Privacy

The FTC's Role in Privacy Protection:

Implications for Food & Beverage Marketing

Paul M. Schwartz
University of California, Berkeley

Daniel Solove
George Washington University

Memo prepared for
The Second NPLAN/BMSG Meeting
on Digital Media and Marketing to Children

for the NPLAN Marketing to Children Learning Community

Berkeley, CA June 29 & 30, 2009

Sponsored by The Robert Wood Johnson Foundation

Introduction: The FTC as Enforcement Agency

Congress created the FTC in 1914 to prevent unfair methods of competition in commerce. The history of the FTC begins, therefore, in the Progressive Era and the battle during that time against trusts. The FTC is an independent agency with five Commissioners at its head. These commissioners are nominated by the President and subject to confirmation by the U.S. Senate.

In 1938, as part of the New Deal, Congress amended the FTC's enabling statute, the FTC Act, to include a broad prohibition against "unfair and deceptive acts or practices." As the FTC defines an "unfair or deceptive act or practice," it is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[1] This language proves to be of critical importance for the FTC's contemporary privacy enforcement actions.

When the FTC issues complaints or takes other legal action, it does so as a public law action, pursuant to the FTC Act or another statute that gives it an enforcement role.

The FTC's Regulation of Privacy

In 1995, Congress and privacy experts asked the FTC to take a role in consumer privacy issues. The FTC began to use its power to protect privacy in 1998. It has done so by maintaining that companies that violate their privacy policies are engaging in an "unfair or deceptive act or practice" under the FTC Act. The FTC also started to conduct a series of public workshops, and issued reports focusing on data collection practices and industry self-regulatory efforts. Two of the most important of the resulting documents are the FTC's report to Congress in 2000 about online profiling, and its February 2009 staff report about online behavioral marketing.[2] The FTC has also led a series of investigations and brought numerous law enforcement actions challenging company practices. Most of the FTC's enforcement actions have led to settlements.

In general, there are four statutory grounds for the FTC's authority to protect information privacy. The FTC typically acts in this area through: (1) its unfairness and deception power pursuant to the FTC Act; (2) statutory authority in the area of financial privacy pursuant to the Gramm-Leach-Bliley Act of 1999; (3) statutory authority in the area of credit reporting under the Fair Credit Reporting Act of 1970; (4) statutory authority in the area of children's online activities pursuant to the Children's Online Privacy Protection Act of 2000.

Non-governmental organizations (NGOs) have also played an important role in keeping pressure on the FTC to take action to promote privacy. In his comprehensive study, *The Privacy Advocates* (2008), Colin Bennett identifies a "loose and polycentric network" of privacy NGO's in the U.S. (2008).[3] These include the Center for Digital Democracy (CDD), the Electronic Privacy Information Center (EPIC), and the United States Public Interest Research Group (US PIRG), among others. According to Bennett, these advocates seek to (1) promote change by reporting facts (information politics); (2) draw on important symbols to connect with culture (symbolic politics); (3) force organizations to live up to their rules (accountability politics); and (4) embarrass organizations that fall short (leverage, or "naming and shaming" politics).[4]

FTC Privacy Enforcement Actions

For purposes of this memorandum, the FTC's enforcement actions in the privacy area can be classified as falling into four groups. These are cases involving (1) a failure to live up to a privacy policy, or promise; (2) an unfair practice in the use of personal information; (3) unreasonable data security followed by a data leak or breach; and (4) violations of the Children's Online Privacy Protection Act. The FTC has also engaged in enforcement actions involving violations of financial or medical privacy. These actions are pursuant to its authority granted by the Gramm-Leach-Bliley Act, or the Health Insurance Portability and Accountability Act (commonly known as HIPAA). Apart from their specific statutory claims, these FTC cases also generally involve claims under the first three categories above.

- ***Deception, or the "Broken Promise" Case.*** The FTC has maintained that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a *deceptive* practice under the FTC Act. These cases can be characterized as "broken promise" cases. In such an enforcement action, the FTC takes action once a company has made a specific assertion as to its privacy practices and then failed to live up to the claim.[5] If a company makes no claims as to its privacy practices, or only promises a low level of privacy, the FTC cannot make a claim of a deceptive practice.
- ***Unfair Practices.*** The FTC has also taken action against *unfair* practices. In these cases, the FTC first finds that a company engaged in a deceptive practice of the "broken promise" variety. The agency then argues that this deception was also an unfair practice. It defines this unfairness as constituted by a substantial injury that could not have been avoided by consumers and that was not outweighed by a countervailing benefit.[6]
- ***Unreasonable Data Security.*** The FTC has found that a failure to provide reasonable protection for sensitive consumer information is deceptive and unfair. In other words, *unreasonable* data security violates the FTC Act. There are also specific statutory and regulatory requirements in financial privacy law and health care law to provide reasonable security for personal information. The FTC's most prominent enforcement action is this area involved ChoicePoint, a national data broker. In settling these charges in 2006, ChoicePoint paid $10 million in civil penalties, which was the largest civil penalty in FTC history, and provided $5 million for consumer redress.[7]
- ***Children's Online Privacy Protection Act (COPPA).*** Finally, the FTC has been active in children's privacy areas pursuant to its statutory authority under COPPA. This statute requires that websites directed to children have a privacy policy and specifies elements of the required policy. It mandates that such websites "obtain verifiable parental consent" for the collection and use of personal information from children. COPPA also gives parents the right to refuse to permit a website operator to use or maintain personal information from the child in the future. The FTC has brought over a dozen COPPA enforcement actions.[8]

The FTC's Enforcement Toolkit and Role of Advocacy Organizations

In its privacy enforcement settlements, the FTC has employed a number of remedies. The privacy-promoting steps begin with the leveling of fiscal penalties. As noted above, for example, the FTC managed to collect a $10 million penalty and to have ChoicePoint set aside $5 million for consumers who could prove injuries from identity theft caused by the data breach in question. More recently, the FTC reached a $2.25 million dollar settlement with Caremark, which was alleged to have failed to protect the medical and financial privacy of its customers and employees. In the COPPA area, the trend has been for the FTC to issue larger fines. These include a $ 1 million penalty against Xanga in 2006, the largest FTC fine under COPPA, and a $400,000 fine against UMG recordings in 2004.

Many other settlements have involved far smaller amounts. For example, the FTC collected less than $10,000 in *In the Matter of Vision I Properties*.[9] This penalty represented merely a "disgorgement" of damages. The FTC considered the defendant, Vision I Properties, to have gained an unjust enrichment and therefore to be obligated only to surrender the profits improperly obtained.

In its settlement orders, the FTC has also required companies to take many types of actions other than paying fines or damages. For example, the FTC has made companies delete all personal information that it obtained in violation of the law, to stop making any further misrepresentations about privacy and security policies, and to notify customers whose information was collected unfairly. The FTC has ordered companies to provide consumers with clear written notice of its information practices. It has also required companies to maintain a comprehensive security program. In many instances, FTC settlements are accompanied by extensive compliance, reporting, and record-keeping obligations on defendants. These requirements can include outside biennial audits by independent professionals over a twenty year period.

Advocacy organizations have lodged complaints with the FTC and other public authorities, appealed to stockholders of companies, generated legislative attention and action on privacy issues, and initiated effective public campaigns.

As noted above, advocacy organizations have also played a significant role in keeping pressure on the FTC to promote privacy. These activities are often an important predicate to this agency's activities. Advocacy organizations have lodged complaints with the FTC and other public authorities, appealed to stockholders of companies, generated legislative attention and action on privacy issues, and initiated effective public campaigns. The CDD, in partnership at different times and in different contexts with EPIC and USPIRG, has helped spark FTC action. For example, the November 2006 CDD/USPIRG petition on behavioral advertising re-ignited the FTC's interest in the issue of privacy and online marketing.

The FTC and Online Behavioral Advertising: the FTC's 2009 Staff Report

In large part, for its consumer privacy enforcement, the FTC has served to bolster the "notice and choice" framework developed by proponents of self-regulation. As we discussed in our companion memo about the notice and choice approach, such an approach is the predominant way that companies protect consumer privacy – by providing notice about their privacy practices in a privacy policy and then by offering consumers some kind of "choice," often in the form of a right to opt out of certain information uses or transfers. The FTC has gone after companies that violate their privacy policies. Yet, it has generally failed to take a more proactive role in shaping the substance of people's information privacy rights.

Early on in its regulation of privacy, the FTC lobbied for greater powers so that it could move beyond merely enforcing business promises in privacy policies. For example, the FTC's 2000 report on online profiling recommended that Congress enact legislation that would "set out the basic standards of practice governing the collection and use of information online for profiling, and provide an implementing agency with the authority to promulgate more detailed standards … , including authority to enforce those standards."[10] Congress did not follow the FTC's recommendations, and the United States continues to lack a federal information privacy law.

During the Bush Administration, the FTC changed course in its public pronouncements. It took a strongly pro-self-regulation approach, becoming one of the leading proponents of self-regulation, the same position advocated by the companies the FTC was regulating.[11] As the New York Times concisely reported in a headline in October 2001, "F.T.C. Plans to Abandon New Bills on Privacy."[12] Such positions led to significant criticism of the FTC as being captured by industry.

Recent events and a new presidential administration signal that the FTC may take a more critical stance on self-regulation. The key question is whether the FTC desires to move beyond championing the self-regulation approach. The FTC's most recent report concerning online behavioral advertising sends mixed signals in this regard.[13] This report contained a useful exploration of how online behavioral marketing works. It also noted the difficulty of distinguishing between personal identifiable information (PII) and non-PII.[14] The 2009 Report also contained revised principles for industry self-regulation. The revised principles represent a tweaking of previous standards based in input from privacy advocates and industry. The revised principles require: (1) transparency and consumer control; (2) reasonable security and limited data retention for consumer data; (3) affirmative express consent from affected consumers for material changes to existing privacy promises; and (4) affirmative express consent to use of sensitive data for behavioral advertising.

Perhaps the most important part of the report is its conclusion, in which the staff warned, "Self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences."[15] The report also stated that the staff would continue over the next year to "evaluate the development of self-regulatory programs and the extent to which they serve the essential goals" of the principles. The report is also notable for two strong concurring statements that accompanied it.

In his concurring statement, then Commissioner, and now FTC Chairman, Jon Leibowitz warned that this report "could be the last clear chance to show that self-regulation can— and will— effectively protect consumer's

privacy in a dynamic online marketplace."[16] He also noted that he was "troubled about some companies' unfettered collection and use of consumers' 'sensitive data" – especially information about children and adolescents."[17] In his view, "Some data is so sensitive and some population so vulnerable that extra protection may be warranted."[18] In a second concurring statement, Commissioner Pamela Jones Harbour concluded that (1) "any legislation should be part of a comprehensive privacy agenda, rather than fostering the current piecemeal approach to privacy," and (2) "Self-regulation has not yet been proven sufficient to fully protect that interests of consumers with regard to behavioral advertising specifically or privacy generally."[19]

The FTC and Privacy Protection: A Turning Point?

Since 1995, the FTC's activities in the privacy area have been ongoing. In general, the FTC has been most active against companies that breach their privacy policies. It has, however, branched out from the "broken promise" cases as, for example, by playing a strong role in data security cases. Congress has also assigned it specific enforcement powers under certain statutes, such as the Gramm-Leach-Bliley Act and HIPAA.

Privacy advocates have generally been disappointed by the scope of its efforts. As an example, Joel Reidenberg complained in 2003, "Reliance on the FTC as a primary enforcer of citizen privacy is misplaced."[20] As he notes, "The prevention of privacy wrongs, and particularly the public wrongs, as such, is simply not part of the core mission of the FTC."[21] The FTC has many other regulatory issues that it must address, including antitrust, mergers, and issues in consumer protection other than privacy, such as debt collection. Consequently, the FTC has only limited resources to pursue its privacy enforcement cases.

The election of Barack Obama in 2008, and, more specifically, the selection of Jon Leibowitz as Chairman of the FTC may mark a turning point in the FTC's role as privacy enforcer. We have seen that Leibowitz in his concurring statement to the 2009 staff report warned about reaching the end of his trust in the effectiveness of self-regulation. More recently, in April 2009, Leibowitz told a financial regulation summit, "From my perspective, the industry is pretty close to its last clear chance to demonstrate" its ability to police itself.[22] Media reports on Leibowitz's selection as FTC Chairman have viewed this selection as a turning point for privacy. Thus, Advertising Age commented that this choice could "step up the FTC's aggressiveness in online privacy, behavioral marketing and in enforcement."[23]

The FTC now has a chairman who is skeptical of self-regulation and open to a new more aggressive and substantive approach toward protecting consumer privacy. Congress and the Presidential Administration might also be amenable to passing legislation to enhance the FTC's powers. A possible opening is also provided by some willingness of private sector companies to accept stricter privacy standards. As an example, AT&T has called for more transparency and consumer control in targeted advertising.[24] It remains to be seen, however, if more companies will share this stance. The coming months and years represent a potential window of opportunity in shaping the FTC's agenda and public positions regarding information privacy —as well as shaping new statutory powers and resources to enable the FTC to become more effective at protecting consumer privacy.

###

References

[1] FTC Act, 12 USC § 45(n).

[2] FTC, *Online Profiling: A Report to Congress, Recommendations* (Part 2) (July 2000); FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting and Technology* (February 2009) [hereinafter FTC Staff Report, *Online Behavioral Ads*].

[3] Colin Bennett, *The Privacy Advocates* 200 (2008).

[4] *Id.* at 96-128.

[5] Examples of the FTC's "broken promise" cases are: Premier Capital Lending (2009); In the Matter of Vision I Properties, 2005 WL 1274741 (F.T.C. 2005); FTC v. Toysmart.com, Civ. Action No. 00-11341-RGS (July 21, 2000); In re Liberty Financial Cos., No. 9823522, 1999 FTC LEXIS 99 (May 6, 1999).

[6] Examples of FTC cases involving an unfairness claim are: In Re Gateway Learning Corp., No. C-4120 (Sept. 10, 2004), and FTC v. ReverseAuction.com, Inc., No. 00-CV-32 (D.D.C. Jan. 6, 2000).

[7] Examples of FTC cases involving data security are: In the Matter of Caremark Corporation, FTC File No. 072 3119 (February 18, 2009); Premier Capital Lending, FTC File No. 0723004 (Nov. 6, 2008); and In Re ChoicePoint, FTC File No 052-3069 (Jan. 26, 2006).

[8] The FTC's COPPA cases include: Imbee.com, FTC File No. 072-308 (Jan. 30, 2008) (ND Cal. Case No CV-08-0639); Xanga, FTC File No. 062-3073 (Sept. 7, 2006) (SDNY Civil Action No.: 06-CIV-6853 (SHS); and UMG Recordings, FTC File No. 022 3272 (Feb. 18, 2004).

[9] In the Matter of Vision I Properties, 2005 WL 1274741 (FTC 2005).

[10] FTC, *Online Profiling, supra* note 2, at 6 (Part III. Recommendations).

[11] Christopher Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment* (2005), available at http://epic.org/reports/decadedisappoint.html.

[12] John Schwartz, *F.T.C. Plans to Abandon New Bills on Privacy*, N.Y. Times, C5 (Oct. 3, 2001).

[13] FTC Staff Report, *Online Behavioral Ads, supra* note 2.

[14] The FTC Report stated, "Staff believes that, in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data" *Id.* at 22-23. As an example, the Report noted that in many contexts, certain items of information which might be anonymous by themselves can be de-identified. *Id.* at 23.

[15] *Id.* at p. 47.

[16] Concurring Statement of Commissioner Jon Leibowitz, Regarding FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* 1 (Feb. 2009).

[17] *Id.* at 2.

[18] *Id.*

[19] Concurring Statement of Commissioner Pamela Jones Harbour, Regarding FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* 2 (Feb. 2009).

[20] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877 (2003).

[21] *Id.*

[22] Reuters, *FTC Says Internet Firms Near "Last Chance,"* April 27, 2009.

[23] Ira Teinowitz, Obama to Name Jon Leibowitz FTC Chairman, *Advertising Age*, Feb. 23, 2009.

[24] Emily Steel, AT&T Backs Privacy Rules, *Wall St. J.* B7 (April 23, 2009).