but through the illusion of privacy protection. If this charge is accurate, it suggests that something unusual is going on. In the usual model of cooperation, when a rational actor forgoes a short-term gain in the hopes of thereby securing a long-term gain, she really forgoes the short-term gain. The implication of the privacy activists critique, however, is that Web sites are often not forgoing the short-term gain.

One possible explanation is that these Web sites merely seek to pretend that they are interested in respecting user privacy. There may be good reason for a Web site 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 Web site, thinking that the Web site is cooperating with them. Thus, deception appears to be a highly desirable strategy; the Web site gains the benefits of being a cooperator without incurring the costs of being a cooperator.[149] Un-

147. This point was illustrated by Robert Axelrod's computer tournaments. *See* ROBERT AXELROD, THE EVOLUTION OF COOPERATION 7–15 (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 to defect in future rounds, cooperation may induce cooperation. *See id.* at 12. If the parties care enough about the future, the discounted benefit from mutual cooperation in future rounds may exceed the immediate benefit from defecting. *See id.* Cooperation is not the dominant strategy, however, because that strategy is easily exploited by strategies that always defect. *See id.* at 9. Even conditional cooperation like the tit-for-tat strategy that won the Axelrod tournament is not dominant. *See id.* at 13–14. 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. *See id.* at 12.

148. *See* text accompanying *supra* note 109.

149. As the old saying in moral theory goes, "[a]ll the advantages of theft over honest toil."

derstanding the actions of many Web sites, then, may require determining whether they are best understood as seeking to simulate respect in order to trick users into turning over their data.

Cooperation in a repeat game is a better description of what occurs with some Web sites, however, for sometimes they incur significant short-term costs in order to provide privacy protections. For example, when a Web site provides an opt-in policy, therefore guaranteeing that it will not transfer data to third parties, and then provides access and redress, or provides heightened security, the Web site incurs real costs. These costs are distinct from those that may be incurred by Web sites that are only interested 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. Web sites 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.[150]

For the reasons discussed in Part Two, consumers increasingly feel entitled to respect and will trust Web sites that demonstrate they are worthy of trust. Consumers may not view their relationship with Web sites as strategic until they perceive it as a moral relationship. But once consumers perceive Web sites as either respecting or disrespecting them, they will consequently trust or distrust them. The more strongly consumers feel about data privacy entitlement, the more they will be morally affronted by instances where Web sites disrespect their privacy. Accordingly, they will be slower to trust Web sites and will be more inclined to retaliate against those that fail to show respect.[151]

---

150. The notion of Web site visitors choosing to trust Web sites 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 have for its own sake, trust is not an item that Web sites would independently desire. *Id.* at 355–56. Rather, a Web site would prefer to gain the trust of its visitors because this trust will be positively correlated with these visitors choosing to interact with the Web site in the future. Robert Cooter's internalization account of norm conformity appears not to play a role as Web sites 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, 1694–95 (1996).

151. Retaliation may take a variety of forms, such as engaging in negative gossip or

The situation is strategic because Web sites are in a position to choose whether to respect the consumer in order to potentially engender consumer trust. Part of the Web site's choice whether to show respect depends in part on its calculation of how much its choice will cause the consumer to trust the Web site and how much the resultant cooperative opportunities are worth to the Web site.[152] The strategic structure of the situation is represented in Figure 1.

Figure 1: Web Site/Consumer Interaction

		Web Site	
		Privacy Norms	No Privacy Norms
Consumer	Trust	3, 3	1, 4
	No Trust	4, 1	2, 2

Each party has two choices that affect the utility of the other party.[153] Each party must consider how its choice and the choice

---

providing false or misleading information to the Web site. In this regard, one author notes the following:

> The obvious product of this distrust is that people avoid disclosing personal information by opting against online transactions and Web site 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 Web sites 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).

152. 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.

153. The numbers represent the ordinal preference rankings of the players, with "1"

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 Web site will consider whether it should attempt to foster consumer trust, and the consumer will consider whether it can influence the Web site's choice to provide privacy.

Because of these strategically interactive choices, a greater number of Web sites 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 Web sites—the larger and better-known ones—offered privacy policies.[154] This makes sense because these Web sites are most likely to have overlapping, multifaceted interactions with consumers; thus making it crucial for these Web sites to have respectful and trustworthy reputations. The number of Web sites that show respect for privacy has continued to grow as public consciousness of online privacy has grown.[155]

2. Mimicking Respectful Privacy Policies

Although Posner's signaling model may fail to account for the genuinely cooperative behavior taking place between some Web sites and their users, an alternative signaling model may be appropriate. As noted earlier, warranties are a standard example of a signal.[156] Privacy policies may serve a parallel role to warranties. In the privacy context, however, it is not necessarily, or typically, the case that one purchases a product from the Web site one visits. The privacy relationship between Web sites and users, then, is not inherently part of any transaction between these par-

---

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 for the column-player.

154. In the Federal Trade Commission's 1998 study, only fourteen percent of Web sites were addressing consumer privacy issues. FTC 1998 PRIVACY REPORT, *supra* note 27, 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 L.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).

155. *See* FTC 1998 PRIVACY REPORT, *supra* note 27, at 3–4, 28–29.

156. *See* BAIRD, GERTNER, & PICKER, *supra* note 131, at 124.

ties. By contrast, warranties are part of the transaction between buyer and seller. 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.[157]

As discussed above, signals are used in situations in which the potential signaler has nonverifiable information. The nonverifiable information that the Web site possesses and the user does not is the Web site's privacy disposition, in other words, the level of its commitment to respect consumer privacy, and its competence to fulfill this commitment. For example, 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.[158] This disposition is not readily knowable to the Web site's users, however. Accordingly, there is the possibility that the privacy policy may be used to signal that this Web site has good privacy dispositions.[159]

The reason warranties work as signals is because firms with high-quality products can provide warranties more cheaply than firms with low-quality products, as the high-quality products break down less often.[160] Is the same true for privacy policies? In other words, will Web sites with more respectful privacy dispositions be able to offer privacy policies more cheaply? The answer is yes. One can imagine two Web sites that each offer the same

157. *See* 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).

158. *See supra* note 66 and accompanying text. This is not to say that Wal-Mart's disposition is immutable. Walmart.com could be spun off, have a name change, and reemerge as a more aggressive data gatherer and user. While 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. *See generally* ROBERT H. FRANK, PASSIONS WITHIN REASON: THE STRATEGIC ROLE OF THE EMOTIONS (1988) (discussing topics such as signaling and cooperation and proposing that noble human tendencies may actually be evolved traits).

159. Some people claim to be indifferent to the use of their personal data by Web sites. 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 whether her data is used by Web sites might still rationally prefer to deal with a Web site that takes privacy seriously because such a site would be signaling that it is interested in long-term relationships generally.

160. *See supra* notes 133–34 and accompanying text.

fairly rigorous privacy policy. Imagine further that one of these Web sites—call it Wal-Mart—has more respectful privacy practices than another Web site—call it Toysmart. In these circumstances, Wal-Mart will be able to offer the privacy policy more cheaply than Toysmart. When Toysmart provides the promise of privacy protections, it must either take steps to live up to these promises or take the chance of being liable for failing to do so.[161] However, for Wal-Mart it is nearly costless to provide the privacy policy as it is already providing the promised protection pursuant to its cooperative relationship with consumers.

One might expect, then, that the Wal-Marts of cyberspace would offer privacy policies while the Toysmarts of cyberspace would not. However, this is not what has happened. Instead, privacy policies have become ubiquitous. The reason appears to be that the less respectful Web sites do not duplicate the signal with exactitude but rather mimic it with an inferior substitute, yet one that is not readily discernable as inferior by the typical user. As was seen in Part Two, many Web sites use deceptive language in their privacy policies to create an impression among 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 Web sites such as Wal-Mart's. This attempt by some Web sites 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.

CONCLUSION

The previous discussion has sought to test Eric Posner's theory of norm emergence. Though Posner does not implicitly say so, and as Richard McAdams does say, it is fair to read him as offering a general theory. As such, it should best explain the emergence of all norms, including cyberspace norms. The examination above indicates, however, that Web site privacy norms may not be best explained as collections of signals by Web sites regarding their discount rates. The privacy norms that have emerged are not col-

161. *See supra* note 121.

lections of arbitrary actions that must only create separating equilibria in order to work. Rather, the sets of actions are specifically targeted to either provide or to stimulate more respect for consumer data privacy. In the case of some of these norms—opt-in consent for example—the participating Web sites appear genuinely interested in entering into cooperative relationships with consumers and have succeeded in doing so. Other privacy norms are motley collections of genuine acts of cooperation on the one hand, and false promises of cooperation on the other hand. The fact that Posner's theory may not provide the best explanation of emerging Web site privacy norms means only that it may not be a general theory of norms. The theory nevertheless provides a convincing and original account of other norms and, hence, is an important contribution to the norms literature.