WILMER, CUTLER & PICKERING

ECOMMERCE NEWS

March 31, 2001

SPOTLIGHT ON ONLINE PRIVACY

U.S. legislators and litigants are continuing to focus on online privacy. Here is a brief summary of the current state of the privacy discussion.

Federal policy makers are increasingly concerned about Internet privacy. Issues at the forefront include the disclosure, exchange, aggregation and merger of personally identifiable information; and the use of cookies, web beacons (see November 1999 ECommerce News), spyware and related information collection technologies. The FTC has been positioning itself as the leader on these issues. Last summer, it recommended legislation for online privacy generally and for the practice of online profiling by third-party advertisers in particular. On March 13, 2001, the FTC sponsored a forum to discuss the issues presented by the merger of data gathered from diverse sources and the exchange of data with other companies — including particularly the ability to merge personally identifying information with detailed information gathered by cookies.

Legislators have proposed a flood of privacy legislation in the 107th Congress addressing a wide range of online (and offline) privacy issues. Both the House and Senate appear to be committed to the issue. The chairman of the House Energy and Commerce Committee, Rep. Billy Tauzin (R-La.) has expressed support for Internet privacy legislation, and Sen. McCain (R-Ariz.), chair of the Senate Committee on Commerce, Science, and Transportation, remains committed to it as well.

online (and offline) privacy issues. Both the House and Senate appear to be committed to the issue. The chairman of the House Energy and Commerce Committee, Rep. Billy Tauzin (R-La.) has expressed support for Internet privacy legislation, and Sen. John McCain (R-Ariz.), chair of the Senate Committee on Commerce, Science, and Transportation, remains committed to it as well.

Broad privacy bills have been introduced. For example, Rep. Rodney Frelinghuysen (R-N.J.) introduced both the Online Privacy Protection Act of 2001, H.R. 89, which would require the FTC to set privacy guidelines for all users not covered by COPPA (see October 1999 ECommerce News), and the Social Security On-line Privacy Protection Act, H.R.91, which would prohibit interactive computer services from disclosing an individual's social security number or related personally identifiable information to third parties without prior written consent.

Rep. Anna Eshoo (D-CA) and Rep. Chris Cannon (R-UT) have introduced the Consumer Internet Privacy Enhancement Act, H.R. 237, giving users the right to limit the use of their personal information by Internet companies. The bill would also require web site operators to disclose how information is gathered and for what purpose. The proposal

tracks a bill introduced in the last Congress by Sen. McCain and cosponsored by Sen. John Kerry (D-Mass), also a member of the committee.

Rep. Gene Green (D-Tex.) introduced the Consumer Online Privacy and Disclosure Act, H.R. 347, which requires the FTC to promulgate privacy regulations. In addition, it prohibits web sites and Internet service providers from (1) correlating certain types of information with personal information, (2) allowing third parties to attach persistent cookies without an opt-out option for individuals, and (3) selling transactional information to satisfy creditors. The legislation would also authorize state enforcement, FTC enforcement and a private right of action.

In addition to broad privacy bills, privacy provisions have been tucked away in bills dealing with other issues. For example, the Bankruptcy Reform Act of 2001, S.420, which passed the Senate on March 15, 2001, contains provisions that would maintain the enforceability of a privacy policy prohibiting the transfer of personally identifiable information that was effective at the time of the bankruptcy filing during bankruptcy proceedings.

In another bill, H.R. 602, dealing with health insurance discrimination based upon genetic information, group health plans and health insurance issuers are prohibited from disclosing protected genetic information, which is defined as genetic test information of an individual or their family members.

Legislators have introduced bills that would enhance or strengthen existing protections for personal financial and health information. For example, Sen. Paul Sarbanes (D-Md.) introduced the Financial Information Privacy Protection Act of 2001, S.30, which would amend the Gramm-Leach-Bliley Act ("GLB") to require affirmative consumer consent before a financial institution shares nonpublic personal information with an affiliate (currently, such consent is only required for disclosures to nonaffiliated third parties) and to impose limits on the reuse and redisclosure of personal information by third parties.

Sen. Richard Shelby (R-Ala.) introduced the Social Security Number Privacy Act of 2001, S.324, which also would amend the GLB. This legislation would prohibit the sale and purchase of social security numbers by financial institutions. (There are a handful of bills specifically directed at protecting social security numbers from disclosure.) The proposed restriction on the *purchase* of personal information reflects emerging concerns over profiling and the merger of data. As panelists at a recent FTC forum noted, a consumer may consent to data collection and use by his or her bank without knowing that the bank is also gathering and merging data from outside sources.

Sen. Shelby introduced another privacy bill, S.536, that also reflects these concerns. This legislation would add a subsection to the GLB, titled *Limitation of Sharing of Marketing and Behavioral Profiling Information*, that prohibits a financial institution from disclosing (1) "any information for the purpose of marketing nonfinancial products to the consumer to whom the information pertains" unless that consumer affirmatively consents or (2) the "identity of any entity (i) to whom that consumer has made a payment …; (ii) with whom that consumer has engaged in a credit transaction; or (iii) from whom that consumer received any payment or transfer of funds."

Importantly, legislators have demonstrated that they are *specifically* interested in and worried about the use of cookies, web bugs, web beacons, spyware and related technological means of collecting information. On

ranging from the nefarious (the copying of the contents of a person's computer) to the arguably benign (the use of web bugs to enable ad-tracking). Senator Shelby escribed some of the demonstrated uses as "frightening." This and similar concerns have been, and will continue to be, reflected in legislation. For example, the Consumer Online Privacy and Disclosure Act, H.R. 347, introduced by Rep. Green (D-Tex.) would require online services to allow consumers to *opt-in* to the use of third-party cookies.

Similarly, Senator Edwards (D-N.C.) has introduced legislation aimed at software that "phones home" with data about users. Under the Spyware Control and Privacy Protection Act, S. 197, vendors that incorporate spyware in their software would be required to provide "clear and conspicuous notice" of that fact, obtain informed consent before using information derived from the spyware, and provide "easily understood instructions" as to how to disable the spyware. Each violation of these requirements would constitute an unfair or deceptive act under the Federal Trade Commission Act.

The Electronic Privacy Protection Act, H.R.112, is a similar bill that would make it unlawful to "knowingly make, import, export, distribute, sell, offer for sale, install, or use an information collection device" unless similar conditions are met.

Congressmen Asa Hutchinson (R-AR) and Jim Moran (D-VA) reintroduced legislation to create a bipartisan Privacy Protection Commission. H.R. 583, The Privacy Commission Act, establishes a seventeen member commission to conduct a comprehensive study of privacy issues and make recommendations for action to Congress. The bill achieved a majority vote in the House of Representatives last year, but failed to reach the supermajority vote required under the legislative procedure used to send it to the Senate.

State Action

States continue to threaten or pursue litigation against Internet companies on consumer protection and privacy grounds. On December 5, 2000, the Cook County State's Attorney filed a lawsuit against Clearstation Inc. (a subsidiary of E-Trade Group Inc.) and DoubleClick, alleging that they misuse cookies in violation of the Illinois Consumer Fraud Act, and Michigan's state attorney general has repeatedly threatened to sue DoubleClick and other companies on the ground that third-party cookies violate Michigan's consumer protection laws. State legislatures are similarly poised to take action against commercial web sites that use cookies. For example, the Chairman of the Nevada Senate's Judiciary Committee has announced that he is seeking legislation aimed specifically at the use of cookies.

Industry Action

Industry groups have traditionally focused on demonstrating the role of self-regulatory efforts in facing the issue of online privacy. In addition, some are focusing on technical ways of confronting the issue. In particular, Microsoft's chief privacy officer recently held meetings on Capitol Hill extolling the virtues of the P3P initiative (see www.w3c.org). P3P is a protocol that allows sites to describe their privacy practices in machine-readable language. In turn, users will be able to set their browsers to signal when they have reached a site whose practices do not conform with the user's preferences. The next version of Internet Explorer, due out this spring, will incorporate default settings for user privacy preferences.

Private Litigation

Private Internet privacy litigation — and in particular privacy litigation based on commercial web sites' use of cookies — continues to be prosecuted. Class action

lawsuits against Netscape, AOL, MatchLogic, Avenue A, Toys R Us, and many other companies are still pending.

Industry received some good news this month, when Judge Buchwald of the Southern District of New York dismissed a multidistrict consolidated class action against DoubleClick that had been brought by "all persons who, since 1/1/96, have had information about them gathered by DoubleClick." The class was represented by the Milberg Weiss firm. (In re DoubleClick Inc. Privacy Litigation, 00 Civ. 0641 (NRB), March 28, 2001.)

Plaintiffs had claimed that DoubleClick's cookies violated the Electronic Communications Privacy Act (ECPA) (which includes an attorney's fee provision). Judge Buchwald found that (a) DoubleClick's client web sites had authorized the placement of these cookies (and DoubleClick had accessed only communications between end-users and these sites), and (b) DoubleClick's cookies stored on end-users hard drives did not fall within the category of temporarily-stored electronic communications addressed by ECPA. (ECPA protects only electronic communications stored for a limited time by electronic communication services while waiting for delivery.)

As to plaintiffs' claim of a violation of the Wiretap Act, Judge Buchwald found that DoubleClick's client sites had consented to any electronic "interception" by DoubleClick.

Finally, with respect to plaintiffs' Computer Fraud and Abuse Act claim, the court found that plaintiffs had failed to allege losses meeting the required $5,000 monetary threshold, stating "A person who chooses to visit a Web page and is confronted by a targeted advertisement is no more deprived of his attention's economic value than are his off-line peers." Having dismissed the federal claims, the court declined to exercise supplemental jurisdiction over plaintiffs' state claims, and dismissed plaintiffs' Amended Complaint.

++++++++++

Wilmer, Cutler & Pickering assists clients in understanding, reconciling, and complying efficiently with global data protection laws. We provide general and strategic counseling, and assist clients in developing disclosures and negotiating contracts for international transfers of data. WCP has expertise in national data protection laws, both US and overseas; laws regulating unsolicited commercial email; Gramm-Leach-Bliley; health records (HIPAA); workplace monitoring laws; technology security and encryption; and related areas.

For further information about our privacy practice, please contact:

Becky J. Burr, Bburr@wilmer.com
(202) 663-6695
Patrick J. Carome, Pcarome@wilmer.com
(202) 663-6610
Lynn R. Charytan, Lcharytan@wilmer.com
(202) 663-6455
Susan P. Crawford, Scrawford@wilmer.com
(202) 663-6455
Christian L. Duvernoy, Cduvernoy@wilmer.com
011 (322) 285-4906
Ronald J. Greene, Rgreene@wilmer.com
(202) 663-6285
David R. Johnson, Djohnson@wilmer.com
(202) 663-6868
Natalie Luebben, Nluebben@wilmer.com
011 (49-30) 2022-6429
Andrew K. Parnell, Aparnell@wilmer.com
011 (44-207) 872-1040