THE NATIONAL
LAW JOURNAL
NLPIP CO. WWW.NLJ.COM MONDAY, AUGUST 6, 2001

INTERNET PRIVACY

Enforcement Actions

By David Medine and Christine Varney

An increasing number of Web sites are displaying privacy policies— more than 62%, according to a study released by the Federal Trade Commission (FTC) last year, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000). The growth in the number of privacy policies over the past few years has been in response to consumers' concerns about the use of their information online, as well as in response to concerns expressed by regulators and lawmakers. The new chairman of the Senate commerce committee, Ernest ("Fritz") Hollings, D-S.C., introduced legislation last year requiring privacy policies for Web sites collecting personal information and mandating affirmative consent (opt-in) for such collection. See S. 2606 (106th Congress).

Considerable care is required in developing a Web privacy policy. A number of legal theories have been used or advanced by government agencies and private parties in an effort to hold Web sites liable for what they say or, sometimes, what they don't say.

In developing a privacy policy, it can be helpful to get ideas from policies on other Web sites. However, rote copying is a recipe for disaster. Instead, privacy policies should be built from the ground up, by first auditing a company's information practices, bringing together marketing, IT and operations people. Next, an effort should be made to anticipate future information uses. Only then is a company ready to develop a policy. And this should still be vetted with all business units for accuracy before posting. Past challenges to Web privacy policies can provide guidance on how to draft policies that are less likely to be challenged and more likely to survive attack.

Making materially inaccurate statements in privacy policies, including over-promising, is a sure way to get into trouble. Sec. 5 of the Federal Trade Commission Act prohibits unfair or deceptive trade practices in commerce. The FTC has treated Web site privacy policies as "representations," subjecting them to scrutiny under the act, thus transforming a decades-old consumer protection law into a comprehensive, modern privacy statute.

A review of the major FTC privacy cases is instructive

In re GeoCities, No. C-3850 (Feb. 2, 1999), was the FTC's first foray into privacy policy enforcement. The FTC alleged that GeoCities falsely promised never to share consumers' personal information without permission. The FTC alleged that, in fact, GeoCities did not follow that pledge and shared this information with third parties. GeoCities signed a consent decree under which it agreed to post a privacy policy and to follow it.

In *In re Liberty Financial*, No. C-3891 (Aug. 12, 1999) the promise did not involve sharing information with third parties. Instead, Liberty Financial offered a Web site for children, Young-Investors.com. A survey was conducted on the site which sought a great deal of information from children, such as the amount of their allowance; types of financial gifts received such as stocks, bonds and mutual funds, and from whom; spending habits; part-time work history; plans for college; and family finances including ownership of any mutual funds or investments. The survey stated that "[a]ll of your answers will be totally anonymous."

The FTC challenged the allegedly false representation that the information collected would remain anonymous. Liberty Financial signed a consent decree requiring posting of, and adherence to, a privacy policy, and parental consent before collecting information from children. Liberty's conduct would now be governed by the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501 et seq.

FTC v. Reverse Auction.com, No. 000032 (D.D.C. Jan. 6, 2000), demonstrates one benefit of having a privacy policy. ReverseAuction.com, an online auction Web site, chose to market and promote its new site by obtaining e-mail addresses from a competing site, eBay. One problem: eBay's privacy policy prohibited collecting e-mail addresses and using them for spamming.

The FTC alleged that ReverseAuction first agreed to eBay's privacy policy by registering on the site and clicking on the "I Agree" button. ReverseAuction then allegedly harvested e-mail

David Medine *and* **Christine Varney** *are partners at Washington, D.C.'s Hogan & Hartson, where they specialize in e-commerce and privacy law. They can be reached at dmedine@hhlaw.com and cvarney@ hhlaw.com, respectively.*

addresses and sent deceptive e-mail messages. These messages falsely warned eBay members that their eBay ID was about to expire. Thus, in this case, a privacy policy was used to create liability for a Web site visitor. In settling, ReverseAuction agreed, among other things, not to misrepresent its adherence to privacy policies or user agreements in the future.

In *In re Toysmart*, No. 00-11341-RGS (D. Mass. July 10, 2000) and No. 00-13995-CJK (Bktcy. Ct. July 21, 2000) the FTC revisited the same legal theory it started with in *GeoCities*, but in a different context. Toysmart, a children's Web site with substantial ownership interest by Disney, was on the leading edge of dot-com failures. As it was going down the tubes, it recognized that one of its most valuable assets was its customer list. Accordingly, it offered the list for sale in the *Wall Street Journal*.

The only problem was that its privacy policy had promised "you can rest assured that your information will never be shared with a third party." The day after the ad appeared, the company's creditors put it into involuntary bankruptcy, triggering a legal battle over the sale of the list. The FTC and a number of state attorneys general went into bankruptcy court in Boston to try to stop the sale because it would violate Toysmart's privacy policy. They differed, however, on the remedy. The FTC would have permitted sale of the list only to a company ready to step into Toysmart's shoes and abide by existing privacy policy. The states would have gone further and required notice to consumers on the list with an opportunity to opt out of future use of their name as a condition of sale. Disney mooted the case by paying to have the list destroyed.

In each case, failure to adhere to a privacy policy, either by the Web site operator or a visitor, triggered an FTC enforcement action.

The FTC has treated Web site privacy policies as 'representations,' subjecting them to scrutiny under the FTC Act.

Taking things beyond straightforward deception law, the Michigan attorney general, in a notice of intended action in *In the Matter of AmericasBaby.com Inc.*, AG File 20006919 (June 12, 2000), has suggested, based on state law, that a Web site can be held liable for failure to disclose in its privacy policy material information concerning aspects of its information collection practices. In particular, the Michigan AG focused on a Web site permitting a third party to place cookies. A cookie is a file placed on an Internet user's hard drive, typically containing a number and an expiration date, and possibly user names, passwords or preferences. It can be read only by the domain that placed it. The same is true of third-party advertisers, although they may place and read cookies through banner ads on thousands of Web sites.

The AG's reasoning was that although consumers who visit Web sites expect those Web sites to place their own cookies or use other tracking technology, such as Web tags or Web bugs, they do not expect the same activity from third parties, such as firms that insert banner ads on Web sites. Hence, the duty arises to disclose this situation to consumers.

Finally, the Michigan AG has also raised the question of how to change a privacy policy. Some have argued that privacy policy changes, even if posted on a Web site, are insufficient notice to consumers of changed policies for use of previously collected information. On the other hand, the challenge of recontacting consumers who provided information is enormous. Many Web sites have tried to resolve this by noting that their privacy polices are subject to change.

Web sites and third-party network advertisers, such as DoubleClick, extensively employ cookies. A federal class action against DoubleClick was recently dismissed in *In re DoubleClick Inc. Privacy Litigation*, No. 00 Civ. 0641 (S.D.N.Y. filed Jan. 31, 2000; dismissed March 28, 2001). The plaintiffs alleged a number of violations based on laws not designed to apply to consumer interactions with Web sites: Title II of the Electronic Communications Privacy Act, 18 U.S.C. 2701 et seq., which is designed to prevent hackers from obtaining, altering or destroying stored electronic communications; the Federal Wiretap Act, 18 U.S.C. 2510 et seq., which prevents intentional interception of electronic communications; and the Computer Fraud and Abuse Act, 18 U.S.C. 1030 et seq., which bars intentional unauthorized access to and obtaining information from a computer. The district court held all three acts to be inapplicable to the consumer interactions with Web sites at issue.

Michigan AG has challenged tracking technologies

Nonetheless, the undisclosed use of cookies has the potential of creating liability for Web sites and for advertisers. A series of consent agreements and notices of intended action by the Michigan AG provides an outline of a number of aggressive legal theories under state unfair and deceptive practices acts that could be used to challenge the use of tracking technology. See, e.g., *In the Matter of DoubleClick Inc.*, AG File 200002052 (Feb. 17, 2000) (Notice of Intended Action); *In the Matter of eGames Inc.*, AG No. 2000011155 (Assurance of Discontinuance). The AG has asserted that use of cookies to develop profiles requires affirmative consumer consent, presumably opt-in, and that placement of cookies is the equivalent of trespass to chattels.

The Michigan AG's settlement with eGames moves past Web sites into the arena of software privacy. eGames included in its computer game software a mechanism that allowed a third party to insert new advertisements when the user's computer was connected to the Internet. This same mechanism was used to track consumers while using the game. Even though the disputed activity took place when using software, the Michigan AG found that the appropriate remedy was to disclose these practices on the company's Web site, from which the software was downloaded.