UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 5

Fall 2000

The De Facto Federal Privacy Commission, 19 J. Marshall J. Computer & Info. L. 109 (2000)

Steven Hetcher

THE *DE FACTO* FEDERAL PRIVACY COMMISSION

by STEVEN HETCHER†
Vanderbilt Law School

I. INTRODUCTION

This article addresses the issue of whether the United States Congress should create a federal agency to regulate online privacy. In this article, I seek to establish that the United States is already well on its way to having such an agency, albeit not by name. In the last five years, the Federal Trade Commission (FTC or Commission) has executed a strategy of increasingly assuming jurisdiction over online privacy. The FTC has been subtle in its actions; it has quietly positioned itself to gain jurisdiction, all the while "talking the talk" of industry self-regulation.

The FTC's true intentions became apparent in the summer of 2000, when the Commission recommended to Congress that it enact new federal legislation to codify and strengthen the FTC's growing *de facto* regulation of Internet privacy.[1] The FTC took this action despite the fact that it was relatively successful in motivating the Web site industry to adopt more respectful privacy practices.[2] Thus, rather than asking whether the United States should create a federal privacy agency, one might instead ask what should rightfully befall the *de facto* privacy agency that already exists. Should Congress increase or decrease the FTC's role in regulating Internet privacy? Or alternatively, if there is a need for regulation at all, should the FTC share regulatory responsibility with another agency or agencies? These questions are especially ripe because the next Congress will consider new privacy legislation.

---

† I am grateful to John Goldberg and Robert Rasmussen for comments and to Catherine Hora for her expert research assistance. The ideas in this article were first presented at a symposium on Internet privacy at the John Marshall Law School. An extended analysis of the arguments contained herein is forthcoming in the Michigan Telecommunications and Technology Law Review.

1. *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, i (F.T.C. May 2000) [hereinafter FTC 2000 Rpt.].

2. *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 Vand. L. Rev. 2041 (2000).

Part One below will provide a brief background on how informational privacy has come to be a key policy issue of the digital age. Part Two will then tell the story of how the FTC has managed to insinuate itself as the leading federal regulator of Internet privacy.

II. BACKGROUND

To fully understand the FTC's actions, it is necessary to have an appreciation of the factual situation that the FTC encountered in the mid-1990s, when it first became involved in regulating privacy. The first subpart below describes the original environment of the early Internet in terms of the data-collection practices of Web sites and their impact on the personal privacy of Web site visitors. The second subpart examines the strategic structures of these practices in order to understand the hurdles faced by the FTC in seeking to increase its regulation of Web site data-collection activities.

A. UNRESTRAINED PERSONAL DATA-COLLECTION BY WEB SITES

Two events in the 1990s set in motion the series of developments that would lead to the FTC's involvement in regulating privacy. The first was the invention of the World Wide Web (Web) in the early 1990s by Tim Berners-Lee.[3] Once the core features of the Web were in place, the Internet became dramatically easier to use, and Web sites sprouted up like dandelions. These were not electronic-commerce sites, however, since the National Science Foundation did not then permit commercial use of the Internet.[4] The Web was not available for consumers until the Bush Administration zoned the Internet as commercial.[5] This rezoning of cyberspace is the second event that precipitated the entrance of the FTC, as commercial Web sites have been the main users of personal data collected under questionable circumstances. The FTC may regulate commercial enterprises for privacy violations under its unfair trade practices jurisdiction.[6]

Early commercial Web sites collected personal data in two ways: first, by simply asking for the data, and, second, by collecting data produced as a by-product of Web site/consumer interactions, such as when consumers provided their credit card numbers or mailing addresses to sites. Each of these initial means of data collection was soon improved upon by Web sites.

---

3. Tim Berners-Lee & Mark Fischetti, *Weaving the Web: the Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (Harper SanFrancisco 1999).

4. Stephen Segaller, *Nerds 2.0.1: A Brief History of the Internet,* 224-25 (1st ed., TVBook 1998).

5. *Id.* at 297.

6. *See* 15 U.S.C. §45(a) (1994).

Regarding explicit requests for data, Web sites began conditioning full access to their sites on the provision by Web site 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, Web sites soon began to deploy sophisticated technological means of data gathering, such as "cookies."[7]

Cookie technology allows a Web site's server to place information about a consumer's visits to the site on the consumer's computer in a text file that only the Web site's server can read. In the early period especially, Web users were typically unaware of the fact that data about them was being gathered, because cookies were planted stealthily and subsequently operated seamlessly.[8] In other words, there was no bargain between the parties; the data was simply spirited away.[9]

When using cookies, a Web site assigns each consumer a unique identifier,[10] so that the consumer may be recognized in subsequent visits

---

7. Stacee Barcelata, *How Cookies Work*, PC Magazine Online, <http://www.zdnet.com/pcmag/ventures/cookie/cksl.htm> (accessed July 4, 2000). *See* Sen. Subcomm. on Commun. of the Comm. on Com., Sci., and Transp., (July 27, 1999) (Prepared state. of the F.T.C. on "self-regulation and privacy online") (F.T.C. June 1998) (available in 1999 WL 550985) 45-46 n.4 [hereinafter FTC 1998 Report]. The report reveals a shortage of social scientific information about cookie use. In its survey of Web sites, the FTC staff did not ascertain whether sites in fact use cookies, or other hidden electronic means, to collect personal information, but looked instead to sites' information practice disclosures. This reveals merely what sites choose to disclose regarding their data-collection practices. *Id.*

8. *See* Lawrence Lessig, *Code: And Other Laws of Cyberspace*, 34-42 (1999).

9. *See* Andrew L. Shapiro, *Privacy For Sale: Peddling Data on the Internet*, 26 Human Rights L. J. 10 (1999); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 Chi.-Kent L. Rev. 1257, 1276 (1998). Lemley discusses distribution of incentives as an explanation for the failure of adequate disclosure of data-collection practice by Web sites. *Id.*

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

Id.

10. 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. *See e.g.* H.R. Subcomm. on Courts and Intell. Prop., Comm. on the Jud., *Oversight Hearing on Electronic Communications Privacy Policy Disclosures,* 106th Cong. (May 27, 1999) (test. of Marc Rotenberg) (discussing how privacy advocates have been concerned about unique identifiers even when connected to machines and not individuals). *Id.* Recently, both Intel and Microsoft have made efforts to tie numbers to names. *See* Don Clark & Kara Swisher, *Microsoft to Alter Windows 98 so Data About Users Won't Be Sent to Company,* Wall St. J., Mar. 8, 1999 (available in 1999 WL-WSJ 5443409) (discussing Microsoft's efforts to use hardware identification numbers to collect personal information). Edward C. Baig, et. al., *Privacy: The Internet*

to the site.[11] In this manner, the site engages in passive tracking of the consumer.[12] On each return visit, the site can call up user-specific information, which will typically 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.[13] Cookies make it easier for firms to engage in highly targeted marketing.[14] Accordingly, cookie data 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 their visitors' interests, but also permits companies to boost their revenues by selling advertising space on their Web sites.[15]

The vast majority of commercial Web sites use their interactions with consumers as an occasion to collect personal data about these consumers.[16] The connection between the collection of personal data and

---

Wants Your Personal Info. What's In It for You?, Bus. Week, Apr. 5, 1999 (available in 1999 WL 8226796); Robert Lemos, *The Biggest Computer Bugs of 1999*, ZDNet, Dec. 23, 1999 (available in 1999 WL 14538475) (discussing Intel's Pentium III serial number, global unique identifiers, and two Microsoft products, Office 97 and Windows 98, that attempted to match various numbers to personal information and names). *See also* Pls. Compl. In the Matter of Intel Pentium III Processor Serial Number, Case No. 982 (FTC 1999) <http://www.cdt.org/privacy/issues/pentium3/990226intelcomplaint.shmtl> (seeking to prevent Intel Pentium III processors from being shipped with a processor serial Number that could be used to compromise users online privacy).

11. *See e.g.* Rivka Tadjer, *Following the Patron Path*, ZD Internet Magazine 95 (Dec. 1997). An industry has emerged to market a variety of software products designed to assist Web sites in collecting and analyzing visitor data and in providing targeted advertising. Thomas E. Weber, *Software Lets Marketers Target Web Ads*, Wall St. J., Apr. 21, 1997, at B1.

12. FTC 1998 Report, *supra* n. 7, at 56 (defining "passive tracking" as information collected by using navigational software.)

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

14. Forester Research, Inc., *Media & Technology Strategies: Making Users Pay*, 4-6 (1998).

15. *See generally* FTC 1998 Report, *supra* n. 7. While America businesses have always collected some information from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. *Id.* It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns. *Id.* 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 W. Huber, *Dig More Coal — The PCs are Coming*, Forbes (May 31, 1999) <http://www.forbes.com/forbes/99/0531/6311070a.htm> (accessed Sept. 1, 2000). Strikingly, 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." *Id.*

16. *See* FTC 1998 Report, *supra* n. 7, at 20. The report describes the various types of information collected by Web sites. *Id.* Two categories of personal information exist. *Id.* The first is data used to identify consumers, such as name, postal or e-mail address ("personal identifying information."). *Id.* The second is data consisting of "demographic and

personal privacy is straightforward; the more personal data that Web sites collect, store, and use, the less privacy that data subjects have. This reduction in privacy may be justified if data subjects agree to exchange their personal information for something they prefer more. Typically, however, personal data is simply taken by Web sites without the subject's knowledge or consent.[17]

The reasons why commercial Web sites behave in this morally dubious but commercially reasonable manner are twofold and straightforward: first, personal data is not owned and, hence, it is not unlawful to collect it without consent; and, second, in the new digital economy, personal data is gold.[18] Given these facts, one cannot be surprised that commercial Web sites, profit maximizers that they are, collect and use as much personal data as possible and at a growing rate.[19]

The resulting norms of the Web site industry admittedly have a certain attractiveness, as Web sites take something from the public domain that was under-utilized and put it to productive use. After all, personal information is a type of data, and the Supreme Court has said that data, as such, is not subject to copyright protection.[20] Rather, data are simply

---

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." *Id.* 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.

17. Anne Wells Branscomb, *Who Owns Information?* 3-4 (Basic Books 1994). The author describes how personal information is being sought for marketing purposes. *Id.* Information considered to be highly personal, such as names, telephone numbers, marital status, academic accomplishments, job and credit histories, even medical records, is being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. *Id.* Such transactions occur without our knowledge or consent. *Id.*

18. *See Online Privacy*, Bus. Week (Mar. 20, 2000) (available in 2000 WL 7825258) (comparing the stockpiles of information to an Internet gold rush); *see also* 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 in 2000 WL 3481300) (stating "personal information is like gold," especially to "get paid to surf," profiling Web sites that entice Internet users to give up information about themselves for rewards); Kathryn Kranhold & Michael Moss, *Companies Are Refusing to Share Their Cookies Tracking Devices' Consumer Data Is Too Precious*, Chi. Trib., (Apr. 10, 2000) (available in 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); Maureen S. Dorney, *Privacy and the Internet*, 19 Hastings Commun. & 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).

19. *See* Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 No. 5 Computer Law (May 1999) (finding commercial activity involving personal data growing at rapid pace).

20. *See Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 359 (1991). Law regarding personal data, indeed all data, is at sea. *Id.* Some commentators have argued

facts that in general should be left in the public domain—the commons—so that they are available for all to use.[21]

Like campers in a wooded area who collect fallen branches for use in their campfires, Web sites, on this view, are simply making use of a common resource that would otherwise be left in an unproductive state. As soon as this comparison is made, however, a salient difference comes to mind: no one suffers a loss when downed wood is burned; whereas, when personal data is used, data subjects may suffer harm in a variety of ways. These injuries may be the result of actions that are criminal or depraved, such as is the case with identity theft,[22] or predation on chil-

---

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). The author advocates statutory recognition of property rights in a "persona" consisting of personal information about the individual. *Id.* Further, heightened intellectual property status for personal data would be a means to greater privacy protection. *Id.* Kenneth C. Laudon, *Markets and Privacy*, Comm. ACM, at 92 (Sept. 1996). Property rights in personal data as a way to protect privacy. *Id.* There are First Amendment tensions with this sort of proposal, however. For a discussion of the First Amendment and privacy, *compare* Paul M. Schwartz, *Free Speech vs. Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 Stan. L. Rev. 1559, 1560 (2000), *with* Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1051 (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. *Id. See* Ira V. Heffan, *Copyleft: Licensing Collaborative Works in the Digital Age*, 49 Stan. L. Rev. 1487, 1492 (1997) (commenting on 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 also* David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Technology and Freedom?* (Addison-Wesley 1998) (arguing that personal data should be subject to open-access rules).

21. *See* Lessig, *supra* n. 8; Steven Hetcher, *Climbing the Walls of Your Electronic Cage*, 98 Mich. L. Rev. 801, 814 (2000). Lawyers are just beginning to grapple with special issues raised by the digital commons.

22. *See e.g.* Jared Sandberg, *Losing Your Good Name Online*, NEWSWEEK, Sept. 20, 1999. Identity theft occurs when one person intentionally assumes another person's online identity. *Id. See* Sen. Subcomm. on Tech., Terrorism and Govt. Info., *The Prepared Statement of the Federal Trade Commission on "Identity Theft,"* 105th Cong. (May 20, 1998) (State. of David Medine, Assn. Div. for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission). *Identity Theft and Assumption Deterrence Act*, 18 U.S.C. § 1028(a) (Lexis 2000). The Act imposes a penalty of 15 years imprisonment and fines for theft of personal information with intent to commit an unlawful act. *Id.* In addition, the FTC indicated the seriousness of the problem and has recently appointed a person to handle the issue. *Id. See* Kurt M. Saunders & 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 of invasion of financial privacy); *Laracuente v. Laracuente*, 599 A.2d 968, 968-969 (Sup. Ct. N.J. 1991) (showing typical social security number identity theft). *Id.* Thus far, identity thieves have typically

dren, respectively.[23] Alternatively, these decisions may be the foreseen but unintended consequences of everyday business decisions by online firms, such as the decision to use personal medical data in making hiring decisions.[24]

Due to a torrent of media exposure, there is a growing public awareness of the data-collection practices of the Web site industry and the ramifications of these practices for personal privacy.[25] By some ac-

---

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. *Id.*

23. *See* FTC Public Workshop on Consumer Information Privacy: Hearings Before the Federal Trade Commission (July 11, 1997) at 229 (test. of Linda Hooper, FBI agent). In the past, children have been especially vulnerable to the online criminal element. *Id.* The FBI and Justice Department's "Innocent Images" investigation has revealed that online services and bulletin boards are quickly becoming the most powerful resources used by predators to identify and contact children. *Id. See also* Sen. Appropriations Subcomm. for the Depts. of Com., J., and St., the Jud., and Related Agencies, 105th Cong. (March 10, 1998) (test. of Louis J. Freeh, Director, Federal Bureau of Investigation) <http://www.fbi.gov/congress/internet/sac310.htm> (accessed Sept. 1, 2000); H.R. Subcomm. on Crime, *Oversight Hearing on Combating Crimes against Children Facilitated by the Internet*, (test. of Stephen R. Wiley, Chief, FBI Violent Crime and Major Offenders Section) <http://www.fbi.gov/congress/children/children.htm>; *See Public Workshop on Consumer Information Privacy* (June 12, 1997) [hereinafter FTC Workshop]. Further, anecdotal evidence indicates that many children surfing the Web claim to have experienced problems such as attempted password theft and inappropriate advances by adults in children's chat rooms. *Id.*

24. *See* Jane Birnbaum, *Look Into It Here's How to Protect Your Medical Records*, Chi. Trib., (Nov. 23, 1999) (available in 1999 WL 2935001). One-third of Fortune 500 companies use personal medical information in hiring, promotion, or termination decisions. *Id.* David F. Linanes & Ray Apencer, *How Employers Handle Employees' Personal Information Report of a Recent Survey*, 1 Empl. Rts. & Empl. Policy J. 153 (1997). This has the significant policy consequence that many people are failing to seek medical diagnosis and treatment. *Id.*; *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."). Subcomm. on Health of the Comm. on Ways and Means, *Patient Confidentiality* (Mar. 24, 1998) (test of Janlori Goldman, Health Privacy Project Institute for Health Care Research and Policy, Georgetown Univ.):

> In the absence of such trust, patients will be reticent to accurately and honestly disclose personal information, or they may avoid seeking care altogether for fear of suffering negative consequences, such as embarrassment, stigma, and discrimination. Along the continuum, if doctors and other health care providers are receiving incomplete, inaccurate information from patients, the data they disclose for payment, research, public health reporting, outcomes analysis, and other purposes, will carry the same vulnerabilities.

Id.

25. *See e.g. The End of Privacy,* Economist 21 (May 1-7, 1999) (covering privacy degradation in online environment); Jared Sandberg, *Identity Thieves Online*, Newsweek (Sept. 20, 1999); Adam Penenberg, *The End of Privacy: I Know What You Did Last Night*, Forbes (Nov. 29, 1999).

counts, this awareness may already come too late. In a now famous remark, Scott McNealy, CEO of Sun Microsystems, advised the public, "You already have zero privacy—get over it."[26] More accurately, however, our privacy is not yet gone, but it is being rapidly degraded. Fortunately, public awareness of this degradation has precipitated public outrage.[27]

In response to the public outcry over online privacy, the United States Congress is showing increased interest in enacting omnibus legislation on the issue.[28] In deference to the general ethos of self regulation which has characterized the Internet, Congress has held back on new regulations.[29] This situation is now changing, as a number of bills are

---

26. John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. Times, at A5 (Mar. 3, 1999). McNealy's remark is self serving, given that it was made at the launch of Jini software, which raised privacy concerns because it enabled all electronic devices to interconnect using an identification number. *Id.* One can imagine McNealy making a similar statement—one appropriately toned down—as a defendant in a civil suit, or as a witness in a congressional hearing, with the implicit message that if privacy is gone already, Sun Microsystems cannot be accused of its further destruction. *Id.*

27. *See generally* FTC 1998 Report, *supra* n.7. Opinion polls show increasing public concern with respect to online privacy. *Id.* A recent U.S. Business Week/Harris Poll found that 92% of Internet users were uncomfortable about Web sites sharing personal information with other sites. *Id.*

28. *See* Hetcher, *supra* n. 21, at 814. More narrow legislation has already been enacted. *Id.*

29. *Self Regulation and Privacy Online: A Report to Congress, Federal Trade Commission* (July 1999) <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (accessed Sept. 1, 2000) [hereinafter FTC 1999 Report]. The Commission has stated that, "self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology." *Id. see e.g.* Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. Pitt. L. Rev. 993, 1054 (1994). 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." *Id.* 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. *Id.* As a general rule, "self-governance is desirable for electronic communities." *Id.* 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. *Id.* Henry H. Perritt, Jr., *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?*, 12 Berkeley Tech. L.J. 413, 419-20 (1997); *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* <http://www.eff.org/~barlow/DeclarationFnal.html> (accessed Jan. 28, 2000); *see also* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *Borders In Cyberspace* 129 (Brian Kahin & Charles Nesson eds., 1997) (discussing the Internet's "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

working their way through Congress.[30]

In the previous discussion, we saw that despite the growing public perception of Internet privacy as a policy concern, nevertheless, there was restraint exercised on the part of lawmakers, due to the ethos that the Internet should be self regulated. Whether privacy regulation was needed was in part influenced by the likelihood that the privacy situation would be susceptible to self regulation.[31] Different industries and different issues are differentially susceptible to self regulation.[32] For example, the securities industry has long been involved in self regulation. In the case of online privacy, the Internet industry was not left completely on its own to self regulate. Rather, the FTC has sought to provide general guidance to Web sites. This guidance still allows room for Web sites to continue to develop their own data-collection practices. For the FTC to shape Web site practices, the agency must understand the strategic structure of these practices. In the following discussion, the strategic structure of the key practices will be examined.

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."[33] Judging by these remarks, the FTC thinks that it would be in the interest of the Web site industry to be more solicitous of user privacy concerns, in order to bring about greater user trust, which in turn would lead to a more robust online marketplace. On this understanding, the Web site industry has a "collective action problem."[34] When other firms respect consumer privacy, consum-

---

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.").

30. There are currently a number of bills before Congress protecting consumer's privacy on the Internet. One such bill, sponsored by Senator John McCain, is the "Consumer Internet Privacy Enhancement Act." S. 2929, 106th Cong. (2000) (the bill requires websites to provide consumers with notice as to how personal information will be used and an opportunity for the consumers to limit how this information is used). *See also Online Privacy Protection Act of 2001* H.R. 89, 107th Cong. (2001) (requiring the FTC to prescribe regulations to protect the privacy of individuals not protected by the Children's Online Privacy Protection Act of 1998).

31. *See supra* n. 28, and accompanying text.

32. *See supra* n. 23, and accompanying text.

33. Fed. Trade Comm'n, *1998 Report To Congress* (1998) 3. Test. and State. for the Rec. of Marc Rotenberg, Dir. Elec. Pri. Infor. Ctr., Oversight Hrg. on Elec. Commun. Priv. Policy Disclosures, before the Subcomm. on Courts and Intell. Property, Comm. of the Jud., U.S. House of Rep. (May 27, 1999). *Id.* "Users of web based services and operators of web based services have a common interest in promoting good privacy practices. *Id.* Strong privacy standards provide assurance that personal information will not be misused, and should encourage the development of online commerce." *Id.*

34. *See* Garrett Hardin, *The Tragedy of the Commons,* 162 Science 1243 (1968).

ers will be less fearful of the Internet and consequently more prone to participate in electronic commerce. This will make it possible for a particular Web site to "free ride" on the respectful practices of other Web sites.

The problem is that the same possibility of free riding is open to other Web sites as well and each Web site has a preference to free ride. Each Web site would like all the other sites to be respectful so that it alone can take advantage of trusting consumers. The overall result is that an industry norm of disrespect for privacy will prevail, as individually maximizing behavior leads in the aggregate to a collectively suboptimal result; this is the classic collective action problem.[35]

Note, however, that the above analysis is based on the assumption of the FTC that the Web site industry would achieve such great gains through increased e-commerce that it is actually in the interest of the various individual Web sites to bring about more respectful privacy norms (if they could just solve their collective action problem). Contrary to this assumption, 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 Web sites. For small sites the very act of creating privacy policies creates a cost that may be significant.[36] For large sites, these development costs are of marginal importance. But sites of large companies face a much larger cost, the increased exposure to litigation they face as a result of making explicit privacy guarantees to their Web site visitors by means of the posted privacy policies. Even if there is some marginal increase in their online traffic due to heightened consumer trust, it is reasonable to think that these sites would forego this benefit in order to avoid exposure to legal liability.[37] Thus, both small and large Web sites prefer not to provide

35. FTC 1998 REPORT, *supra* note 7. Based in part on its survey of over 1,400 commercial Web sites, the FTC 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." *Id.*

36. 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.

37. *See* Sara Robinson, *CD Software Is Said to Monitor Users' Listening Habits*, N.Y. Times CyberTimes <http://www.nytimes.com/library/tech/99/11/biztech/articles/o/real.html> (Nov. 1, 1999). For example, RealNetworks recently admitted that its RealJukebox assigned a personal ID number to users and uploaded information about their listening habits to its servers. *Id. See RealNetworks Is Target of Suit in California Over Privacy Issue*, N.Y. Times CyberTimes <http://www.nytimes.com/library/tech/99/11/biztech/articles/09real.html> (Nov. 9, 1999) . The company was subsequently slapped with a $500 million class action lawsuit for violating California's unfair business practices law. *Id.* A second class action suit filed in Pennsylvania one day later. *Id.*

greater privacy protections. They do not have a collective action problem of the sort described by the FTC.

B. Web Site Industry Coordination Game

As the following discussion demonstrates, the strategic structure faced by the Web site industry with regard to collection of personal data is actually that of a coordination game.[38] A coordination game is a practice in which each conformer receives a "coordination benefit," which is the added benefit received for conformity, given the conformity of other participants.[39] A coordination game may have a structure of an "equilibrium," a "coordination equilibrium" or a "proper coordination equilibrium."[40]

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, even though the actor prefers its choice to other choices the actor might have made, 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. With a proper coordination equilibrium, other conformers receive a benefit when a particular actor conforms. Thus, conformers may sanction one another for nonconformity because it is in the interest of others that each conform. The sanctions are meant to ensure the conformity of others.

The original Web site data-collection practices appear to be a proper coordination equilibrium, as particular Web sites have an interest in the conformity of other Web sites. Web sites care that other Web sites conform for two reasons. First, Web sites will be able to more successfully collect data when consumers are left in the dark. Thus, all Web sites will be hurt to the extent that a particular Web site takes it upon itself to be more forthcoming in telling consumers about its data-gathering activities, because the greater the public awareness of Web site data-gathering activities in general, the more likely it is for any particular Web site that

38. *See infra* § III C.

39. *See* Steven Hetcher, *Creating Safe Social Norms in a Dangerous World*, 73 S. Cal. L. Rev. 1, 43-45 & n.n. 161-68 (1999) (offering a more general definition than that of Ullmann-Margalit or David Lewis).

40. *See id* at 35, 44. *See generally* David Lewis, *Convention* (1969); Edna Ullmann-Margalit, *The Emergence Of Norms* (1977). *See also* Margaret Gilbert, *Game Theory and Convention*, 46 Synthese 41 (1981). The economics literature on "network externalities" encompasses a similar but broader rational structure as not all networks with significant externalities are norms. *Id.*

it will be made to feel public pressure to alter its practices in the direction of greater respect.

The second reason why Web sites prefer that other Web sites conform to disrespectful privacy norms is that in privacy law, reasonable expectations of privacy matter.[41] An action in tort for invasion of privacy may be brought in civil litigation by aggrieved parties. In such cases, a central consideration is whether the plaintiff had a reasonable expectation of privacy.[42] This comes down to a determination of extant practices. If most Web sites are collecting data at will with no safeguards and no notice, then the tortfeasor will have a colorable defense based on the claim that the plaintiff did not have a reasonable expectation of privacy.

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.[43] Note that the Web site industry coordination norms function efficiently from a point of view internal to the conformers themselves. The harm resulting from the practices—the degradation of personal privacy—is successfully externalized onto the Web-surfing public.

Because Web site practices are bad for Web users as a group, however, there is the potential for these users to secure an important collective good, the abatement of disrespectful data-collection practices.[44] Data subjects will face a collective action problem in seeking as a group to bring about the collective good of more respectful Web site privacy policies, however, as contributions to the joint effort will entail costs to individuals. Thus, we come to the surprising result that while the Web site industry does not face a collective action problem, the users of their Web sites do. Given the fact that the group of Web users is large and diffused, it is unlikely that they could solve this collective action problem.

---

41. *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) (noting that "[a]ssurances of privacy protection by e-commerce vendors and Internet service providers demonstrate that the commercial side of the Internet recognizes that respect for privacy is a significant expectation of Internet users.").

42. *See Katz v. U.S.*, 389 U.S. 347 (1967) (holding that a violation of the Fourth Amendment does not involve simply a physical trespass, but implicates a reasonable expectation of privacy).

43. *See generally* Hetcher, *supra* note 39 at 17.

44. *See* Ullmann-Margalit, *supra* n. 40. The classic norm-emergence account emphasizing that the first step is to identify underlying social situations in which an emergent norm would promote efficiency. *Id.*

Summing up, this subsection looked at the strategic situations faced by two different groups: Web sites and Web site visitors. First, we saw that the FTC engaged in wishful thinking in supposing that the Web site industry faces a collective action problem with respect to increasing the level of respect for consumer privacy in order to stimulate greater electronic commerce. Second, we saw that Web sites are best analyzed as conforming to coordination norms that provide them with a safe harbor from the demands of privacy advocates. Finally, we saw that consumers face a large-scale collective action problem in attempting to shape industry norms more in their favor. Accordingly, there is reason to think Web sites will maintain their coordination norms, despite the fact that these create harm to consumers. Understanding the strategic structure of the practices of Web sites and consumers will be the key to understanding the actions taken by the FTC to guide the Web site industry in the direction of more respectful practices.

III. ARGUMENT

A. THE FTC USES THREATS TO GUIDE INDUSTRY SELF REGULATION

In 1995, the FTC was asked by Congress to investigate the privacy risks associated with computer databases. The agency has been increasingly involved ever since.[45] The FTC acts pursuant to its authority under section 5 of the Federal Trade Commission Act, which mandates that the agency address unfair and deceptive trade practices.[46] Generally speaking, then, the FTC's hook into the privacy debate comes by means of casting Web site data-gathering practices as potentially unfair and deceptive.[47]

The FTC does not justify its involvement by means of moral arguments grounded in the proposition that privacy is a fundamental human right that must be protected. Rather, it is because consumers strongly feel entitled to data privacy that the FTC claims it is moved to action.[48] In other words, it is the existence of a strongly held community norm

45. *See* Hetcher, *supra* n. 2.

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

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

48. The FTC cites consumer preference studies to bolster its claims regarding the public's desire to maintain privacy online. The FTC does not discuss the peculiarity that in

that pulls the initial causal levers leading toward greater consumer online privacy protection.

The FTC promotes more respectful Web site privacy norms by attempting to affect the behavior both of consumers and of the Web site industry. First, the agency has sought to educate the public about what is occurring with respect to their personal data. The agency maintains a Web site that provides information as well as tools to assist consumers who wish to be proactive in seeking their own privacy. In addition, it has held numerous workshops to get industry representatives and privacy advocates together.

The FTC has also made efforts to educate the Web site industry. A critic of the FTC's approach might claim that the FTC's efforts at educating the online industry are naïve. The industry has all the information it needs; what it lacks is the motivation to show respect. In other words, the industry's interest is in easy access to personal data, and this is in opposition to consumer privacy. Hand wringing over the need for better education simply papers over this fundamental tension. This is incorrect, however. There is genuine room for norm education, although it must be coupled with some incentive to change the payoff structure of the practices, such that cooperation comes to promote the self interest of Web sites.[49] The FTC utilizes both approaches. First, it educates the Web site industry about the agency's expectations regarding an adequate degree of respect for privacy. In concrete terms, this amounts to the agency's articulation of and support for fair information practice principles. Second, the FTC issues threats to change the incentive structure faced by the Web site industry. The fair practice principles are discussed in the following subsection. Subsequently, the FTC's use of threats will be examined.

B. The Issuance of Fair Information Practice Principles

The following list sets out the privacy principles promoted by the FTC.

The FTC's Fair Information Practice Principles ("FIPPs") are:

1. The Notice/Awareness Principle
2. The Choice/Consent Principle

---

other contexts, a mere desire for control of property in the public domain does not create entitlement to control this property.

49. 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 simply been to educate the company's large number of engineers worldwide that more data, *per se*, is not better.

3. The Access/Participation Principle
4. The Integrity/Security Principle
5. The Enforcement/Redress Principle

The FTC contends that these principles would be best promoted by their incorporation into Web site privacy policies. According to studies performed by the FTC, these principles, under any reasonable interpretation, fail to be fully instantiated in the practices of most Web sites.[50]

The FTC considers the Notice/Awareness Principle to be the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. According to the agency, 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.[51]

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.

In principle, all of the fair information practice principles can be promoted in a privacy policy. A privacy policy that accurately and completely states the site's personal data practices would be an instantiation of the principle of notice/awareness. Once the consumer has notice of the Web site's practices, she can consent to the exchange or exit the site. Access/participation to one's personal data on file with the site can be promised in the privacy policy, as can guarantees to integrity/security and enforcement/redress.

In reflecting on the FIPPs, one might reasonably wonder why they are characterized as "fair" information principles. Here, the FTC engages in persuasive definition, as it is certainly not obvious what fairness requires in terms of Web site behavior, and the FTC says nothing of a substantial nature to explain how each of the principles promotes fairness. In general, other proponents of online privacy have not reduced

50. *See generally* FTC 2000 Report, *supra* n. 1.
51. FTC 1999 Report, *supra* n. 28, at 3.

the Web site privacy debate down to a concern for fairness per se. The likely explanation has to do with the fact that section 5 of the FTCA allows the FTC authority over "unfair" trade practices.[52] Thus, by characterizing Web site activities in terms of fairness and unfairness, the FTC is attempting to shoehorn the Web site privacy debate more squarely into the agency's jurisdictional purview.[53]

The agency has provided little discussion to elucidate what standards of fairness it applies in determining which Web sites might fall below an acceptable level of fairness.[54] Based on its actions or inactions, rather, it is evident that the FTC is reluctant to bring an enforcement action against a Web site for simple unconsented-to data gathering or use. This may be due to the fact that the activities of Web sites 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.[55]

---

52. 15 U.S.C. § 5 (1994).

53. *See* Hetcher, *supra* n. 39, at 17.

54. In general, the FTC explicates fairness, for enforcement purposes, in general terms.

55. *See* Diane Anderson & Keith Perine, *Privacy Issue Makes DoubleClick a Target*, Industry Standard <http://www.thestandard.com/article/display/,1151,9480,00.html> (Feb. 3, 2000). Lawsuits filed so far have involved more than simple unconsented data collection and use. *Id. See also* Will Rodger, *Activists Charge DoubleClick Double Cross*, USAToday.com <http://www.usatoday.com/life/cyber /tech/cth211.htm.> (Feb. 21, 2000); Jeri Clausing, *Privacy Adovcates Fault New DoubleClick Service*, N.Y. Times, at C2 (Feb. 15, 2000); *Privacy on the Internet*, N.Y. Times Feb. 22, 2000. *In the Matter of DoubleClick, Inc.*, Fed. Trade Com. at A26 <http://www.epic.org/ privacy/internet/ftc/DCLK_ complaint.pdf> (filed Feb. 10, 2000). The complaint alleges violations of the FTCA 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. *Donaldson v. DoubleClick*, No. 00-Civ.-0696 (S.D.N.Y. 2000). The complaint alleges 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 using cookies to create profiles of Internet users in contradiction of its stated privacy policy. *Id.* It seeks class action status. *Id. See also DoubleClick's Legal Troubles Deepen* <http://www.internetnews.com/bus-news/article/ 0,1087,3_299 771,00.html> (Feb. 4, 2000) (discussing *Donaldson v. DoubleClick* and *Healey v. DoubleClick*, alleging violations of the federal Electronic Communications Privacy Act and other federal statutes, deceptive advertising under New York law, common law unjust enrichment and invasion of privacy for DoubleClick's alleged practice of using cookies to create profiles of Internet users in contradiction of its stated privacy policy and also seeks class action status). *Healey v. DoubleClick*, No. 00CIV.00641 (S.D.N.Y., 2000). The complaint alleges violations of the 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, and seeks class action status. *Id. Judnick v. DoubleClick*, No. CV-421 (Marin Cty. Sup. Ct., 2000) (copy available in <http:// www.perkinscoie.com/resource/ ecomm/netcase/ complaint1.pdf>). The complaint alleges

Thus, the situation is one in which the data-collection activities of Web sites are legal, on the one hand, but unfair by the lights of the criteria articulated by the FTC, on the other hand. This unfairness apparently does not rise to a level, however, at which the FTC is willing to engage in enforcement actions. Instead, the FTC issued threats in order to cause Web sites to be more solicitous of their users' privacy.

C. CREATING A NEW GAME THROUGH THREATS

In 1998, the FTC threatened to recommend to Congress that it enact privacy legislation if more respectful industry customs and usages were not forthcoming through industry self regulation.[56] The threat was highly credible and particularly salient due to the Commission's recent success in influencing legislation.[57] This threat had a tremendous impact on the Web site industry, causing many firms to alter their behavior. The impact of the FTC's threat appears to correlate with Web site size and structure. Generally, the larger and more multi-faceted a Web site's activities, the more likely it is that the Web site will have reason to react to the threats by seeking to provide more respectful privacy practices.

In modeling the strategic structure of the practices at issue, 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

---

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 and seeks private attorney general status. *Id.*

56. *See generally* Hetcher, *supra* n. 2. There is a compelling public choice explanation for the Commission's activity, which is that by channeling disputes that arise when companies and consumers interact into a contract paradigm, the FTC thereby enhances its jurisdiction. *Id.*. 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. *Id.* Unlike many 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. *Id.*

57. *See e.g. The Children's Online Privacy Protection Act*, 15 U.S.C. §§ 6501- 6506, PUB. L. 105-277, 112 Stat. 2681, 2681-287 (codified at 15 U.S.C. §§ 6501-6506) (Oct. 21, 1998), (reprinted in 144 Cong. Rec. H11240-42) (Oct. 19, 1998). 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 (COPPA). *Id.* On Oct. 21, 1998, the President signed COPPA into law. *Id.* Title XIII, *Omnibus Consolidated and Emergency Supplemental Appropriations Act*, 1999. The stated goals of COPPA are: (1) to enhance the parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children online for a 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. *See also* 144 Cong. Rec. S12741 (Oct. 7, 1998) (Stat. of Sen. Bryan).

Web sites threaten the small Web sites. The strategic structure of each of these time periods will be modeled in the following three game payoff matrices below. Attention will be focused on the FTC's main initiative, the provision of privacy policies, or privacy statements, by Web sites. The following matrix of four possible sets of payoffs characterize the strategic situation faced by a particular representative web site, "A," vis-à-vis two alternative Web site industry practices, one in which privacy policies are the industry custom and practice, and the other in which they are not.

		Web Site Industry	
		Privacy Policy	No Privacy Policy
Firm A	Privacy Policy	3,3	4,1
	No Privacy Policy	1,4	2,2

Figure 1: Web Site Industry Before Threat

Note that in the southeast cell, each party receives 2, her second most preferred outcome.[58] This compares favorably with the outcome for each in this type of situation, as characterized by the FTC under its set of assumptions, as discussed earlier. With Figure 1 above, each actor prefers that all other actors fail to cooperate, rather than that all cooperate. Thus, the noncooperative outcome in Figure 1 is not Pareto inferior to the cooperative solution whereas, under the FTC's earlier assumption, it would be Pareto inferior.

Failing to provide a privacy policy gives the sites much greater flexibility. They can experiment with various business plans that use personal data in different ways, without having to worry that doing so violates previous representations made to the site's users. If the site seeks to take advantage of new opportunities that make use of personal data, they do not need to first acquire the data from the data subject. These are significant benefits of avoiding privacy policies. They are surely not outweighed by an amorphous and speculative promise of greater consumer willingness to participate in electronic commerce, as is sometimes assumed by the FTC.

Next, consider the situation in which the FTC has promulgated the fair information practice principles.

In this situation, large web sites do better for respecting privacy than not respecting privacy, regardless of what the small or medium Web sites do. They receive 1, representing their most preferred outcome,

58. The numbers in the payoff matrix represent the ordinal preferences of the players ("1" represents a player's most preferred outcome and "4" represents a player's least preferred outcome.)

		Large Web Site (IBM, Microsoft & Disney)	
		Privacy Policy	No Privacy Policy
Small & Medium Web Sites	Privacy Policy	3,1	4,2
	No Privacy Policy	1,1	2,2

Figure 2: Web Site Industry After Announcement of Fair Information Practice Principles

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 Web sites. It is enough for each of the large sites that it individually benefits from conforming. This conclusion is plausible. These sites are prominent and they run the risk of coming under FTC scrutiny for questionable, albeit legal, trade practices, were they to fail to make a reasonable effort to show respect for user privacy, as newly spelled out by the FTC, with its fair information practice principles.

In contrast, the small and medium Web sites retain a dominating preference to not provide privacy policies. They receive a higher payoff in either of the southern cells (1 over 3, in the southwest, as compared to the northwest cell, and 2 over 4, in the southeast as compared to the northeast cell, respectively).

In addition, the small and medium Web sites are not neutral as to what the large Web sites do. Rather, it is plausible to suppose that they prefer that the major sites conform to privacy respecting practices, as this will be conducive to favorable conditions for smaller sites, as there will both be less public clamoring for greater privacy protection, and more personal data available for the taking, due to fewer takers and a more trusting public. Accordingly, the payoff for smaller sites is higher in the southwest as compared to the southeast cell, that is, 1, as compared to 2. Note that the southwest cell is an equilibrium for both the large sites and the small and medium sites, that is, given the choices of others, no one could unilaterally do better.[59]

Consider next the situation in which the FTC issues a threat to the Web site industry. The major Web sites 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 Web sites, but particularly the large sites, as they have the most to lose from onerous legislative requirements. This new strategic situation is represented in the following payoff matrix. Note there is no longer a stable equilibrium in this situation. Large sites most prefer

59. When it is possible for players to do better and no one to do worse, the change in situation would be Pareto superior.

the northwest cell while small and medium sites prefer the southwest cell. In contrast to the previous situation, as represented in Figure 2, the large sites now prefer that the small and medium 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.

		Large Web Site (IBM, Microsoft & Disney)	
		Privacy Policy	No Privacy Policy
Small & Medium Web Sites	Privacy Policy	3,1	4,3
	No Privacy Policy	1,2	2,4

Figure 3: Web Site Industry After FTC Threat

Faced with this situation, large sites devised means to bring small and medium sites into conformity with more respectful data collection practices. Most important, large sites are threatening to withhold advertising from sites that do not respect privacy.[60] This is having the desired result, as an increasing number of small and medium sites are offering privacy policies.[61] Indeed, as indicated by the FTC's 1998 Report to Congress, Web site provision of privacy policies has gone up dramatically.

We see, then, that the FTC is able to indirectly promote its goal of data privacy by getting large Web sites to do its bidding. In the case of the threat by large Web sites to withhold advertising, there is no dependence on repeat interaction. Even if the small Web sites only interact once with Microsoft or IBM, they will typically prefer that this interaction allow for advertising rather than that it not. The instrumental allocation of advertising is functioning like a selective incentive that rewards cooperative behavior on an individual basis.[62]

Summing up then, we saw that the FTC was able to incentivize large Web sites such as IBM and Disney to be significantly more respect-

60. FTC 1998 Report, *supra* n. 7. 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." *Id.*

61. *Id.* The FTC writes: "These types of business-based initiatives are critical to making self-regulation meaningful because they can extend the reach of privacy protection to small and medium-sized businesses where there is great potential for e-commerce growth." *Id.*

62. Mancur Olson, *The Logic Of Collective Action* (1965). Selective incentives allow the party seeking to incentivize conformity to be able to provide incentives to individuals in order to elicit their conformity. *Id.* 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. *Id.*

ful of consumers' online privacy by making it in their interest to be respectful of privacy. The FTC was able to change the payoffs for large sites by threatening them with the prospect of congressional action. We saw that the FTC's actions had the effect of changing the strategic situation faced by a segment of the Web site industry from a large-scale coordination game to that of a collective action problem. But this left a large number of sites still interested in following less respectful practices. For a number of these sites, however, it nevertheless came to be in their interest to be more respectful of privacy. They will wish to conform to the more respectful practices in order to stay in the good graces of the larger sites, which threaten to withhold advertising if more respectful behavior is not forthcoming. Other sites, however, will have little prospect of receiving advertising revenue from large firms and may stand to benefit significantly from the use of personal data.

Thus, there may still be a significant number of sites that do not find it in their interest to respect consumer privacy. The net result of this network of threats instigated by the FTC and carried forward by the large sites, then, is a bi-normative world in which some sites are privacy respecting while others are not. The important and difficult issue is whether and how the latter sites might come to show greater respect for privacy. Very recently, a large number of these sites do appear to be adopting more respectful privacy practices.[63] The question posed for norms theory, then, is what theoretical account best explains this new spread of norms.

D. Additional Web Sites Respond to New Privacy Equilibrium

The key to understanding the expanding emergence of more respectful privacy practices is to see how the world changes even for those Web sites not immediately affected by the twin-fold regime of threats just discussed. As already mentioned, due to the regime of threats, there has been a movement from a uni-normative world of disrespect for privacy to a bi-normative world in which one set of norms is more respectful to data privacy than the other set. This creates a choice for consumers that did not exist before.

Other things equal, consumers who value privacy will protect it by using privacy-respecting sites over non-respecting sites whenever possible. If consumers begin to pay increased attention to privacy in making decisions regarding their Web use, Web sites that formerly were not interested in engaging in respectful practices may come to be more interested in promoting privacy in order to adjust to shifting consumer

63. FTC 1998 Report, *supra* n. 7.

demand.[64] A cost to the company of conforming is the foregone benefit from using personal data as they please. The benefit is more consumers and more pleased consumers, or, at any rate, consumers who do not spurn them in favor of more respectful sites. Thus, to the extent that Web sites are capable of providing privacy to consumers in a cost-effective manner, they will do so.

In addition, there appears to be a causal feedback loop in operation whereby as more respectful practices have begun to emerge, consumers have become more informed of the issue of online privacy, and so more demanding of their privacy interests. In a criminal law context, Kahan observes the phenomenon whereby a rise in crime makes social sanctions less powerful, which makes crime rise again. In this situation, the causal feedback loop leads to normative breakdown. McAdams sets out a similar example involving norms pertaining to wearing fur and smoking cigarettes. He plausibly observes that these are activities in which the more people who shun the behavior, the more negative is the impact that will be felt by those remaining participants in the activity. A parallel situation appears to pertain to Web sites. The fewer the number of sites that fail to provide privacy policies, the more intense will be the perception that these sites are disrespectful of the interests of their users. This in turn causes Web sites to be more intent on appearing or actually being respectful. The end result is that for many sites, the newly emergent bi-normative world provides a background against which it may now make sense to be more respectful of privacy than existed previously. In other words, due to the norm shock introduced by the FTC, these sites will be caught up in the resulting norm cascade.

IV. CONCLUSION

In the short history of the Internet, there has been a major shift—a norm cascade—toward norms that are more respectful of privacy. The transition has been from a Wild West world in which Web sites acted with near impunity in collecting whatever personal data they could, to a world in which a significant percentage of Web sites are explicitly addressing privacy concerns.

Part One of the article 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

64. As consumer demand for privacy grows, the threat and the consequences of lawsuits grow. Matt Fleischer, *Lawyers Eye Privacy Cases Against Many DoubleClick Rivals*, 22 Natl. L.J. 27, A1 (Feb. 28, 2000) (noting many lawyers are now searching for the next privacy lawsuit against DoubleClick competitors, such as Engage, 24/7 Media, Open Vertical, MatchLogic, Flycast, and L90, each collecting over 100 Mbytes of clickstream-data information per day).

thousands of commercial Web sites 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 Web sites and consumers had the problem that they created significant negative externalities for consumers, for commercial Web sites were rampantly extracting personal data with little or no concern for the privacy interests of their visitors.

Part One then examined the strategic structure of the relationships between Web sites and consumers that allowed these highly exploitative norms to flourish. Consumers face a large-scale collective action problem. By the light of standard game theory, this is precisely the type of collective action problem that is most difficult to solve. There is a collective good that consumers could potentially achieve, namely, the abatement of disrespectful data-collection practices by Web sites, but consumers will have great difficulty in organizing to secure this collective good, due to their large numbers and lack of repeat play or overlapping relationships. Not surprisingly, then, the original Web site data-collection norms did not reflect the privacy interests of Web site users.

Reacting to this sub-optimal social situation, the FTC promoted the fair information practice principles. The FTC then used threats to induce Web sites to adopt these principles. The FTC created a large-scale collective action problem for the Web site industry, where none had 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. Some of the large sites in turn threatened to withhold advertising from smaller sites with whom they do business, if these sites were not more respectful of consumer privacy. The result of this network of threats by the FTC and large Web sites is a new situation in which there is no longer a uniform norm of disrespect for privacy as existed in Stage One, but instead a bi-normative world in which numerous sites conform to disrespectful practices while many other sites conform to more respectful practices. On the whole, this represents a significant increase in the degree to which Web sites are subject to governmental regulation with regard to their data-collection practices. Accordingly, the FTC is fairly viewed as a nascent, *de facto* federal privacy commission.