THE EMERGENCE OF WEBSITE PRIVACY NORMS

*Steven A. Hetcher**

Cite as: Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. TECH. L. REV. 97 (2001), *available at* http://www.mttlr.org/volseven/hetcher.html.

INTRODUCTION

There is a burgeoning privacy crisis due in large part to the explosive growth of the Internet.[1] In large measure, this crisis has emerged in

* Associate Professor of Law, Vanderbilt University School of Law. J.D., Yale University; M.A. (Public Policy), University of Chicago; Ph.D. (Philosophy), University of Illinois at Chicago; B.A., University of Wisconsin. Earlier portions of this Article were presented at a symposium entitled "Taking Stock: The Law and Economics of Intellectual Property Rights," at Vanderbilt Law School, at a symposium on the need for a federal privacy commission at the John Marshall Law School, and at a faculty workshop at Vanderbilt Law School. I wish to gratefully acknowledge the numerous helpful comments received on those occasions. In addition, Robert Rasmussen provided comments. I also wish to thank the members of my Spring 2000 Advanced Regulation of the Internet course at Vanderbilt Law School, where many of the ideas in the article were first explored. Finally, I am especially grateful for the research assistance of Robert Brewer, Mark Plotkin, Linda Potapova and Angela Vitale.

1. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter 1998 FTC REPORT TO CONGRESS] ("While American businesses have always collected some

a legal vacuum, as there is little positive law that directly regulates the private collection of personal data.[2] Because of this legal vacuum, informal social norms have the potential to play an especially important role in the regulation of data collection online.[3] This Article studies the emergence of website norms pertaining to data collection that have emerged in the past decade. In particular, the Article focuses on the manner in which the government has sought to regulate online privacy at a distance, purportedly out of respect for the established norm of Internet self-regulation.[4] This case study of the emergence of online norms

---

information from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns."). Emerging online technologies make the transmission of data virtually costless, which has contributed to a situation in which dramatically higher levels of personal data are now flowing across the Internet. Peter Huber and Mark P. Mills have estimated that it takes "about 1 pound of coal to create, package, store and move 2 megabytes of data." Peter W. Huber, *Dig More Coal—the PCs are Coming*, FORBES (May 31, 1999), *available at* http://www.forbes.com/forbes/99/0531/6311070a.htm.

2. *See also* Maureen S. Dorney, *Privacy and the Internet*, 19 HASTINGS COMM. & ENT. L.J. 635, 639 (1997) (explaining that because the Constitution primarily regulates government action, it does not prohibit private party collection and use of personal information).

3. *See* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 85–90 (1999) (distinguishing four principal regulators of human behavior in cyberspace: norms, law, technology, and the market); *see also* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1126 (2000) (endorsing Lessig's four-part approach to regulation in context of privacy).

4. The Federal Trade Commission has stated that "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology." *See* FEDERAL TRADE COMMISSION, SELF REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (July 1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf [hereinafter 1999 FTC REPORT TO CONGRESS]; *see* LESSIG, *supra* note 3, chap. 1 (lengthy discussion of dominant anti-regulatory outlook regarding governance of the Internet). Numerous commentators have taken the view that since the Internet is growing so rapidly and successfully, it is sensible to be cautious before adopting any significant regulatory measures that might curtail this development. *See, e.g.*, I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1054 (1994) (contending that rules of conduct in cyberspace should be governed by presumption of decentralization, using self-help, custom, and contract of cyberspace participants, and noting that because the Internet is changing so rapidly, the first answer to how a legal problem in cyberspace should be solved is to "do nothing"); Henry H. Perritt, Jr., *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413, 419–20 (1997) (contending that as a general rule "self-governance is desirable for electronic communities"). In addition, because the Internet is an inherently transnational phenomenon, it may be improper and overreaching for particular nations to attempt to exert too great an influence over its development. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); *see also* John Perry Barlow, *A Declaration of the Independence of Cyberspace* (visited Jan. 28, 2000), *available at* http://www.eff.org/~barlow/Declaration-Final.html; A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, in BORDERS IN CYBERSPACE 129 (Brian Kahin & Charles Nesson eds., 1997) (discussing the Internet's

is of interest in its own right. It is intended, as well, to be instructive regarding the possibilities for more effective regulation of online privacy, on a going forward basis.

The vast majority of commercial websites use their interactions with consumers as the occasion to collect personal data about these consumers.[5] The connection between the collection of personal data and personal privacy is straightforward; the more personal data that websites collect, store, and use, the less privacy that data subjects have. This reduction in privacy may be justified if the data subjects agree to exchange their personal information for something they prefer more.[6] Typically, however, personal data has been taken by websites without the subject's knowledge or consent.[7] Commercial websites behave in this morally dubious, but commercially reasonable manner for two reasons. First, personal data is not owned and hence it is not unlawful to collect it without consent, and second, in the emerging digital economy, personal data is becoming increasingly valuable.[8] Given these facts, it is no surprise that commercial websites collect and use as much personal

---

"resistance to control"); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 178–83 (1997) (noting the cyber-utopian argument that "the technology of the medium, the geographical distribution of its users, and the nature of its content all make the Internet specially resistant to state regulation").

5. There are two broad information categories of personal data: information that can be used to identify consumers, such as name, postal or e-mail address ("personal identifying information"); or demographic and preference information (such as age, gender, income level, hobbies, or interests) that can be used either in aggregate, non-identifying form for purposes such as market analysis, or in conjunction with personal identifying information to create detailed personal profiles. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 1, at 20. It is the first sort of threat that particularly raises privacy concerns, for the reason that once others have information about a person's identity, they may use the information in new ways that adversely affect the person.

6. *See* Samuelson, *supra* note 3, at 1128 (discussing utilitarian and autonomy-based rationales for regulation of data collection).

7. ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 3–4 (1994) ("A great deal of information we consider to be highly personal, and of interest to ourselves and the town gossip—our names, telephone numbers, marital status, educational accomplishments, job and credit histories, even medical, dental, and psychiatric records—is now being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. These transactions usually take place without our knowledge or consent.").

8. *See Online Privacy*, BUS. WEEK, Mar. 20, 2000, *available at* 2000 WL 7825258 (comparing the stockpiles of information to an Internet gold rush); Kathryn Kranhold & Michael Moss, *Companies Are Refusing to Share Their Cookies Tracking Devices' Consumer Data Is Too Precious*, CHICAGO TRIB., Apr. 10, 2000, *available at* 2000 WL 3654616 (discussing how large Fortune 500 companies are protecting online tracking devices from Internet advertising companies because consumer data is a veritable "gold mine"); Melissa Preddy, *Metro Teenagers Take Bait, Hook Prize on the Net—The Yield on Privacy in Bid for College Cash*, DETROIT NEWS, June 15, 2000, *available at* 2000 WL 348130 (stating "personal information is like gold," especially to "get paid to surf," profiling websites that entice Internet users to give up information about themselves for rewards).

data as possible, and at a growing rate.[9] Due to a torrent of media exposure, there is a growing public awareness of the data-collection norms of the website industry, and the ramifications of these norms for personal privacy.[10]

Public awareness of this erosion in privacy has precipitated public outrage. Opinion polls show increasing public concern with respect to online privacy.[11] This outrage sets the stage for rapid policy shifts by private industry and lawmakers alike. The United States Congress increasingly has shown an interest in enacting omnibus privacy legislation.[12] The Federal Trade Commission repeatedly has articulated an interest in regulating online data collection.[13] Although increased governmental regulation of online privacy likely will ensue, norms and customs will continue to play a significant role due to the continued strength of the norm favoring Internet self-regulation.[14]

Because of the importance of informal social and industry norms in regulating privacy in cyberspace, this topic presents a natural arena for the application of "law and norms" theory. Laws and norms theory is arguably the most important development in contemporary law and

---

9. *See* Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, THE COMPUTER LAW., May 1999, at 7–8 (noting that commercial activity involving personal data is growing rapidly).

10. *See, e.g.*, *The End of Privacy: The Surveillance Society*, ECONOMIST, May 1, 1999, at 21 (covering privacy degradation in online environment); Rep. Asa Hutchinson and Rep. Jim Moran, *Commission is First Step to Privacy*, ROLL CALL, July 10, 2000, *available at* http://www.rollcall.com; Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, *available at* 1999 WL 28466750; Jared Sandberg, *Identity Thieves Online*, NEWSWEEK, Sept. 20, 1999, *available at* 1999 WL 19354964; Celia Santander, *Web-Site Privacy Policies Aren't Created Equal*, WEB FINANCE, Dec. 11, 2000.

11. *See* Glenn R. Simpson, *E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise*, WALL ST. J., Jan. 6, 2000, at A24. A recent U.S. Business Week/Harris Poll found that 92 per cent of Internet users were uncomfortable about websites sharing personal information with other sites. *See Online Privacy*, *supra* note 8.

12. N.Y. TIMES, June 8, 2000, at A5 (strategists for major political parties analyze best means to capitalize on voter concern for online privacy). The lobbying muscle of the information industry suggests, however, that any such laws would stop short of providing a level of privacy deemed adequate by privacy advocates. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2000).

13. *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2043 (2000).

14. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter 2000 FTC REPORT TO CONGRESS] (recommending continued support of self-regulatory approach along with legislation); *see also* Rep. Billy Tauzin, *How Can Congress Protect Online Privacy? Self-Regulation is Key to Web Privacy*, ROLL CALL, Feb. 22, 1999, *available at* http://www.rollcall.com (confident that Internet was moving in right direction to make self-regulation a reality).

economics.[15] Analytic social norms theory entered the law with the publication in 1991 of Robert Ellickson's book, *Order Without Law*.[16] Based on empirical studies of ranching and farming communities in Northern California, Ellickson developed the hypothesis that efficient norms will emerge in "close-knit communities."[17] These norms will serve as solutions to the iterated "collective-action problems" faced by the group.[18]

With regard to Ellickson's hypothesis, the Internet may present an especially difficult context for the emergence of efficient norms, however, as online participants would appear to be anything but close-knit.[19] The apparent implication is that website privacy norms are inefficient as they are the product of communities that are not close-knit.[20] Thus, while these norms indeed are emerging rapidly, there is reason to conclude that they are not moving toward greater efficiency. The task at hand, then, is not only to examine how and why website privacy norms are emerging, but also to evaluate and hopefully improve their efficiency.

---

15. Judge Richard Posner views law and norms theory as second-generation law and economics. Richard A. Posner, *Social Norms, Social Meaning, and Economic Analysis of Law: A Comment*, 27 J. LEGAL STUD. 553 (1998). Ellickson views law and norms as representing a new paradigm within the traditional law and economic approach. Robert C. Ellickson, *Law and Economics Discovers Social Norms*, 27 J. LEGAL STUD. 537 (1998). Social norms theory has been the subject of a number of important recent symposia. *See* Symposium, *Law, Economics, and Norms*, 144 U. PA. L. REV. 1643 (1996); Symposium, *Law and Society & Law and Economics*, WIS. L. REV. 375 (1997); Symposium, *The Nature and Sources, Formal and Informal, of Law*, 82 CORNELL L. REV. 947 (1997). Symposium, VIRGINIA L. REV. (2000); *see also* Symposium, *The Informal Economy*, 103 YALE L. REV. 2119 (1994).

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

17. *Id.* at 137.

18. RUSSELL HARDIN, COLLECTIVE ACTION (1982).

19. *See* Reno v. ACLU, 521 U.S. 844, 851 (1997) (J. Stevens, dissenting) ("Taken together, these tools constitute a unique medium—known to its users as 'cyberspace'—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."); Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168–69 (S.D.N.Y. 1997) ("Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet."); Dan L. Burk, *Trademark Doctrines for Global Electronic Commerce*, 49 S.C. L. REV. 695, 716 (1998) ("Notwithstanding that the Internet is and will be segmented by economic, social, and technological divisions, those divisions will not necessarily map onto the geographic, political, and economic divisions already existing offline . . . the current technological structure of the Internet . . . ignores customary political and geographical boundaries on which much of our legal system is based.").

20. *See* Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1275 (1998) (author dubious of claim that Internet norms are efficient).

The concept of "privacy" is itself generally understood in rights-based terms.[21] In an online context, there is frequent discussion of the need for greater "respect" for privacy. Phrased simply, respect is a deontological concept. Despite the rhetorical focus on deontological concepts, the emergence of online privacy norms that has occurred over the last decade is equally well described as a move toward a more efficient regime of regulation of the flow of personal data. One of the goals of the following discussion will be to establish a "compatibility thesis" with regard to privacy and utility.[22] The crucial norms that have emerged in the website industry are both more efficient and more respectful of privacy.

The compatibility between efficiency and privacy has been possible because respect for data privacy has been cashed out in terms of autonomy. Respect for privacy does not require minimizing the amount of personal data that is collected and processed.[23] Rather, it requires that data collection and processing not violate the autonomy of the data subject. Data collection that is respectful of autonomy is accomplished through the mechanism of consent.[24] When data subjects consent to the use and collection of their data by websites, then the websites are collecting data in a manner that respects the autonomy of the data subjects. These exchanges of data for valuable consideration are also productive of social utility because through exchange each party is able to receive something it prefers more by trading away something it prefers less.

---

21. *See, e.g.*, Simon G. Davies, *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, in TECHNOLOGY & PRIVACY 143–45 (Philip E. Agre & Marc Rotenberg eds., 1997) (noting a change in society's approach from privacy protection to data protection); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497–498 (1998) (arguing that a citizen's right to participate in government depends "on the ability to control the disclosure of personal information"); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999) (claiming that the absence of privacy norms threatens democracy); *see also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 982–83 (1996) (arguing that digital copyright management technologies violate First Amendment Rights protecting speech and freedom of thought). The EU Directive is based on a conception of personal data protection as a fundamental civil liberty interest. Council Directive 95/46/EEC, art. 1.1, 1995 O.J. (L 281) 281 [hereinafter Privacy Directive].

22. Pamela Samuelson, *supra* note 3, at 1128 n. 18 ("It is therefore both unnecessary and counterproductive to choose between, e.g., the market-based and civil liberty-based visions of privacy.").

23. Minimization of data collection is sometimes stated as the goal of privacy regulation. *See, e.g.*, Litman, *supra* note 12.

24. *See* Samuelson, *supra* note 3, at 1156–58.

Part I of the Article will first look at the original privacy norms that emerged at the Web's inception in the early 1990s.[25] Two groups have been the main contributors to the emergence of these norms; the thousands of commercial websites on the early Web, on the one hand, and the millions of users of the early Web, on the other hand. The main structural feature of these norms was that websites benefitted through the largely unrestricted collection of personal data while consumers suffered injury due to the degradation of their personal privacy from this data collection. In other words, degradation of consumer privacy resulted as a third-party externality of free-market data-collection norms of the website industry.[26] Broadly speaking, then, these injuries occurred in a tort context as the injurers and victims were not in a bargaining relationship with regard to the injurer's procurement of the victim's personal data.[27]

Next, Part I will examine the strategic structure of the relationships between websites and consumers that allowed these highly exploitative norms to flourish. Analysis will indicate that consumers faced a large-scale collective action problem. There is a collective good that consumers potentially could have achieved, namely, the abatement of disrespectful data-collection practices by websites. Web users would have great difficulty in organizing to secure this collective good, however, due to their large numbers and lack of repeat play and overlapping relationships.[28]

Reacting to this sub-optimal but stable social situation, "norm entrepreneurs" entered the picture.[29] Three main types of norm entrepreneurs have been involved: public-interest advocates, website industry advocates, and governmental actors, particularly the Federal Trade Commission ("FTC"). Part II will examine how new, more

25. The Web is that portion of the Internet that runs HTTP, TCP/IP and utilizes uniform resource locators. TIM BERNERS-LEE, WEAVING THE WEB (1999).

26. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998). Yet another feature of the complex normative story behind the convergence of Internet privacy norms has to do with the recognition of entitlements in personal data. At the beginning of the period under study there was a divergence between the legal recognition of entitlements to personal data and the informal social norms that existed with respect to this data. Over the decade, the law has come to more closely represent the informal norms of entitlement.

27. The tortious relationship between the parties is itself expressed in deontological terms of unfair competition and breach of confidentiality. *See* Samuelson, *supra* note 3, at 1154–1157.

28. By the lights of standard game theory, large-scale collective action problems are the most difficult to solve. *See generally* HARDIN, *supra* note 18; ELLICKSON, *supra* note 16.

29. Norm entrepreneurs are actors who promote norms. Cass Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909 (1996).

respectful website privacy norms recently have begun to emerge, due largely to the efforts of these norm entrepreneurs.

The following study of the impact of norm entrepreneurs on website privacy norms will reveal a highly significant event. In the short history of the Internet, there has been a major shift—a "norm-cascade"—toward more respectful privacy norms.[30] The transition has been from a wild-west world in which websites did almost whatever they wanted with impunity, to a world in which a significant percentage of websites are explicitly addressing privacy concerns.

Part II models the norm cascade toward greater respect for online privacy in two stages. In the first stage, the privacy advocacy community and the website industry are described as battling to define the appropriate set of aspirational norms that should govern website/consumer interactions.[31] The privacy advocacy community began to form in the 1960s to fight against wide-scale personal data collection and aggregation by agencies of the U.S. government, newly armed with mainframe computers.[32] Norms of data privacy that emerged out of this process subsequently have been adapted to an online context by Internet rights advocacy groups. In response, the Website industry developed its own set of suggested online privacy norms, which it promotes as alternatives to those offered by the public-interest, advocacy community.

In the second stage of the emergence account, the FTC is described as first developing its own set of aspirational privacy norms, which it labels the "fair information practice principles." These principles represent a compromise between the demanding norms proposed by the advocacy community and the more permissive norms proposed by the website industry. While the FTC invokes the rhetoric of fairness, its proposed principles are best understood as promoting consensual data exchanges between websites and consumers.

Having specified its own set of aspirational norms, the FTC next sought to educate the public so that it would demand behavior on the part of websites consistent with these norms. The FTC then issued a threat to promote Congressional action in order to incentivize the website industry to bring its behavior in line with the FTC's norms.

---

30. *Id.*

31. An "aspirational norm" is the linguistic expression of a putative norm, that is, an expression regarding a practice that the speaker would like to see come into existence. Steven A. Hetcher, *Creating Safe Social Norms in a Dangerous World*, 73 S. CAL. L. REV. 1 (1999).

32. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306–08 (1989); PRISCILLA M. REGAN, LEGISLATING PRIVACY—TECHNOLOGY, SOCIAL VALUES AND PUBLIC POLICY 70 (1995); Interview by Mary Kathleen Flynn with John Berard, *Internet Privacy Issues*, CNNfn DIGITAL JAM (Feb. 5, 2000).

Initially, the FTC's threat was more effective on the larger and more established websites. Subsequently, however, these larger sites found it in their interest to themselves introduce threats to bring about compliance on the part of smaller sites. For example, large firms such as IBM and Disney have threatened to withdraw advertising from affiliated sites that fail to provide a minimal threshold of privacy protection.[33] The result of this network of threats by the FTC and large websites was the creation of a new equilibrium in which there was no longer a uniform norm of disrespect for privacy as existed in Stage One, but instead a bi-normative world in which numerous sites conformed to disrespectful practices while other sites conformed to more respectful practices. In this bi-normative world, an increasing number of sites provided "privacy policies" that could be linked to, from the site's home page.[34] Some sites, however, went farther by adopting privacy specialists within the firm. In fact, as growing numbers of *Fortune 500* companies are creating a new position in the executive suite: the Chief Privacy Officer.[35]

Taken together, the two stages described above produced a regime of data-gathering based to a greater extent on exchange relationships. Privacy policies put consumers on notice of the data practices of websites. This puts consumers in a position to choose whether or not to take part in the data exchange, depending on the conditions of the bargain. The current situation is far from ideal, however, as many websites have failed to adopt more respectful privacy practices. Worse yet, other firms have endorsed such practices in word but not in deed, by posting privacy policies on their sites but regularly violating the terms of these policies.[36] This may be worse than providing no privacy assurances at

33. *See infra* text accompanying notes 108–12.

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

35. An in-house lawyer representing Novell, speaking at the tenth annual Computers, Freedom & Privacy Conference, Toronto, April 4–7, 2000, remarked on the rapid rise of privacy specialists within large corporations such as hers. Universities have begun developing programs to train privacy specialists. *See SMU Teams with Privacy Council: Announces First Executive Chief Privacy Officer Training Program*, FINANCIAL NEWS, Jan. 29, 2001; *see also* David Bicknell, *Directors Face E-Laws Overload*, COMPUTER WEEKLY, Feb. 24, 2000, at 16 (the coordination of complying with European privacy policies has led some companies to be pro-active and engaging in "self-help" through privacy specialists).

36. For example, in bankruptcy proceedings, Toysmart.com recently moved to sell personal data it had collected pursuant to a specific privacy guarantee. *See Judge Is Urged to Reject Toysmart.com Settlement*, WALL ST. J., July 26, 2000, *available at* 2000 WL-WSJ 3037882; *Toysmart.com's Plan To Sell Customer Data Is Challenged by FTC*, WALL ST. J., July 11, 2000, *available at* 2000 WL-WSJ 3035966; *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, *available at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (July 21, 2000). While the FTC may settle,

all, as users are lulled by a false sense of security. Still other websites offer privacy policies that are so unclear in their meaning or complex in their provisions that there may be no practical sense in which consumers consent to these provisions. Nevertheless, on the whole, improvements in the moral quality of the interaction between consumers and websites have been made. Most important is the fact that overall an aspirational *grundnorm* of respect for website data privacy has begun to emerge in American culture generally. Only time will tell whether this *grundnorm* can become more adequately instantiated in actual online practices.

It is important that the policy community better understand the mechanics whereby more respectful website privacy norms have emerged. If better norms are already emerging through informal social processes and minimalist governmental guidance, there may not be a need for sweeping legislation of the sort currently being proposed by the FTC, as well as by many privacy advocates who suggest that the United States adopt the comprehensive European model of privacy regulation, despite its evident tension with sacred free speech principles.[37]

I. THE ORIGINAL WEBSITE PRIVACY NORMS

The first subpart below describes the original privacy-related norms that emerged in the unrestrained environment of the early Internet. The second subpart utilizes informal game theory in order to analyze these norms in terms of their strategic structures.

A. *Norms of Unrestrained Data Gathering*

The first message sent across the Internet occurred one month after the moon landing in late 1969.[38] In theory, from that moment onward, the Internet could have been used by one person to impermissibly gather personal data about another person. There is nothing in the historical record to suggest, however, that the invasion of data privacy was a problem in this early stage of the Internet's development. One reason

---

Toysmart still faces a lawsuit filed by TRUSTe, which contends that Toysmart is in violation of its online agreement not to sell consumer data to third parties. *See* Elinor Abreu, *TRUSTe to File Antiprivacy Brief Against Toysmart*, INDUSTRY STANDARD (June 30, 2000), *available at* http://www.thestandard.com/article/display/0,1151,16577,00.html; *see also* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1180 (1997).

37. *See* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTL. PROP. MEDIA & ENT. L.J. 97, 98 (2000); Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 665.

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

may be that, in this early period, the Internet was mainly used by academic researchers working in shared disciplines.[39] Such groups tend to have fairly small numbers and overlapping, multiple interactions. In Ellickson's terms, these were close-knit communities in which there would have been internal incentives to deter opportunistic behavior.[40]

It took the occurrence of two events in the 1990s in order to set in motion the series of developments that would lead to the current privacy crisis. The first was the invention of the World Wide Web in the early 1990s by Tim Berners-Lee.[41] Once the core features of the Web were in place, the Internet became dramatically easier to use, and a vast flowering of websites spurted up spontaneously and rapidly. These were not electronic-commerce sites, however, as the National Science Foundation did not then permit commercial use of the Internet.[42] The Web was not available for consumers until the Bush Administration zoned cyberspace for commercial use.[43] The commercialization of cyberspace is the second event that precipitated the privacy crisis, as commercial websites have been the main users of personal data collected under questionable circumstances.

Early commercial website norms facilitated data collection in two ways. First, many websites explicitly requested user information. Second, many websites collected data that was produced as a byproduct of website/consumer interactions, such as when consumers provided their credit card numbers or mailing addresses to sites. With the introduction of these online techniques of data-collection, the commodification of personal data entered a phase of rapid acceleration, as each of these initial means of data collection was soon improved upon by websites.[44]

---

39. *Id.* at Chapter Four.

40. Ellickson specifically mentions academic communities as often close-knit. ELLICKSON, *supra* note 16.

41. TIM BERNERS-LEE, WEAVING THE WEB (1999).

42. *See* Segaller, *supra* note 38, at 224–25.

43. *See id.* at 297.

44. *See generally* MARGARET JANE RADIN, CONTESTED COMMODITIES 15 (1996); Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1302 (1998). The term "commodification" is not inherently pejorative. Whether, and to what extent, the commodification of personal data is a negative development depends on one's normative theory. For utilitarian theories generally, and economic analysis in particular, "commodification," per se, has no *sui generis* moral meaning. The core idea of this type of moral theory is that all things of value may be put on a single scale. Thus, to commodify data, or anything else, is not to change its moral status. In fact, economic theorists may view commodification as an instrumental good, as commodifying data may promote efficiency by allowing this data to more easily reach the hands of those who will value it most. For some versions of deontological theory, on the other hand, personal data may not morally be made the subject of market exchanges. *See* Samuelson, *supra* note 3, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."). *See generally* Pamela S. Karlan, *Not*

Regarding explicit requests for data, websites soon began conditioning access to their sites, or to prized pages within their sites, on the provision by website visitors of some personal data. For example, one who wanted to receive the New York Times online had to fill out a detailed data questionnaire first. Alternatively, users might receive discounts, coupons, or free entry in contests as an inducement for the provision of information.

Regarding the collection of data without consumer notice, websites soon began to deploy sophisticated technological means of data gathering, such as cookies.[45] Cookie technology allows a website's server to place information about a consumer's visits to the site on the user's computer in a text file that only the website's server can read. In the early period especially, because cookies were planted secretly and subsequently operated seamlessly, Web users were typically unaware of the fact that data about them was being gathered.[46] In other words, there was no bargain between the parties; the data was simply spirited away.[47]

When using cookies, a Website assigns each consumer a unique identifier,[48] so that the consumer may be recognized in subsequent visits

---

By Money but By Virtue Won? Vote Trafficking and the Voting Rights System, 80 VA. L. REV. 1455 (1994) (explaining rationale for public policies against vote trafficking). This type of deontological theory, however, is not the type that is implicit in most discussions of online privacy. Most deontologically-oriented discussions of privacy implicitly accept the notion that under proper conditions, such as when there is informed consent, a data subject my morally alienate personal data in a market exchange.

45. Neil Randal, *How Cookies Work*, PC MAGAZINE ONLINE, *available at* http://www.zdnet.com/pcmag/

ventures/cookie/cksl.htm (last visited July 4, 2000). There is a shortage of social scientific information about cookie use. In its survey of Web sites, the FTC staff did not ascertain whether sites use cookies, or other hidden electronic means, to collect personal information, but looked instead to sites' information practice disclosures as a gauge of the extent of such practices. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 1, at 45 n. 4.

46. LESSIG, *supra* note 3, at 34–42 .

47. *See* Andrew L. Shapiro, *Privacy For Sale: Peddling Data on the Internet*, HUM. RTS., Winter, 1999, at 10.

48. Generally, a unique identifier is connected to the machine and not to a named individual. The problem is that this is a small gap to bridge. Consequently, privacy advocates have been concerned about unique identifiers even when connected to machines and not individuals. *See, e.g., Electronic Communications Privacy Policy Disclosures: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (1999) (statement of Mark Rotenberg, Executive Director, Electronic Privacy Information Center). Recently, both Intel and Microsoft have made efforts to tie numbers to names. *See* Edward C. Baig, *Privacy: The Internet Wants Your Personal Info. What's In It for You?*, BUS. WEEK, April 5, 1999, *available at* 1999 WL 8226796; Don Clark & Kara Swisher, *Microsoft to Alter Windows 98 So Data About Users Won't Be Sent to Company*, WALL ST. J., March 8, 1999, *available at* 1999 WL-WSJ 5443409; Robert Lemos, *The Biggest Computer Bugs of 1999!*, ZD INTERNET MAGAZINE, Dec. 23, 1999, *available at* 1999 WL 14538475 (discussing Intel's Pentium III serial number, global unique identifiers, and two Microsoft products, Office 97 and Windows 98, that attempted to match various

to the site.[49] In this manner, the site engages in "passive tracking" of the consumer.[50] On each return visit, the site can call up user-specific information, which typically will include the consumer's preferences or interests, as indicated by pages the consumer accessed in prior visits, items the consumer clicked on while at the site, or information downloaded.[51] Cookies make it easier for firms to engage in highly targeted marketing.[52] Cookie technology has proven to be extremely valuable to online companies because it not only enables merchants to target products and services that are increasingly tailored to consumer preferences but it also permits other companies to boost their revenues by selling more highly-valued advertising space on their web sites.[53] As Michael Froomkin says, cookies are the tip of the iceberg.[54] Once firms collect personal data, they may then aggregate it, or sell it to others who aggregate it, into databases containing profiles of named individuals. For example, a firm named Acxiom currently holds personal and financial information about nearly all U.S., U.K., and Australian consumers.[55] The personal-data norms of the early website industry are characterized in the following list.

Personal-Data Norms of the Early Website Industry

1. Websites may freely gather as much personal data as desirable from consumers.
2. Websites need not ask permission to gather personal data.

---

numbers to personal information and names); *see also In re* the Matter of Intel Pentium Processor Serial Number, Compl., Case No. 982 (Federal Trade Commission Feb. 26, 1999).

49. An industry has emerged to market a variety of software products designed to assist websites in collecting and analyzing visitor data and in providing targeted advertising. *See, e.g.*, Rivka Tadher, *Following the Patron Path,* ZD INTERNET MAGAZINE, Dec. 23, 1997, at 95; Thomas E. Weber, *Software Lets Marketers Target Web Ads*, WALL ST. J., Apr. 21, 1997, at B1.

50. "Passive tracking" refers to information collected by using navigational software. 1998 FTC REPORT TO CONGRESS, *supra* note 1, at 56.

51. *See id.* at 3, 45.

52. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1487 (2000).

53. FORESTER RESEARCH, INC., MEDIA & TECHNOLOGY STRATEGIES: MAKING USERS PAY 4–6 (1998).

54. Froomkin, *supra* note 52, at 1487 ("Cookies, however, are only the tip of the iceberg. Far more intrusive features can be integrated into browsers, into software downloaded from the Internet, and into viruses or Trojan horses. In the worst case, the software could be configured to record every keystroke."). A trojan horse is a "malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or . . . a program. . . ." FOLDOC, *Trojan Horse*, *available at* http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=+trojan+horse (last visited Mar. 25, 2001).

55. Froomkin, *supra* note 52, at 1473–74.

3. Websites need not inform consumers of their data-gathering practices.
4. Websites may use personal data in any manner they prefer, such as selling or licensing it to third parties.
5. Websites need not allow consumers access to their data.
6. Websites need not provide security for personal data in their possession.

The most striking feature of these early website personal-data norms is that they were completely geared toward serving the interests of the website industry. They reflect the fact that most websites felt neither legal nor social pressure to respect the data privacy of the visitors to their sites.[56] There was no legal pressure because there were no laws on the books that clearly prescribed the above practices and there was little social pressure because most people had little or no awareness that these practices were taking place.[57] In other words, these norms did not reflect any informal bargaining taking place between websites and consumers.

The fact that they emerged in a context in which there was a lack of bargaining is the most salient feature of the personal-data norms of the early website industry. Despite a lack of bargaining, there may be reason to think these norms were efficient. They are potentially justifiable from an economic perspective, as websites take something from the public domain that was under utilized, and put it to productive use. Like campers in a wooded area who collect fallen branches for use in their campfires, websites, on this view, are simply making use of a common resource that would otherwise be left lying in an unproductive state. After all, great quantities of personal data are produced as a by-product of other online activities. If not collected, this data would simply go unused. In fact, the economic argument in favor of shared use of personal information is stronger than it is for downed wood. Personal data is a "non-rival" good in the classic economic sense of the term; collection and use of personal data by one website does not diminish the amount available, either for other websites or for the data subject herself to

56. Mark A. Lemley, *supra* note 20, at 1276 ("[Non-consensual website interactions are] particularly likely when incentives are asymmetrically distributed in the community, as when buyers and sellers have their own conflicting norms. The norm that results from this conflict may represent a variety of things besides consensus: superior bargaining power on the prevailing side, collective action problems on the other side, or the use of strategic behavior.").

57. Ellickson emphasizes the important role that knowledge plays in the monitoring process that allows for successful solution of strategic problems. ELLICKSON, *supra* note 16.

use.[58] Because data is non-rival, arguably it should be left unregulated so that the greatest number of users will have free access to its use.

In this regard, note the important difference between personal data and creative expression of the sort protected by copyright law. Creative expression—original works of authorship—received legal protection, pursuant to Article I of the U.S. Constitution, in order to create incentives for authors to produce works.[59] Such an incentive is not necessary for the production of personal data, however, as it is produced as a by-product of living a life. Thus, there would appear to be a presumption in favor of treating personal data as a public good available to all.

There is an important disanalogy, however, between personal data and other shared goods such as fallen branches in a national forest. No one need suffer an injury when downed wood is burned, whereas data subjects often suffer significant harm when their personal information is used by others. Commentators have noted a wide variety of harms that may arise due to improper online data collection and use.

One type of harm is "identity theft." Identity theft occurs when one person intentionally assumes another person's online identity. Thus far,

---

58. Patrick Croskery, *Institutional Utilitarianism and Intellectual Property*, 68 CHI-KENT L. REV. 631, 632 (1993).

59. *See* U.S. CONST. art. I, § 8, cl. 8. In the landmark case, *Feist v. Rural Telephone Service*, the Supreme Court has said that facts are not subject to copyright protection. Rather, they must be left in the public domain—the intellectual commons—available for all to use. 499 U.S. 340 (1991). *Feist* involved facts of a particular sort, namely, personal data; the names and addresses of the residents of a particular region of Kansas, as contained in a regional telephone directory. *See id.* at 359–60. Lawyers are just beginning to grapple with special issues raised by the digital commons. *See* LESSIG, *supra* note 3; Steven Hetcher, *Climbing the Walls of Your Electronic Cage*, 98 MICH. L. REV. 801, 814 (2000). Law regarding personal data, indeed all data, is at sea. Some commentators have argued for heightened intellectual property status for personal data as a means to greater privacy protection. *See* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 78 (1996) (advocating statutory recognition of property rights in a "persona" consisting of personal information about the individual); Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92 (suggesting property rights in personal data as a way to protect privacy). There are First Amendment, however, tensions with this sort of proposal. For a discussion of the First Amendment and privacy, compare Paul M. Schawrtz, *Free Speech v. Privacy: Eugene Voloch's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000), with Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. LAW. REV. 1049 (2000). The tension between privacy and free speech can be avoided if data-subject control, as opposed to ownership, of personal data, can be protected. A trend leading in an opposite direction from heightened intellectual property protection is "copyleft," which argues that the Internet radically undermines ownership concepts for intellectual goods in the online world. *See* Ira v. Heffan, *Copyleft: Licensing Collaborative Work in the Digital Age*, 49 STAN. L. REV. 1487, 1491–92 (1997); *see also* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998) (arguing that personal data should be subject to open access rules).

identity thieves have typically gone on shopping sprees at the expense of their victims, but the possibilities for abuse through identity theft will grow as the functionality of the Internet expands.[60] Another type of harm that has received a good deal of attention is predation on children. Prior to recent legislation, children were especially vulnerable to questionable website practices.[61] A wide variety of detailed personal information has been collected online from children through various stratagems, such as encouraging a child to register for a contest, enroll in an electronic "pen pal" program, complete a survey, sign up for informational updates, or play a game.[62] Still other sites used "imaginary" characters to request information from children, or had them sign a "guest book."[63] Data-gathering norms of the early website industry, however, did not distinguish children from adults. All visitors were equally disrespected.

Alternatively, harms may result as the foreseen but unintended consequences of mundane business operations, such as when firms use private medical information of potential employees in making hiring decisions. For example, one-third of Fortune 500 companies use personal medical information in hiring, promotion, or termination decisions.[64] This has the significant policy consequence that may people are failing to seek medical diagnosis and treatment.[65]

---

60. *See, e.g.*, Jared Sandberg, *supra* note 10. Indicating the seriousness of the problem, the FTC has recently appointed a person to handle the issue. *See The Prepared Statement of the Federal Trade Commission on "Identity Theft": Hearing Before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary*, 105th Cong. (1998) (Statement of David Mendine, Ass'n Div. for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission). A recently passed Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a), imposes a penalty of fifteen years of imprisonment and fines for theft of personal information with intent to commit an unlawful act. *See* Kurt M. Saunders and Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUBL. POL'Y 20 (1999); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, WASH. U. L. Q. 461, 470–74 (giving examples); *see also* Laracuente v. Laracuente, 599 A.2d 968 (N.J. Law Div. 1991) (showing typical social security number identity theft).

61. Discussions pertaining to the special concerns regarding data collection from children often mention the inability of children to effectively consent to such data collection. This demonstrates a special concern for the autonomy, or lack thereof, of children.

62. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 1, at 4–5.

63. *Id.*

64. *See* Jane Birnbaum, *Here's How to Protect Your Medical Records*, CHICAGO TRIB., Nov. 23, 1999, *available at* 1999 WL 2935001; David F. Linanes & Ray Apencer, *How Employers Handle Employees' Personal Information: Report of a Recent Survey*, 1 EMPLOYEE RTS. & EMPLOYMENT POL'Y J. 153 (1997).

65. *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 22 (1997) ("[W]ide disclosure of certain kinds of information may distort individual behavior in an inefficient fashion. Fearing loss of employment and social discrimination, people will either lie to their physicians or avoid seeking care that might lead to the creation of sensitive health care or genetic information."); *Patent Confi-*

Some commentators have used the fact that personal data has a public-goods structure to argue that website/consumer interactions will be inefficient.[66] The mere fact that websites need not internalize the costs they create for third-party Web users does not, by definition, mean that the resulting website privacy norms are inefficient. The determinative factor will be a Kaldor-Hicks test.[67] This test makes a hypothetical comparison of whether the websites' benefits from the activity could in principle more than compensate Web users for their losses. As a practical matter, this determination is often exceedingly difficult to make with any degree of certainty.

In the eyes of many privacy advocates, the calculation is not even close, as the loss to individual privacy is thought to be so grievous and fundamental as to outweigh any claim based merely on the prospect of more efficient electronic commerce. The website industry sometimes makes pronouncements to the effect that the benefits to industry, and therefore to consumers indirectly, are great, while privacy-related harms, although not insignificant, are nevertheless relatively small and greatly exaggerated. The fact that the website industry makes this claim cannot be taken as evidence of the industry's true estimation of the likely result of a Kaldor-Hicks test, however, as industry speakers can be expected to seek to maximize profit, not candor. Due to the lack of a parallel profit motive, there may be less reason for cynicism with regard to the distance between the expressed views and the actual views held

---

dentiality: Hearing Before the Subcomm. on Health of the House Comm. on Ways and Means, 105th Cong. (1998), *available at* 1998 WL 18089939 ("In the absence of such trust, patients will be reticent to accurately and honestly disclose personal information, or they may avoid seeking care altogether for fear of suffering negative consequences, such as embarrassment, stigma, and discrimination. Along the continuum, if doctors and other health care providers are receiving incomplete, inaccurate information from patients, the data they disclose for payment, research, public health reporting, outcomes analysis, and other purposes, will carry the same vulnerabilities.").

66. *See* SWIRE & LITAN, *supra* note 26 ("Consider the incentives of a company that acquires private information. The company gains the full benefit of using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties. The company, however, does not suffer losses from the disclosure of private information. Because customers often will not learn of the overdisclosure, they may not be able to discipline the company effectively. In economic terms, the company internalizes the gains from using the information but can externalize some of the losses and so has a systematic incentive to overuse it. This market failure is made worse by the costs of bargaining for the desired level of privacy. It can be daunting for an individual consumer to bargain with a distant Internet merchant . . . about the desired level of privacy. To be successful, bargaining might take time, effort, and considerable expertise in privacy issues.").

67. *See* J.R. Hicks, *The Valuation of the Social Income*, 7 ECONOMICA 105, 110 (1940); Nicholas Kaldor, *Welfare Propositions of Economics and Inter-Personal Comparisons of Utility*, 49 ECON. J. 549, 550 (1939).

by public-interest privacy advocates. Accordingly, there is some reason to suppose that a Kaldor-Hicks test may favor consumers over websites.

Some consumers, however, may be in a position on their own to sanction misuses of their personal data.[68] If it is the sort of site that one might visit on a repeated basis, then users can sanction these sites by withholding their visits and instead visit competing websites. In addition, disaffected users may sanction sites through negative gossip or criticism. Consumers also may adopt self-help measures such as supplying false information to the site.[69] Under typical circumstances, this behavior would be ruled out by a widely shared norm against deception and lying. But there is a competing norm of turnabout-is-fair-play, which may prove dispositive for numerous people who might otherwise not be given to deception.[70]

The problem, however, is that all of these self-help measures assume that consumers have knowledge of the data extraction practices of offending websites. It is precisely for this reason that websites have generally sought at all costs to avoid explicit disclosure of their personal-data practices. Even when the consumer is aware that personal data is being collected, there is still the potential for abuse because consumers may be unaware of the uses to which their data is being put. For example, a user might be passively aware that personal data, such as credit card number or mailing address, are being collected, but have no idea that this data is then being used by a website for purposes other than processing payment or mailing a product. In particular, many sites furtively sell data to third parties.[71]

---

68. Sanctions have the potential to promote efficient norms. The role that sanctions play is to incentivize actors to adjust their norm conformity so as to take account of the sanction in their overall calculation of the worthiness of conforming to the norm.

69. *See* George R. Milne, *Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue*, 19 J. PUB. POL'Y & MKT. 1, 9 (2000) (summarizing studies: "When Web sites require consumers to provide information to register, many consumers provide false information. Surveys report that half the Internet users report false information about a quarter of the time (Graphic, Visualization, & Usability Center 1998). Many surfers do not fill in reports because they are concerned about their privacy and do not want to be spammed (Greenman 2000). As noted by Petty (2000), unwanted contact is a primary concern of many consumers and a reason that consumers balk at providing information. Sheehan and Hoy (2000) provide empirical evidence that unwanted email contact is of high concern to online consumers."); Tan, *supra* note 37, at 665 (citing a TRUSTe study stating "40% of Internet users have provided false information at least once when registering at a website, and over 70% worry about making on-line purchases."); Jerry Guidera, *Online Shoppers Often Lie To Guard Privacy, Survey Says*, WALL ST. J., Mar. 16, 2000, *available at* 2000 WL-WSJE 2948132.

70. Some commentators have explicitly promoted the acceptability of supplying false information as a self-help measure.

71. Studies indicate that consumers are particularly afraid of transfers of their personal data to unknown third parties. *See* 1999 FTC REPORT TO CONGRESS, *supra* note 4.

The website industry did not trumpet the fact that the website industry data-collection norms above characterized its behavior with regard to the collection of personal data. The industry maintained these norms because it was profit maximizing and legal for individual websites to conform to them, not because the managers of the various online firms, acting as a coherent group, wished to establish justified norms of obligatory behavior for their industry. Thus, it served the website industry's interests that these norms in general remained unarticulated. This highlights the fact that norms, at their core, are patterns of behavior as opposed to rules, statements, or other linguistic entities.[72]

The early website norms are fairly described as "permissive norms." They create normative freedom for their conformers rather than obligations or constraints.[73] This is noteworthy as norms theorists often write as if norms by definition express obligatory behavior.[74] One illuminating way to conceive of the project of privacy norm reformers, then, is that their goal is to shift website norms from permissive norms to obligatory norms.

B. *Game-Theoretic Structure of the Original Website Personal Data Norms*

The purpose of informal game theory is to model the strategic structure of social situations. The most famous and perhaps pervasive strategic structure of interest to social scientists and policymakers has been the structure variously known as the Prisoner's Dilemma, collective action problem, public good problem, or tragedy of the commons.[75] As the following discussion will demonstrate, the collective action problem is applicable to the topic of online privacy.

---

72. A norm need not be expressed in linguistic terms in order to have content, whereas a rule is by definition linguistic. A norm's content is defined in terms of its strategic structure. A norm, then, is behavior of a certain sort, which may or may not have an attached linguistic component. When characterizing a group's norms, it is necessary to keep in mind the difference between norms and rules, as it is important to be able to look at the actual practices of groups, rather than merely going by what they express linguistically. Talk is cheap; it is conforming behavior that creates benefits for conforming groups and externalities for third parties. *See* Steven Hetcher, *Norms*, in ENCYCLOPEDIA OF ETHICS 909, 909–12 (2d ed., Lawrence C. Becker ed., 1992). Elsewhere, I adopt the term "norm statement" or "rule" for the linguistic component of a full norm. *Id*.

73. *See generally*, SHELLEY KAGAN, THE LIMITS OF MORALITY (1989).

74. Robert D. Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 587–88 (1998); Eric Posner, Symposium, *Law, Economics & Norms: Law, Economics, and Inefficient Norms,* 144 U. PA. L. REV. 1697, 1699 (1996) ("A norm can be understood as a rule that distinguishes desirable and undesirable behavior and gives a third party the authority to punish a person who engages in the undesirable behavior.").

75. *See generally* HARDIN, *supra* note 18.

Much less understood than the collective action problem is the coordination game.[76] While political scientists, economists, and philosophers have been developing a deeper understanding of the coordination game for a generation, legal theorists have only recently come to appreciate its significance.[77] The following discussion will demonstrate that coordination games have an important role to play in modeling the strategic structure of some of the social situations that undergird the online privacy debate.

This sub-part has three sections, each of which will explore a strategic situation of concern to the privacy debate. Once these distinct strategic structures are understood, it will be easier to proceed on a path toward more respectful and efficient online personal-data norms. The first section considers whether the original permissive norms of the website industry can be accurately modeled as failed solutions to an iterated collective action problem. This question arises because the FTC has made remarks which suggest that it intuitively views the situation in these terms. I argue in the second section, however, that this characterization is incorrect. Instead, the original, permissive norms of the website industry are best modeled as a multi-party coordination game. Getting clear on this distinction matters tremendously because it affects how various norm entrepreneurs should approach the task of bringing about more respectful practices in the website industry. The third section demonstrates that there is a significant collective action problem. It is website users, not the websites, however, who face a collective action problem. Their collective action problem arises with regard to organizing themselves to demand more respectful privacy norms.

1. Purported Website Industry Prisoner's Dilemma

The FTC contends that it would be in the interest of the website industry to provide better privacy protection for consumers. The idea is that by showing more respect for the data privacy of consumers, websites will gain their trust and confidence. This in turn will lead to substantial growth in electronic commerce as trusting consumers will be more inclined to use the Internet to conduct their business. In its 1999 Report to Congress, the FTC stated that, "The Commission's efforts have been based on the belief that greater protection of personal privacy on the Web will not only benefit consumers, but also benefit industry by increasing consumer confidence and ultimately their participation in the online marketplace."[78]

---

76. *See* Hetcher, *supra* note 31, at 42.

77. *Id*. at 42 n. 160.

78. 1999 FTC REPORT TO CONGRESS, *supra* note 4, at 2–3; 1998 FTC REPORT TO CONGRESS, *supra* note 1, at 3–4.

In his recent testimony before Congress, Marc Rotenberg of the Electronic Information Privacy Center ("EPIC") made a similar assertion: "Users of web-based services and operators of web-based services have a common interest in promoting good privacy practices. Strong privacy standards provide assurance that personal information will not be misused, and should encourage the development of on-line commerce."[79]

As these remarks indicate, both the FTC and EPIC think that it would be in the interest of the website industry to be more solicitous of the privacy concerns of consumers, in order to bring about greater user trust, which in turn will lead to a more robust online marketplace. This shared assumption by these leading online policy makers is crucial because of the policy implications which the FTC appears to think flow from it. Specifically, if it is in the industry's interest to respect privacy, bringing about more respectful practices will be a task of creating recognition across the website industry of the importance of privacy for consumers and why it is in the industry's interest to be solicitous of this concern of consumers. Not surprisingly, then, the FTC has sought to promote more respectful industry practices by means of educating the website industry. The FTC has held a number of workshops and related events with the goal of raising industry consciousness of the importance of data privacy.[80]

The problem with the FTC's education program, however, is that it implicitly treats the website industry as if it were a unitary actor capable of behaving in a concerted fashion so as to promote its collective goals. In its belief that its education program could achieve this result, the FTC unwittingly falls prey to the so-called fallacy of composition.[81] This is the fallacy of thinking that because a group, considered as a whole, would benefit from some particular political outcome, that therefore it is in the interest of each of the particular members of that group to do its part to

79. Rotenberg, *supra* note 48.

80. *See, e.g.*, FEDERAL TRADE COMMISSION, THE INFORMATION MARKETPLACE: MERGING AND EXCHANGING CONSUMER DATA, *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.html (March 13, 2001) (Public workshop notices posted on the FTC homepage at www.ftc.gov).

81. HARDIN, *supra* note 18, at 2 ("Although it can make good sense to say that an individual is rational, there is no obviously useful new sense in which we can typically say that a group is rational. Yet, one of the more widely accepted doctrines of modern political science—the group theory of politics—was based on a presumption from the fallacy of composition: that a group of people with a common interest will take action to further that interest. That doctrine has collapsed in the face of two major developments . . . Mancur Olson's logic of collective action and game theory's Prisoner's Dilemma. In the latter, there is a dilemma precisely because what it makes sense for an individual to do is not what would make sense for the group to do—if one could meaningfully speak of what the group should do.").

help bring about this political outcome. It is simply false to assume that a typical website would have such an interest.[82]

The benefit of a particular website's individual contribution to the collective good, for all but the largest sites, will be marginal. Whether the collective good comes about almost surely will not depend on the additional contribution of the particular site. Thus, from a narrowly rational, economic perspective, the site is better off to free ride on the contributions of the other sites. Either enough other sites cooperate and the collective good is provided, or enough other sites do not cooperate, and the collective good is not provided. Either way, the behavior of the particular website will have but a marginal impact. Thus, it might as well refrain from incurring the expense of cooperating, that is, it might as well free ride.

The problem is that all the other websites are similarly situated. Each will have a dominating preference to free ride. The result is that all will free ride and the collective good will not be produced.

The strategic structure of this situation may be represented as follows:

FIGURE 1:
WEBSITE INDUSTRY COLLECTIVE ACTION PROBLEM

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

Figure 1 displays the strategic relationship between a particular firm, call it Website A, and all other websites (as based on the FTC's assumption described at the outset of this section). As indicated by the cardinal payoffs in the southwest cell, A's first preference is that other firms "Respect Privacy," so that it will be able to free ride on this set of prac-

82. Lighthouses are a classic example of a collective good as there is a collective action problem with regard to the provision of the lighthouse. Each individual potential beneficiary would benefit from the provision of a lighthouse. Nevertheless, there is a collective action problem because once the lighthouse is provided, it is provided for all. In other words, the individual cannot be excluded from benefitting from the good even though she did not contribute toward its provision. Thus, each individual does best by defecting from providing her share toward its provision. But since all potential beneficiaries are similarly situated, each will free ride and hence the good will not be provided.

tices and "Disrespect Privacy." For the time being, "Disrespect Privacy" should just be taken to mean that the site will conform to the set of personal-data norms of the early website industry listed above, and "Respect Privacy" should be taken to mean that the site will refrain from conforming to these norms. Part Two below will provide greater content to the notion of respecting consumer data privacy.

In the circumstance in which A free rides on the respectful behavior of the other sites, A receives the highest payoff, 4.[83] According to the FTC, when other firms respect privacy, consumers will be less fearful of the Internet and consequently more prone to participate in electronic commerce. This will make it easier for website A to benefit from its own disrespectful practices, as consumers will be less leery of providing personal data to the site, based on their generally positive experiences with other sites.

The problem is that the same strategic situation pertains for the other websites as well. Each website would like all the other sites to be respectful so that it alone can take advantage of the more trusting consumers. Because defection is the dominant strategy for all, however, the southeast cell will be the result. Note that in the southeast cell, each site receives 2, its second lowest payoff. If, however, the website industry were to be successful in solving its collective action problem, the situation as characterized in the northwest cell would obtain instead. In this situation, each site would receive 3, its second highest payoff.

Note the distressing result that while all parties would do better by cooperating and thus ending up in the northwest cell, nevertheless, due to the fact that each is compelled by narrow self-interest to perform the noncooperative action, the mutually dispreferred group outcome as represented in the southeast cell is the actual result.[84] We see then that individually maximizing behavior leads to a collectively suboptimal result; the classic collective action problem.

Uncovering this strategic structure inherent in the relationship among websites has important policy implications. Recall that one of the FTC's initiatives in order to promote online privacy was to educate the website industry about the connection between treating consumers with respect

83. Each of the four pairs of numbers represents the payoffs to each party in each of the four possible outcomes, the left-hand number is the payoff to the row-player and the right-hand number is the payoff to the column player. Higher numbers represent more preferred outcomes.

84. Based in part on its survey of over 1400 commercial websites, the FTC in 1998 concluded that there was not yet effective self-regulation: "The Commission's examination of industry guidelines and actual online practices reveals that effective industry self-regulation with respect to online collection, use, and dissemination of personal information has not yet taken hold." 1998 FTC REPORT TO CONGRESS, *supra* note 1.

and the expansion of electronic commerce. In light of the preceding discussion, however, it is clear that things are not so simple; educating the industry participants, as to their collective interest will in no way address the collective action problem faced by each of the particular members of the industry with regard to the supply of this collective good. Education may enhance the appreciation of each of the members as to the value of the potential collective good available to the group, but it will not change the incentives of individual members so as to bring the group any closer to realizing the collective good.

It will be difficult for the website industry to solve this collective action problem on its own. According to Ellickson's hypothesis, close-knit communities may produce solutions to collective action problems, as they provide opportunities for repeat play and multiplex relationships among "neighbors."[85] When there is repeated interaction, parties may have an incentive to reach a mutually preferable manner of interaction because they will take their long-term interests into account, and these will often favor cooperation in current games in order to foster cooperation in future games. In the present context, this would mean individual websites not defecting on the cooperative behavior necessary to bring about a higher level of consumer trust in online commerce.

It may not be possible to apply Ellickson's hypothesis in the present context, however, as it is unclear whether the notions of "close-knittedness" or "neighbor" have any reference in cyberspace. Ellickson provides an extended discussion of land-use practices of the close-knit ranching and farming community that inhabits Shasta County in Northern California. This community's norms concern issues such as liability for damage done by cattle and allocation of the costs of fencing, so as to avoid damage from cattle. This discussion implicitly assumes that the space in which interaction was taking place was physical space, not virtual space. What allows the ranchers and farmers to be close-knit was their physical proximity, as the subtitle of Ellickson's book—"How Neighbors Settle Disputes"—indicates.[86]

If the notion of close-knitedness is to have meaning online, then the term must be cashed out in non-geographical terms. The Internet pro-

85. ELLICKSON, *supra* note 16, at 250. Ellickson defines "close-knit" groups as follows: "A group is *close-knit* when informal power is broadly distributed among group members and the information pertinent to informal control circulates easily among them." *Id.* at 177–78. Ellickson's definition of close-knittedness implies "group members" having both "continuing reciprocal power over one another and also a bank of shared information." *Id*. at 238. Ellickson notes that close-knittedness is inversely related to group size—the smaller the group, the greater the degree of close-knittedness. *See id.* at 182. However, "[A] group does not necessarily have to be small to be close-knit." *Id.*

86. ELLICKSON, *supra* note 16.

motes communication, par excellence, and thus is a boon to the formation and maintenance of social relationships. There is no reason those online relationships cannot involve repeat play and be overlapping, and there is no reason they cannot involve sanctions. Thus, the core preconditions for Ellickson's hypothesis may in principle be satisfied. More research is needed on the extent to which mechanisms such as hyperlinking may provide the foundation for close-knit communities in cyberspace. Despite the potential significance of this suggestion for our understanding of cyberspace generally, the implication for website privacy norms is untoward, as the relevant relationships at issue—those between websites and other websites, websites and users, and users and other users—are typically not close-knit. It is simply not the case that all the numerous sites on the Internet have repeated and overlapping interactions with one another.[87] The unavoidable conclusion appears to be that the website industry will not be able to solve its collective action problem on its own.

The collective action problem is a classical justification for governmental intervention.[88] Websites could simply be required to adopt more respectful practices.[89] This would have the effect of forcing websites to produce the cooperative outcome represented in the northwest cell in Figure 1. It is doubtful, however, whether the FTC has the authority to demand that websites change their behavior.[90] Even if the FTC had the authority, if one takes their remarks at face value, this is not authority they would care to exercise in this manner. As discussed earlier, the FTC has all along avowed an interest in promoting industry self-regulation to the extent possible.[91] If the agency is to remain faithful to this goal, it must somehow indirectly encourage websites to solve their industry-wide collective action problem. Collective action problems, however, are

87. Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS 311, 314 (1995) ("In addition, the rapid growth in the number of network users has worked to transform cyberspace in important respects. With its forty or fifty million users, the Internet is no longer comprised of a limited set of close-knit communities in which private ordering can be based on shared values and understanding."); *see also, The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1676–1680 (1999).

88. For the classic discussions, see WILLIAM J. BAUMOL, WELFARE ECONOMICS AND THE THEORY OF THE STATE (1952); ANTHONY DOWNS, AN ECONOMIC THEORY OF DEMOCRACY (1957).

89. For example, the E.U. Privacy Directive has a complex set of requirements to which firms that use personal data of Europeans must adhere. *See* Privacy Directive, *supra* note 21.

90. *Consumer Internet Privacy: Hearing Before the Senate Comm. on Commerce, Science, and Transportation*, 106th Cong. (2000) (Marc Rotenberg, Executive Director, Electronic Privacy Information Center) ("The reliance of privacy guidelines on the FTC Act prohibiting unfair and deceptive business practices has not provided an adequate basis for the protection of privacy interest. . . .").

91. Elsewhere, I question the FTC's sincerity in its stated desire to promote industry self-regulation. *See* Hetcher, *supra* note 13.

notoriously difficult to solve. Thus, the FTC would face an especially daunting task in seeking to do so in an indirect manner.

2. Website Industry Coordination Norms

As noted at the outset of the previous section, the analysis of that section was based on the assumption of the FTC that the website industry has an overriding interest in bringing about more respectful privacy norms, if only the constituent websites could coordinate their efforts to bring about the cooperative result. It is more plausible to suppose, however, that the benefit of increased electronic commerce is not worth the high cost that providing respect for privacy might impose on websites.

The most significant cost for many sites of course will be the fact that consumer personal data will no longer be theirs to use and manipulate at will for free. In addition, for small sites, the very act of creating privacy policies imposes a cost that may be significant.[92] For large sites, these development costs are of marginal importance. But sites of successful or well-funded companies face a much larger cost: the increased exposure to litigation they face as a result of making explicit representations to site visitors regarding the site's data-collection practices.[93] Even if there is some marginal increase in their online traffic due to heightened consumer trust, it is more plausible to think that most sites would forego this benefit in order to avoid exposure to legal liability. Thus, the problem the FTC has in seeking to foster respect for privacy by self-regulatory means is not best modeled as the problem of helping an industry group that is not close-knit procure a collective good. Instead, as the following discussion demonstrates, the strategic structure faced by the website industry is actually that of a coordination norm.

A coordination norm is a practice in which each conformer receives a "coordination benefit" for conforming to the norm. A coordination benefit is the added benefit an actor receives for conformity, given the conformity of other participants.[94] To take a simple example, if the norm is to walk on the right side of the sidewalk, such as it is in America, then a particular

92. Anecdotal evidence suggests, however, that some sites avoid this cost by simply, and illegally, cutting and pasting from the privacy policies of other sites that they find on the Web.

93. For example, RealNetworks recently admitted that its RealJukebox assigned a personal ID number to users and uploaded information about their listening habits to its server, contrary to its privacy policy. *See* Sara Robinson, *CD Software Is Said to Monitor Users' Listening Habits*, N.Y. TIMES, Nov. 1, 1999, *available at* http://www.nytimes.com. The company was subsequently slapped with a $500 million class action lawsuit for violating California's unfair business practices law. *See RealNetworks is Target of Suit in California Over Privacy Issue*, N.Y. TIMES, Nov. 9, 1999, *available at* http://www.nytimes.com.

94. *See* Hetcher, *supra* note 31, at 43–45 & nn. 161–68.

conformer to this norm receives a benefit when others conform to the norm as well, as she is less likely to be involved in a pedestrian collision.

A coordination norm may be "an equilibrium," a "coordination equilibrium" or a "proper coordination equilibrium."[95] An equilibrium is a combination of choices in which each actor has done as well as the actor can, given the choices of the other actors. No actor will regret its choice given the choices of the others. A coordination equilibrium is a combination of choices such that no one would have been better off had any one actor, either the actor or someone else, behaved differently. A proper coordination equilibrium is a combination of choices such that no one would have been as well off had any one actor behaved differently, either the actor or someone else.[96]

Details aside, the crucial feature of coordination norms is that actors conform to them because it is in their direct interest to do so. This contrasts with collective action problems in which each actor's direct preference is not to conform but instead to defect, or free ride. With collective action problems, conformity will be forthcoming only if the participants are able to incentivize one another to conform due to the possibility of repeat play that results as a by-product of the overlapping social relationships of close-knit communities. With coordination norms, by contrast, actors want to conform, given the conformity of others. Hence, efficient coordination norms may emerge in communities that are not close-knit.[97]

The present concern, then, is whether personal-data practices are best modeled as coordination norms. The core feature of a coordination norm is that an actor receives a coordination benefit from performing the conforming action, given the conformity of others. This condition is met with regard to the permissive, data-collection practices of the early website industry. As already noted, particular websites have a direct interest in not

95. *See* Hetcher, *supra* note 31, at 44, 74; DAVID LEWIS, CONVENTION (1969); EDNA ULLMANN-MARGALIT, THE EMERGENCE OF NORMS (1977); *see also* Margaret Gilbert, *Game Theory and Convention*, 46 SYNTHESE 41 (1981).

96. LEWIS, *supra* note 95. With a proper coordination equilibrium, other conformers receive a benefit when a particular actor conforms. It is this feature that causes David Lewis to claim that "conventions" are best modeled as proper coordination equilibria. Conventions, on Lewis' well-known account, are maintained in part by sanctions. Conformers sanction one another for non-conformity because it is in the interest of others that each conform. The sanctions are meant to ensure the conformity of others. The economics literature on "network externalities" encompasses a similar but broader rational structure as not all networks with significant externalities are norms.

97. Coordination norms have similar structural features to "network effects." On network effects generally, see, e.g., Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998) (arguing for limiting the assumption that network effects produce suboptimal lock-in); S.J. Liebowitz & Stephen E. Margolis, *Path Dependence, Lock-In, and History*, 11 J.L. ECON. & ORG. 205 (1995).

showing respect for consumers. By this means, they gain use of valuable user data at less expense and effort and they avoid the worry of exposing themselves to legal liability by making explicit representations to consumers as to how their data will be used.

In addition, it is plausible to suppose that websites prefer that other websites also fail to show respect for consumer privacy. First, websites will be able to more successfully collect data when consumers are left in the dark. Thus, all websites will be hurt to the extent that some particular website takes it upon itself to be more forthcoming in telling consumers about its data gathering activities. The greater the public awareness of website data-gathering activities in general, the more likely it is for consumers to be wary of the activities of any particular website, and the more the site will be made to feel public pressure to alter its practices in the direction of greater respect.

The second reason why websites prefer that other websites conform to disrespectful privacy norms is that in privacy law, reasonable expectations of privacy matter.[98] An action in tort for invasion of privacy may be brought in civil litigation by aggrieved parties.[99] In such cases, a central consideration is whether the plaintiff had a reasonable expectation of privacy. If most websites are collecting data at will, with no safeguards and no notice, then the website-defendant will have a colorable defense based on the claim that the plaintiff did not have a reasonable expectation of privacy.[100]

For both of the above reasons, then, it is to be expected that industry insiders will discretely promote disrespectful norms among their number on whatever occasions present themselves, such as through trade association meetings and the like, as doing so strengthens the norm and consequently solidifies their safe harbor.[101] This means that these disrespectful website coordination norms will tend to be stable. Particular websites will have no internal motivation to change their behavior, and

98. *See, e.g.*, Dorothy Glancy, *Symposium on Internet Privacy: At the Intersection of Visible and Invisible Worlds: United States Privacy and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 363–64 (2000) ("Assurances of privacy protection by e-commerce vendors and Internet service providers demonstrate that the commercial side of the Internet recognizes that respect for privacy is a significant expectation of Internet users.") (footnotes omitted).

99. *See generally* Fletcher v. Price Choppers Foods of Trumann, Inc., 220 F.3d 871 (2000); Cramer v. Consolidated Freightways, Inc., 209 F.3d 1122 (2000).

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

101. *See* Hetcher, *supra* note 31.

further, each site will have an incentive to motivate the other sites to continue their disrespectful behavior.

The original website data collection norms appear then to be a proper coordination equilibria, as it is the case with each particular website that it would not have been as well off had either it or some other website acted differently by not conforming to the disrespectful privacy practices. This situation is represented in the following payoff matrix.

FIGURE 2:
WEBSITE INDUSTRY COORDINATION GAME

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

The payoff matrix in Figure 2 displays the outcomes received by websites depending on whether each of them, as well as the other websites, participate in personal data collection practices that either "Respect Privacy" of Web users, on the one hand, or "Disrespect Privacy" of Web users, on the other hand. Note that the payoff to a typical website, call it Website A, is affected by whether other websites respect privacy or disrespect privacy. The dominating preference is to disrespect privacy. Website A prefers to disrespect privacy regardless of what other sites are doing. Thus, A's payoffs are higher in either of the southern cells as compared to either of the northern cells. But A receives a coordination benefit when other sites also disrespect privacy. Thus, the payoff for A is higher in the southeast cell as compared to the southwest cell. A least prefers the situation represented in the northeast cell in which it respects privacy and other sites disrespect privacy. In this situation, there will be no noticeable increase in electronic commerce and yet A has lost all the benefits from the free receipt of user data.

Like A, other sites prefer to disrespect privacy, so their highest payouts come in the eastern cells. They prefer, however, that A also disrespect privacy, due to the coordination benefit of keeping consumers in the dark. Thus, the other sites do better in the southeast as compared to the northeast cell. If the other sites are respecting privacy, however, then they will likely prefer that A do so as well, so that A is not at a

competitive advantage. Thus, their payoff is higher in the northwest as compared to the southwest cell.

Note that the outcome as represented in the southeast cell in which all websites are disrespecting privacy is a stable equilibrium. No website has any incentive to change its behavior, nor does any website have any incentive to get another website to change its behavior. Just the opposite, each website has an incentive to encourage each other website not to change its behavior. As should be obvious, this is not a happy outcome, from the perspective of consumers or the FTC.

3. Web User Collective Action Problem

Note that the data-collection coordination norms of the website industry discussed in the previous section may function efficiently from a point of view internal to the conformers themselves. The harm resulting from these practices—the degradation of personal privacy—is successfully externalized onto the Web-surfing public.[102] Because these data-collection practices are bad for consumers as a group, there is the potential for this group to secure an important collective good, the abatement of these practices. As the current section demonstrates, however, there is a severe practical problem in consumers securing this good.[103] Consumers will face a collective action problem in seeking as a group to bring about the collective good of more respectful website privacy practices. Thus, when the analysis of this subsection is combined with that of the previous two subsections, the surprising result is reached that while the website industry does not face a collective action problem, the users of their websites do.

As discussed earlier in the context of website practices, standard game theory teaches that groups will stand their best chance of pursuing collective goods when their membership is close-knit such that members have repeated interactions across a number of dimensions.[104] This is more likely

---

102. The possibility of externalization of the costs of an industry custom is one reason why the established "rule of custom" in tort law is that conformity to industry custom may serve as evidence of due care, but is not dispositive. *See* Hetcher, *supra* note 31.

103. ULLMANN-MARGALIT, *supra* note 95 (recounting classic norm emergence and emphasizing that the first step is to identify underlying social situations in which an emergent norm would promote efficiency).

104. Sociologists refer to such relationships as "multiplex." *See, e.g.*, ELLICKSON, *supra* note 16, at 55. In the early days of the non-commercial Internet, online interactions were typically between members of particular research communities. The members of those communities often had "multiplex" relationships with one another. These researchers might see each other at conferences; they might be former classmates, or share advisors or mentors; or they might wish to seek future employment at one another's institutions. Accordingly, there would often exist ample opportunities to sanction non-cooperative behavior, or reward cooperative behavior. Listservs such as *The Well* are of interest in this regard. *The Well* was pre-

for smaller groups than larger groups, for groups that are close to one another in geographical space, and for groups that share similar interests, preferences, and histories. For example, the civil rights protestors who fought for months and ultimately prevailed in integrating Nashville's downtown restaurants in 1960 were African-American students of Fisk University, who had together participated in extensive group training in Gandhian methods of passive resistance.[105]

The Internet, however, makes collective action of this sort difficult. In theory, privacy militants might electronically enter previously targeted sites and all request downloads at the same time, such that the site's servers might be overwhelmed.[106] Clearly, this technique would require a good deal of coordination and effort among a large number of people. Thus, while possible in theory, such collective action is unlikely in practice.[107] Visitors to a website are the opposite of close-knit—they are globally interspersed strangers. Thus, a solution to the Prisoner's Dilemma of the sort outlined by Ellickson is unlikely, due to the larger numbers of web users who lack overlapping or close-knit relationships. Accordingly, we can predict that extant website practices will represent a failure by consumers to solve collective action problems regarding the abatement of the degradation of their data privacy.

Moreover, the mere existence of a collective action problem does not imply that a norm, or set of norms, has been identified to deliver the potential collective good. A particular consumer who wanted to do her part to bring about the collective good of greater respect for consumers would

---

Web and non-commercial. In addition, many of its members were part of a relatively close-knit community, the Bay Area Internet *cognoscenti*. *The Well* nevertheless allowed members to interact anonymously if they wished. Predictably, serious problems arose with the community. *See* ESTHER DYSON, RELEASE 2.0: A DESIGN FOR LIVING IN THE DIGITAL AGE (1998).

105. *See* DAVID FARBER, THE AGE OF GREAT DREAMS: AMERICA IN THE 1960S, 76 (1994).

> In Nashville, which became the focal point for the sit-in movement, the means by which a protester should politely refuse to accept the legal bounds set by civil society were carefully codified. James Lawson, a longtime student of Gandhian nonviolence, explained: 'Do show yourself friendly on the counter at all times. Do sit straight and always face the counter. Don't strike back or curse if attacked.' With discipline, the protesters were turning American society on its head.

Id.

106. Tom Kirchofer, *Microsoft Networks Tap Akamai*, BOSTON HERALD, Jan. 30, 2001, at 29 (noting that "Denial of Service" attacks overwhelm a company's computer with information and prevent legitimate traffic from getting through); *see also* Greg Miller, *Microsoft Hit by New Wave of Outages; Internet: Hackers Cripple Company's Most Popular Websites; FBI is Asked to Probe "Denial of Service" Attacks*, L.A. TIMES, Jan. 26, 2001, at C3.

107. In addition, websites may have more ready access to technological means to remove protesters. *See* LESSIG, *supra* note 3, at 66–70 (noting that no protesters allowed in AOL space through restrictive coding).

not know where to start. There are no previously identified norms of behavior which, if conformed to by consumers, would help force websites into more respectful behavior. Because there is no cooperative norm under way, there is no form of cooperative behavior to *internalize*,[108] no issue of loss of *esteem* for failing to be cooperative,[109] and no concern to *signal* to others that one is a cooperative online activist.[110] It seems unlikely, then, that better website practices will emerge as a result of consumer collective action along the lines of any of the other leading models for solving collective action problems.

It will be useful to summarize the discussion of this first Part in order to see how this last finding regarding the dismal prospects for consumer collective action fits in with the earlier findings. The key fact on which the whole analysis thus far is predicated, is that the original data-collection norms adopted by the website industry demonstrated a good deal of disrespect for consumer privacy. Essentially, the vast majority of websites did whatever they wanted with regard to the use of personal information on consumers, with complete disregard for the impact of these activities on the privacy interests of these consumers. Despite growing complaints about this significant threat to individual privacy, the government was reticent to directly regulate this activity, apparently in response to the widespread norm that, as much as possible, the Internet should be left free to self-regulate.

Internet self-regulation, at least in the context of website practices with regard to the personal data of consumers, has been widely regarded as a failure.[111] In the above discussion, informal game theory was utilized in order to better understand why self-regulation has failed to produce a set of online practices that better respected consumer privacy. Generally speaking, self-regulation failed due to the strategic structure of the underlying social situations that obtained regarding the relationships between consumers and websites, on the one hand, and websites with one another on the other hand. Specifically, websites are in a coordination game with one another, not an iterated collective action problem. Thus, efforts to

---

108. Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643, 1690–94 (1996).

109. Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 342 (1997) ("theory of origin and growth of norms" in which "the initial force behind norm creation is the desire individuals have for respect or prestige, that is, for the relative esteem of others.").

110. ERIC A. POSNER, LAW AND SOCIAL NORMS (2000); Eric A Posner, *Symbols, Signals, and Social Norms in Politics and the Law*, 27 J. LEGAL STUD. 765, 780 (1998).

111. *See* Marc Rotenberg, *supra* note 90; *see also* Brendan Maher, *Self-Regulation*, TARGET MARKETING, Dec. 1, 2000, *available at* 2000 WL 10932469 (arguing that consumers and businesses have little confidence in self-regulation and citing to a survey claiming 24% of adults polled felt the federal government should set privacy rules).

educate websites on the importance of privacy to consumers, and on the connection between allaying consumer privacy fears and the promotion of consumer confidence, will not work to change website behavior in the manner desired by the FTC. Nor will consumers be able to band together to demand more respectful privacy practices on the part of websites due to the large-scale collective action problem they face.

A number of commentators concluded that the failure of self-regulation to overcome these hurdles mandated that the government step in and take a direct role in requiring more respectful informational practices on the part of websites. In the discussion in Part II below, however, it will be shown that direct government regulation of website practices has in fact not been required in order to bring about more respectful privacy practices. While the FTC has played an important role, its role has been that of a norm entrepreneur rather than a norm imperialist.

II. WEBSITE NORM ENTREPRENEURS PROMOTE PRIVACY-RESPECTINGWEBSITE INDUSTRY CUSTOMS

Despite the serious obstacles explored above, significant progress has been made in moving toward industry norms that are more respectful of consumer privacy. In less than a decade, norms of respect for consumer privacy have emerged on the Internet. Evidence of this norm is everywhere. For example, AOL/Time-Warner's advertisements now typically contain assurances that the company ensures consumer privacy. A dramatic shift such as this, occurring over a relatively short period of time, is fairly characterized as a "*norm cascade*."[112] This cascade in turn was precipitated by a "*norm shock*," introduced by the FTC.[113] The *grundnorm* of respect is still aspirational to a large extent, in that many websites are not yet complying, or are under-complying.[114] Nevertheless, many websites are indeed taking consumer privacy more seriously, and those that are tend to be the largest and busiest sites.[115] Furthermore, those sites not currently taking privacy seriously are increasingly feeling the heat to do so.

The situation has gone from one of a solid, albeit unarticulated, norm of permissive non-respect for data privacy in the early to middle 1990s, to one in which there are two competing sets of norms, the old, non-respectful norms of permissiveness with regard to personal data, and the

112. *See* Sunstein, *supra* note 29.
113. *See* Hetcher, *supra* note 13.
114. *See* 2000 FTC REPORT TO CONGRESS, *supra* note 14.
115. *Id.*

new norms which are more respectful of consumer privacy concerns. In the public mindset, there are now good websites and bad websites, when it comes to the issue of consumer privacy. In effect, a market in websites is emerging, such that consumers are increasingly in a position to choose among websites based on the extent to which these sites participate in personal data practices that suit the particular consumer's individual preferences. This represents a shift toward a situation in which marketplace-oriented norms of fair exchange are increasingly coming to dominate the policy framework governing online privacy.

Based on the manner in which many online privacy advocates talk, one might initially think that the only data-collection practices attractive to consumers were those that collected no data whatsoever. In fact, however, this is not what consumers expect, or indeed want. The vast majority of websites are free. The business models of many of these sites have been based mainly on deriving advertising revenue from banner ads. A secondary source of revenue comes from data collection and processing. In addition, personal data is used increasingly as a means to more personalized marketing. Personal information about individuals is used to market products and services suited to their specific preference profiles. Many consumers willingly will trade away personal data as long as they receive valuable consideration in return.[116] Indeed, the efforts of the norm entrepreneurs that will be discussed below are not best understood as seeking to minimize data collection and use, per se, but rather to change the nature of the relationship between websites and consumers from a nonconsensual to a consensual relationship. Under this normative framework, personal data is increasingly becoming a commodity that data subjects can bargain away for valuable consideration.[117]

There have been two main stages in the development of these increasingly consensual and respectful norms. The first stage involved the articulation of aspirational norms. This process was initiated by the public-interest privacy advocacy community. Much of the early advocacy work of defining appropriate privacy norms was performed in the United States. More recently, however, the European Union has exerted pressures

116. The FTC recommends that any legislation passed be in broad and technologically neutral terms so industry and consumers can continue self-regulatory initiatives. *See Privacy Online: Fair Information Practices in the Electronic Marketplace: Hearing Before the Senate Comm. on Commerce, Science, and Transportation*, 106th Cong. (2000) (Prepared Statement of the FTC), *available at* http://www.ftc.gov/as/2000/05/testimonyprivacy.htm. This enables consumers to "trade away" their personal data for prizes or discounts if they so choose. *See* Jennifer Jones, *Cashing in on Privacy*, NETWORK WORLD FUSION, Sept. 12, 2000 (noting that consumers are willing to trade personal data if the incentives are high enough).

117. *See* Radin, *supra* note 44.

that are increasingly affecting the domestic policy agenda regarding data privacy. The website industry has become involved, apparently out of a fear that if it did not, the public-interest advocacy community would completely dominate the terms of the debate.

In the second stage, the FTC began introducing incentives to get the website industry to take these aspirational norms more seriously. The norms promoted by the FTC are seen best as a compromise between the expansive set of aspirational norms promoted by the privacy advocacy community, and the more limited norms proposed by the website industry. Strange as it sounds, the FTC has sought to promote consumer data privacy by seeking to change the nature of the strategic situation faced by the website industry from a coordination game into a large-scale, collective action problem. The FTC has sought to create a situation in which it would be in the industry's interest to better respect consumer privacy as a means to securing a collective good made possible by the FTC. This collective good is the avoidance of a statute that would force the industry to provide a high level of privacy protection. The FTC essentially threatened the website industry that either the industry perform substantially better, industry-wide, in respecting privacy, or else the agency would press for a statute. This threat created a situation in which the larger websites were incentivized to conform to more respectful privacy norms, and to incentivize smaller sites to do so as well, by threatening to withdraw their substantial advertising dollars from these smaller sites if they did not show more respect for consumer privacy.[118]

Stage One: The Articulation of Aspirational Norms

The public-interest, privacy advocacy community has played a venerable role in articulating aspirational website privacy norms. The community first arose in the 1960s in response to the United States government's initial efforts to use supercomputers to construct comprehensive databases of personal data on its citizens. When websites first emerged in the early 1990s and began to take part in questionable data-collection practices, this community had a normative framework already available, which could then be applied to the new set of facts. Especially influential early on were the norms developed by the Organization for Economic Cooperation and Development ("OECD"), which endorsed eight "privacy guidelines," as set out in the following list:

118. *See infra* text accompanying notes 109–10.

OECD Privacy Guidelines[119]

1. Collection limitation
2. Data quality
3. Purpose specification
4. Use limitation
5. Security safeguards
6. Openness
7. Individual participation
8. Accountability

Marc Rotenberg, director of EPIC, has stated that OECD's eight principles for data protection are still the "benchmark for assessing privacy policy and legislation."[120] Recently, EPIC has translated the OECD's privacy norms to the context of websites. The following five website-specific privacy norms are the result.

EPIC Website Privacy Norms

1. Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the homepage by looking for the word "privacy."
2. Privacy policies should state clearly how and when personal information is collected.
3. Web sites should make it possible for individuals to get access to their own data.
4. Cookies transactions should be transparent.
5. Web sites should continue to support anonymous access for Internet users.[121]

These aspirational website privacy norms are fairly seen as representative of the sorts of protection currently being demanded by public-interest privacy advocates generally. The five items on the list are each "thick" norms that concretely describe specific practices that will increase

119. Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/dsti/sti/it/secur/ (Sept. 23, 1980).

120. Rotenberg, *supra* note 48.

121. *Id.*

consumer privacy vis-à-vis websites.[122] In fact, these proposed norms are so ambitious that they created fear in the website industry, which views the norms as unworkable and overly expensive to implement.[123] The industry's response has been to promote less demanding norms.

The website industry acknowledges that consumers have legitimate privacy interests in their personal data.[124] This is a striking admission. One might well have expected the industry to take the more aggressive position that since personal data is in the public domain, they are as entitled to its use as the data subjects. Instead, the typical posture of industry is to acknowledge, in effect, that data subjects have some special entitlement to their personal data, despite a dearth of protection within the letter of the law.

The website industry's bone of contention with public-interest, privacy advocates is over the proper conception of privacy, how much privacy is appropriate, and which thick behavioral practices should instantiate the norm of respect for privacy. In other words, the disagreement is not over respect for privacy, per se, but instead over which second-order norms and which thick behavioral norms should be instantiated to promote this respect.

The website industry generally has promoted a fairly minimalist set of practices. In principle, the industry supports giving consumers "notice" and "consent" to the collection and use of personal data. The crucial debate, however, is over how the general requirements of notice and consent are to be concretely implemented. The most heated debate has focused on whether fair notice and consent require an "opt-in" regime or instead whether an "opt-out" regime is satisfactory. With opt-out, personal data will automatically be collected unless a consumer specifically takes some action to indicate that she does not wish to have her data collected, while with opt-in, the default is that personal data will not be collected unless the consumer takes a specific action to explicitly agree to the collection of data.[125] EPIC and other public interest advocates support an "opt-in" regime while the website industry supports an "opt-out" regime.

---

122. The notion of "thick" moral features derives from the philosophical literature on moral realism. *See, e.g.*, JOHN MCDOWELL, MORAL REALISM (1991).

123. Todd R. Weiss, *Bush Faces His First Privacy Challenge Proposals from Industry, Advocates Differ*, COMPUTERWORLD, Jan. 22, 2001.

124. Schwartz, *supra* note 21, at 1691 (arguing that the concept of notice being equivalent to privacy protection seems to be capturing much of the policy debate).

125. An opt-in policy has been promoted by industry groups such as the Direct Marketing Association ("DMA") and the Online Privacy Alliance. Both groups have been leading proponents of industry self-regulation. The Online Privacy Alliance is a coalition of more than eighty companies and trade associations that formed in early 1998 to encourage self-regulation of data privacy. *See* 1999 FTC REPORT TO CONGRESS, *supra* note 4, at 7.

This section briefly has considered the competing aspirational norms promoted by public-interest electronic privacy advocates, such as EPIC on the one hand, and the website industry, on the other hand. While these organizations articulated aspirational norms, they were not well positioned to bring them into reality. Private industry advocates generally lacked the desire, while public-interest advocates generally lacked the power. The website industry had adopted a reactive posture, in essence, contending that online privacy is not a significant problem worth addressing, but if it is to be addressed, then the industry's more minimal norms are preferable. The pubic-interest advocates, on the other hand, have done everything in their power to promote expansive privacy norms. While this group may have lacked the direct power to change website norms, nevertheless it has dramatically raised the level of public awareness regarding the threat to consumer privacy posed by commercial online activities. This impact appears to have been significant, engendering an outcry among the public and media.[126] This outcry, in turn, is plausibly being reflected in the increase in attention shown to online privacy issues in Congress and the previous Administration.[127]

A. *Stage Two: The FTC's Attempt to Create an Industry-Wide Collective Action Problem*

In 1995, the FTC was asked by Congress to investigate the privacy risks associated with computer databases. The agency has been increasingly involved with the issue of online privacy ever since. The FTC acts pursuant to its authority under § 5 of the Federal Trade Commission Act, which mandates that the agency address "unfair" and "deceptive" trade practices.[128] Generally speaking, then, the FTC's hook into the privacy

126. Brian Krebs, *IT Industry Council Signals Privacy-Law Advocacy*, NEWSBYTES, Feb. 2, 2001 (reporting that due to public outcry lawmakers are suggesting federal electronic privacy protections); *see also* Rosalind C. Tritt, *Privacy: A Threat to Free Speech?*, PRESSTIME, Jan. 2001, at 27*; PrivacyRight, Inc. Forms Strategic Equity Partnership with Venture Factory*, PR NEWSIRE, June 6, 2000.

127. In a series of hearings beginning in October and November of 1995, the FTC has examined consumer protection issues, including privacy concerns. *See Internet Privacy: Hearing Before House Comm. on the Judiciary*, 105th Cong. (1998), *available at* http://www.ftc.gov/os/1998/9803/privacy.htm.

128. 15 U.S.C. § 45(a) (1994). The FTC prosecutes "[u]nfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce" under § 5 of the Federal Trade Commission Act ("FTCA"). *See id.* Section 13(b) authorizes the prosecution of actions to enforce § 5. *See id*. § 57(b). Section 18 permits the FTC to create rules to prohibit deceptive or unfair practice prevalent in certain industries. *See id*. § 57(a).

debate comes by means of casting website data-gathering practices as potentially unfair and deceptive.[129]

Significantly, the FTC claims it is moved to action because consumers strongly feel entitled to data privacy.[130] In other words, it is the existence of a strongly held community norm of entitlement to one's own data that pulls the initial causal levers leading the FTC toward greater consumer online privacy protection.[131] The FTC does not take note of the fact that in other contexts, a mere desire for control of property in the public domain does not create entitlement to control this property. As the previous discussion indicated, while the website industry disputes the level of privacy protection necessary, it does not contest the fundamental proposition that data subjects have some sort of entitlement to, or property claims in, their personal data. Thus, the FTC has not met with resistance from the website industry on the issue of data subject entitlement to personal data, per se.

The FTC has promoted more respectful website privacy norms by attempting to affect the behavior both of consumers and of the website industry. As discussed in Part I, the agency early on made efforts to educate the public about industry uses of their personal data, maintained a website that provided information, as well as tools, to assist consumers who wished to be proactive in seeking their own privacy, and held workshops to get industry representatives and privacy advocates together.[132]

---

129. 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 has jurisdiction over website activities without a change in the intellectual property status of personal data.

130. The FTC cites consumer preference studies to bolster its claims regarding the public's desire to maintain privacy online. *Fair Information Partners in the Electronic Marketplace: Hearing Before the Senate Comm. on Commerce, Science, and Transportation*, 106th Cong. (2000) (prepared statement of the FTC noting that 92% of consumers are concerned about misuse of their personal information and 62% are "very concerned"), *available at* http://www.ftc.gov/os/2000/os/testimonyprivacy.htm.

131. *§ 809: "Online Privacy Protection Act of 1999": § 2606 "Consumer Privacy Protection Act," § 2928 "Consumer Internet Privacy Enhancement Act": Hearing Before the Senate Comm. on Commerce, Science and Transportation*, 106th Cong. (2000) (FDCH testimony arguing Americans believe they own their personal data).

132. At the 2000 *Computers, Freedom & Privacy* conference, a Novell representative who is in charge of worldwide privacy compliance for Novell explained that engineers by training build databases that are capable of gathering as much information as possible, whether this be personal data or data of some other sort, even if the narrow purposes for which the databases are created do not require such comprehensiveness. As she explains it, part of her job has been simply to educate the company's large number of engineers worldwide that more data, per se, is not better. Thus, while education alone cannot change the basic fact that most websites may have a dominant preference to disrespect consumer privacy concerns, nevertheless, education may be able to irradicate unnecessary data collection. *Commissioned Research Confirms Privacy is a Key Issue Influencing Consumer Acceptance*

The FTC appeared, however, to have reached the conclusion that these educational efforts by themselves, were not enough. Rather, they must be coupled with incentives to change the payoff structure of current norms, such that cooperation would come to promote the self-interest of websites. The FTC integrated its education and incentive approaches in the following manner. First, it began educating the website industry about the agency's expectations regarding an adequate degree of respect for privacy in more concrete terms, by proffering the so-called "fair information practice principles" ("FIPPs"). Second, the FTC issued threats to change the incentive structure faced by the website industry. The fair practice principles are discussed in the following section. The FTC's use of threats to incentivize websites to adopt these norms will be examined in the section following that.[133]

1. The Issuance of Fair Information Practice Principles

The following list sets out the fair information practice principles promoted by the FTC.

The FTC's Fair Information Practice Principles

1. The Notice/Awareness principle
2. The Choice/Consent principle
3. The Access/Participation principle
4. The Integrity/Security principle
5. The Enforcement/Redress principle

These five principles are best understood as second-order norms, as they are susceptible to a number of colorable concrete interpretations. The

of Internet Billing; Gallup Poll Uncovers Opportunities to Build Consumer Confidence in 2001 by Implementing Best Practices for Online Privacy, PR NEWSWIRE, Jan. 16, 2001.

133. The FTC has become the leading website privacy norm entrepreneur. While diverse instances of norm entrepreneurs are found in the legal literature, there are only a few instances of governmental entities discussed as norm entrepreneurs. In its everyday use, the word "entrepreneur" applies to someone in business, usually a principal in the business. Government agencies, however, are not in business. In what sense, then, may they function as entrepreneurs? By the lights of economic analysis, all actors are entrepreneurs in the sense that all actors seek to maximize something, whether it be a private firm seeking to maximize profit or a public-interest privacy advocate seeking to maximize the aggregate level of individual privacy throughout society. The core assumption is that actors are rational and that rationality demands that the actor act so as to maximize that which the actor values, its utility function. In the context of live persons, economics generally conceives of actors seeking to maximize their self-interest, welfare or happiness. Firms are thought to aim at maximizing profit. Governmental agencies are often conceived by economists as seeking to maximize size and power of the agency. *See* Hetcher, *supra* note 13.

FTC contends that these principles would be promoted best by their incorporation into website "privacy policies." Consider first the basic characterizations of these principles and then their relationship to privacy policies.

The FTC considers the Notice/Awareness principle to be the most fundamental. According to this principle, consumers must be given notice of a company's information practices before personal information is collected from them. The scope and content of the notice may properly vary with a company's substantive information practices, but the notice itself is essential, as the other core principles have meaning only if a consumer has notice of an entity's information practices and his or her respective rights.[134]

The Choice/Consent principle requires that consumers be given options with respect to whether and how personal information collected from them may be used. The Access/Participation principle requires that consumers be given reasonable access to information collected about them and the ability to contest that data's accuracy and completeness. The Integrity/Security principle requires that companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use. Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of the Enforcement/Redress principle, which requires that governmental and/or self-regulatory mechanisms impose sanctions for noncompliance with fair information practices.[135]

The FTC calls these five principles "fair information practice" principles. The FTC says nothing of a substantial nature, however, to explain how each of the principles promotes fairness.[136] Nor is it at all intuitively

134. 1999 FTC REPORT TO CONGRESS, *supra* note 4, at 3; Robert MacMillan, *Congress to Air Public Concerns Over Privacy*, NEWSBYTES, Sept. 5, 2000 (arguing that privacy advocates are split with some advocating very strong privacy protections).

135. The European Union ("EU") has recognized that self-regulation may in certain circumstances constitute "adequate" privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking "adequate" safeguards. *See* Privacy Directive, *supra* note 21, art. 25. The EU has noted, however, that non-legal rules such as industry association guidelines are relevant to the "adequacy" determination only to the extent they are complied with and that compliance levels, in turn, are directly related to the availability of sanctions and/or external verification of compliance. *See* European Commission, Directorate General XV, *Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?* (1998), *available at* http://www.europa.eu.int/comm/dg15/en/media/dataprot/wp7.htm.

136. Elsewhere, I argue that there is a compelling public choice explanation for the FTC's shoehorning of the panoply of activities into single normative notion of fairness, which is that doing so allows the FTC to exert jurisdiction over the growing area of public concern. *See* Hetcher, *supra* note 13. If the agency is thought of as a business, it can be seen as having executed a heads-up strategic play to move onto the Internet. And unlike many

clear what fairness requires when it comes to the collection and use of personal data by websites. The industry has complained, for example, that it is held to a higher standard than off-line firms. Despite this ambiguity, the agency has provided little guidance as to the standards of fairness it intends to apply in determining which websites might fall below an acceptable level of fairness.

It appears, however, that the FTC has been reluctant to bring enforcement actions against websites for simple non-consensual data gathering or use.[137] This is likely due to the fact that the activities of websites are, facially at least, legal. It is not illegal to collect data from consumers and use this data in a variety of ways, such as by selling it, while never informing the data subject, much less seeking explicit consent. Thus, the situation is one in which the data-collection activities of websites are legal, on the one hand, but unfair by the lights of the fairness norms articulated by the FTC, on the other hand. Unwilling or unable to bring enforcement actions based on current website practices, the FTC

---

businesses currently facing this task, the FTC did not need to cannibalize from its traditional base, as it continues to regulate in the non-virtual world as well.

137. Lawsuits filed so far have involved more than simple unconsented data collection and use. *See* Diane Anderson & Keith Perine, *Privacy Issue Makes DoubleClick a Target*, INDUSTRY STANDARD (Feb. 3, 2000), *available at* http://www.thestandard.com/article/display/0,1151,9480,00.html; Jeri Clausing, *Privacy Adovcates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000, at C2; Will Rodger, *Activists Charge DoubleClick Double Cross*, USAToday.com (Feb. 21, 2000), *available at* http:// www.usatoday.com/life/cyber/tech/cth211.htm; *Privacy on the Internet*, N.Y. TIMES, Feb. 22, 2000, at A26; *see also* Complaint filed In the Matter of DoubleClick, Inc. (F.T.C. Feb. 10, 2000) (alleging violations of the FTC Act prohibiting unfair or deceptive acts or practices in or affecting commerce in its alleged practice of using cookies to create profiles of Internet users in contradiction of its stated privacy policy), *available at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Complaint filed in Donaldson v. DoubleClick, Inc. (S.D.N.Y. Feb. 1, 2000) (No. 00-Civ.-0696) (seeking class action status while alleging violations of federal Electronic Communications Privacy Act and other federal statutes, deceptive advertising under New York law, and common law unjust enrichment and invasion or privacy, for DoubleClick's alleged practice of using cookies to create profiles of Internet users in contradiction of its stated privacy policy); Complaint filed in Healey v. DoubleClick, Inc. (S.D.N.Y. Jan. 31, 2000) (No. 00-CIV.-00641) (seeking class action status while alleging violations of federal Electronic Communications Privacy Act and other federal statutes, deceptive advertising under New York law, and common law unjust enrichment and invasion of privacy, for DoubleClick's alleged practice of surreptitiously using cookies to create profiles of Internet users); Complaint filed in Judnick v. DoubleClick, Inc. (Marin Cty. Sup. Ct. Jan. 27, 2000) (No. CV-421) (seeking private attorney general status while alleging state law claims of unfair business practices and false and misleading advertising by DoubleClick for its alleged practice of using cookies to create profiles of Internet users in contradiction of its stated privacy policy), *available at* http://www.perkinscoie.com/resource/ecomm/netcase/complaint1.pdf; Pamela Parker, *DoubleClick's Legal Troubles Deepen*, Internet News (Feb. 4, 2000), *available at* http://www.internetnews.com/bus-news/article/0,1087,3_299771,00.html.articles; Sandeep Junnarkar, *DoubleClick Accused of Unlawful Consumer Data Use*, CNET News.com (Jan. 28, 2000), *available at* http://www.cnet.com/news/0-1005-200-1534533.html.

devised a plan to issue threats in order to cause websites to be more solicitous of their users' privacy, despite the fact that the websites' behavior was not illegal.

2. Creating a New Game Through Threats

In 1998, the FTC threatened the website industry that it would recommend that Congress enact privacy legislation if more respectful industry customs and usages were not forthcoming through industry self-regulation. The threat was highly credible and particularly salient, due to the Commission's recent success in influencing legislation to protect children's online privacy.[138] This threat was a shock to the normative equilibrium of the website industry, causing many firms to alter their behavior. Generally, the impact of the FTC's threat correlated with website size and structure, the larger and more multi-faceted a website's activities, the more likely it was that the website had reason to react to the FTC's threat by seeking to provide more respectful privacy practices. In fact, some large sites apparently felt so threatened that they took it upon themselves to incentivize smaller sites into compliance with more respectful norms.

In modeling the shift in norms that occurred, there are three relevant time periods to consider: 1) the time prior to FTC's threat, 2) the time after the FTC's threat, and 3) the time after the large websites began threatening the small websites. The strategic structure faced by the website industry in each of these time periods will be modeled with three informal, game-theoretic payoff matrices.

Attention will be focused on the FTC's main policy initiative during this period, which was to encourage websites to adopt "privacy policies," or "privacy statements." As already mentioned, the FTC apparently viewed privacy policies as the most effective means to implement fair information practice principles. According to the FTC, all the fair

138. In 1998, after finding self-regulation of children's online privacy to be inadequate, the FTC recommended to Congress that it enact legislation, which Congress quickly did, enacting the Children's Online Protection Act. On October 21, 1998, the President signed into law the Children's Online Privacy Protection Act of 1998 ("COPPA"). Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, PUB. L. 105-277, 112 Stat. 2681, 2681–287 (codified at 15 U.S.C. §§ 6501–6506) (October 21, 1998), *reprinted at* 144 CONG. REC. H11,240–42 (Oct. 19, 1998). The stated goals of the Act are: (1) to enhance the parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of online fora for children such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent. 144 CONG. REC. S12,741 (1998) (Statement of Sen. Bryan).

information practice principles can be promoted in a privacy policy.[139] A privacy policy that accurately and completely stated the site's personal data practices would be an instantiation of the key principle of notice/awareness. Once the consumer has notice of the website's practices, she can consent to the data exchange or exit the site. In addition, stipulations concerning access/participation to the user's personal data on file with the site can be set out in the privacy policy, as can stipulations concerning integrity/security and enforcement/redress.

Payoff matrix Three below represents the strategic situation faced by a particular representative website, A, *vis-à-vis* the rest of the website industry, with regard to two alternative website industry practices: one in which privacy policies are the industry custom and practice, and the other in which they are not. This situation, then, is a particular instantiation of the general coordination game faced by the website industry *vis-à-vis* respect for privacy, *tout court*, as represented in Figure 2 above.

FIGURE 3:
WEBSITE INDUSTRY BEFORE THREAT

		Website Industry	
		Privacy Policy	No Privacy Policy
Firm A	Privacy Policy	2,2	1,3
	No Privacy Policy	3,1	4,4

Note that in the southeast cell, which represents the situation in which no site provides a privacy policy, A receives 4, her highest payoff. Failing to provide a privacy policy gives A greater flexibility. The site can experiment with various business plans that use personal data in different ways, without having to worry that doing so violates previous representations made in the site's privacy policy. If the site seeks to take advantage of new opportunities that make use of new forms of personal data that happen to be available to it as a by-product of its interaction with users,

139. *Could Try Harder: Protecting Privacy on the Internet*, THE ECONOMIST, May 27, 2000 (noting that only 20 percent of websites collecting personal information implement all of the fair information practice principles—leaving the FTC to argue that if implemented the principles would be effective. The FTC recommends Congress establish some basic privacy rules and give the FTC the power to implement these rules); *see also* Nancy Weil, *FTC Says Internet Privacy Legislation is Not Needed-Yet*, INFOWORLD DAILY NEWS, July 13, 1999, *available at* 1999 WL 10504347.

the site will not need to first notify the user and seek consent. And, of course, nor will it need to offer some new consideration to the user in return for its use of the new data. These are significant benefits of avoiding privacy policies. The FTC is wrong to suggest that these concrete benefits would be outweighed by an amorphous and speculative promise of greater consumer willingness to participate in electronic commerce.

Next, consider the situation once the FTC promulgates the fair information practice principles.

FIGURE 4:
WEBSITE INDUSTRY WITH FAIR
INFORMATION PRACTICE PRINCIPLES

		Large Websites	
		Privacy Policy	No Privacy Policy
Small Websites	Privacy Policy	1,2	1,1
	No Privacy Policy	2,2	2,1

In this situation, large websites do better for respecting privacy than not respecting privacy, regardless of what the small or medium websites do. They receive 2, representing their most preferred outcome, in the northwest and southwest cells. They receive the same payoff in each of these boxes, indicating their relative indifference to the actions of the small and medium websites. It is enough for each of the large sites that it individually benefits from conforming. This is plausible as these sites are prominent and they would run the risk of coming under FTC scrutiny for questionable, albeit legal, trade practices, were they to fail to make a respectable effort to show respect for user privacy, as newly spelled out by the FTC, in its fair information practice principles.

In contrast, small websites would plausibly have a dominating preference to not provide privacy policies. Because they are small, they will be able to fly under the FTC's radar. The FTC merely has outlined the principles that it contends are fair. It did not mandate them. Accordingly, the small sites receive a higher payoff in either of the southern cells, as compared to the northern cells. Note that the southwest cell is an equilibrium, that is, given the choices of others, no actor could unilaterally have done better. Thus, the situation in which large websites respect privacy and small sites do not, will tend to be stable.

Consider next the situation in which the FTC issues its threat to the website industry. The major websites are no longer indifferent to the actions of the smaller sites, for the failure of these sites to adopt privacy-respecting practices might lead to privacy legislation, which would adversely affect all websites, but particularly the large sites, as they have the most to lose from onerous legislative requirements. The major online firms are mega-corporations with some of the largest market capitalizations in history. The strategic situation once the industry-wide threat is in place is represented in the following payoff matrix:

FIGURE 5:
WEBSITE INDUSTRY AFTER FTC THREAT

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

Note that there is no longer a stable equilibrium in this situation. Large sites most prefer the northwest cell while small sites prefer the southwest cell. In contrast to the previous situation, as represented in Figure 4, the large sites now prefer that the small sites respect privacy. This is because the FTC has made it clear that it expects industry-wide improvement and that if this is not forthcoming, a statute will be forthcoming. Thus, the large sites now prefer the northwest to the southwest cell. For any particular small site, however, it will still prefer to defect in order to reap the benefits of unrestrained data collection and use. If the larger sites become more respectful of privacy, this may serve a particular small site's interests as there will be less pressure from the FTC on the website industry generally. But the small site will nevertheless do better still if it can successfully free ride on this public good. Thus, the small website's highest payoff comes in the southwest cell, in which it does not provide a privacy policy but the large websites do.

Faced with this situation, large sites devised a means to bring small sites into conformity with more respectful data collection practices. Large sites began threatening to withhold advertising from sites that did not

demonstrate adequate respect for privacy.[140] This is apparently contributing toward the desired result as an increasing number of small sites are now offering privacy policies. Indeed, as indicated by the FTC's 1999 Report to Congress, website provision of privacy policies has gone up significantly. Regarding the issuance of threats by large websites, the FTC writes:

> Companies like IBM, Microsoft and Disney, which have recently announced, among other things, that they will forego advertising on sites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues.[141]

The FTC, then, is able to indirectly promote its goal of data privacy by getting large websites to do its bidding.

Note that when large websites threaten to withhold advertising from small sites, the effectiveness of the threat does not depend on repeated interaction between the parties. Even if the small websites only interact once with Microsoft or IBM, they will typically prefer that this interaction allow for advertising rather than that it not. In the terminology of informal game theory then, the instrumental allocation of advertising is functioning like a "selective incentive" that rewards cooperative behavior on an individual basis.[142] Selective incentives allow the party seeking to incentivize conformity to be able to provide incentives to individuals in order to elicit their conformity. This is in contrast to the collective good itself, which, by definition, has the feature that the good is public, that is, when provided for one, it is provided for all, and thus is open to free riding.

Note that this type of selective incentive cannot be expected to work for all small sites. Some small sites will have little prospect of receiving advertising revenue from large sites and may stand to benefit significantly from the unfettered use of personal data. These sites may continue to have a dominating preference to free ride on the growing practice of providing privacy policies. The net result of the threats instigated by the FTC and carried forward by the large sites, then, is a bi-normative world in which large sites and some small sites are respectful of privacy while other small sites are not. The important and difficult issue, then, for future scholarship on website privacy norms is whether and how additional small sites might come to show greater respect for privacy.[143]

---

140. 1999 FTC REPORT TO CONGRESS, *supra* note 4, at 12–13.

141. *Id.*

142. MANCUR OLSON, THE LOGIC OF COLLECITVE ACTION (1965).

143. Recently, software vendors have begun marketing so-called "privacy-solutions." For example, Zero-Knowledge Systems lets Internet users surf the net anonymously. *See Tech Leaders of the Year; They're Young; They're Aggressive; They're Taking on the World.*

CONCLUSION

This article has developed a case study of the emergence of website privacy norms. In the short history of the Internet, there has been a major shift—a norm cascade—toward norms that are more respectful of privacy and more efficient. The transition has been from a wild-west world in which websites acted with near impunity in collecting whatever personal data they could, to a world in which a significant percentage of websites are explicitly addressing privacy concerns.

Like other case studies in the law and norms tradition, the goal here has been two-fold. First, to utilize a theoretical framework to model a complex and important social phenomenon, namely, the evolving relationship between websites and their visitors *vis-à-vis* data privacy. Second, to learn more about the theory of law and norms itself, by coming to better understand its powers and limitations in an important applied context. In particular, the most significant theoretical feature of the foregoing account was the study of the complex and complimentary roles played by various norm entrepreneurs.

Part I first looked at the original privacy norms that emerged at the Web's inception in the early 1990s. Two groups have been the main contributors to the emergence of these norms; the thousands of commercial websites on the early Web, on the one hand, and the millions of users of the early Web, on the other hand. The norms originally created by the interaction of websites and consumers had the problem that they created significant negative externalities for consumers, as commercial websites were rampantly extracting personal data with little or no concern for the

---

And They're Just Getting Started, PROFIT, Nov. 2000, at 73; *see also Company Chosen from Elite Group of Industry Players to Present Its Internet Privacy Solution*, PR Newswire, Oct. 27, 2000. Privacy Solutions typically come in the form of software that users, websites, or both can install in order to create a more private online environment. John Graubert & Jill Coleman, *Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet*, 25 CAN. U.S. L.J. 275, 290 (1999) ("In the case of Internet privacy, several technologies potentially capable of protecting the online privacy of consumers are evidently already on the market or under development. Technology-based privacy solutions may eventually provide consumers with the confidence and security that they need to conduct business on the Internet on a global scale."); ZDWIRE, *P3P: Just a Start*, 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."). There may remain websites that are not reachable. But if there are a small enough number of such sites, this may be an acceptable level of defection from acceptable norms. The hardest sites to reach are those that can completely externalize costs to consumers. These would be sites that would not have repeated interactions with the same consumers and ones that would be able to avoid reputational costs. For consumers might not even go to the site in the first place, if the site's reputation was bad and widely known.

privacy interests of their visitors. Part I then examined the strategic structure of the relationships between websites and consumers which permitted these highly exploitative norms to develop. Consumers were seen to face a large-scale collective action problem. There is a collective good that consumers could potentially achieve, namely, the abatement of disrespectful data-collection practices by websites. But consumers were not in a position to organize in order to secure this collective good, due to their large numbers, lack of repeat play and overlapping relationships. Not surprisingly, then, the original website data-collection norms did not take account of the privacy interests of website users.

Reacting to this undesirable social situation from the perspective of consumers, "norm entrepreneurs" entered the picture to promote website norms that would better serve consumers' privacy interests. Part II examined how improved website privacy norms have recently emerged, due to the efforts of a number of different norm entrepreneurs. The activities of these norm entrepreneurs were broken down into two main stages. In the first stage, the privacy advocacy community and the website industry battled to define the appropriate set of aspirational norms that each group thought should govern website/consumer interactions. The privacy advocacy community applied its pre-existing second-order norms of data privacy to the context of Internet websites. In response, the Website industry entered the arena in order to promote a competing set of norms that were loss demanding on the industry. In the second stage, the FTC was seen to adopt a set of privacy norms based on those proposed by the competing norm entrepreneurs discussed in Stage One. The FTC then used threats to induce websites to adopt these norms. The FTC created a large-scale collective action problem for the website industry, where none has existed before. It did this by creating a collective good that the industry would be interested to promote: the avoidance of Congressional legislation. The agency threatened to push for legislation unless the industry demonstrated greater respect for privacy.

In a later Stage-Two development, some of the large sites in turn threatened to withhold advertising from smaller sites with whom they did business if these sites were not more respectful of consumer privacy. The result of this network of threats by the FTC and large websites was the emergence of a new social equilibrium in which there was no longer a uniform norm of disrespect for privacy as existed in Stage One, but instead a bi-normative world in which numerous sites continued to conform to disrespectful practices while many other sites adopted more respectful practices. The emergence of the bi-normative equilibrium created favorable conditions for a new stage, which is beginning to develop. In this stage, software firms have begun to sell "privacy solutions" to websites

concerned to signal to consumers their respect for consumers' privacy, in the hope that consumers will thereby give the sites their business. This third stage is newly emerging and quickly gaining momentum.

It is important that we continue to make efforts to better understand how privacy norms are emerging. First, we need to see if we can continue to make progress in producing better website practices through predominantly informal means. While there have been significant improvements to date, the current situation is unsatisfactory. By better understanding the processes that have worked thus far to promote website privacy, we will be in a better position to see if more progress may still be made, either through previously utilized methods, or through new ones. With Congress poised to act, it is important that we achieve this clarity now. In particular, if better norms are already emerging through informal social processes, and minimalist governmental guidance, there may not be a need for sweeping legislation of the sort currently being proposed by many privacy advocates.