House
Legislative
Analysis
Section

Romney Building, 10th Floor
Lansing, Michigan 48909
Phone: 517/373-6466

# INTERNET PRIVACY ACT

**House Bill 5356 (Substitute H-1)**
**First Analysis (11-10-98)**

**Sponsor: Rep. Lingg Brewer**
**Committee: Advanced Technology and Computer Development**

## *THE APPARENT PROBLEM:*

The Internet affords users quick access to sources worldwide for newspapers, shopping, medical information, governmental services, travel, research, stock market investments, and so forth. In Michigan, the Internet has brought state government closer to the people by providing websites for state agencies and increased accessibility to the legislative process. For instance, at www.michiganlegislature.org, a person can access House and Senate bills, committee schedules and membership, and addresses and phone numbers for Representatives and Senators, among other available information. Even tax returns can be filed electronically via the Internet.

Unfortunately, along with the good it has brought, the Internet has had some negative effects on society. For instance, many people believe the Internet has taken a toll on personal privacy. The right to personal privacy is a major tenet of Western law, and has been protected through various statutes and court decisions through the decades. However, it has yet to be proven how effective current state and federal privacy rights laws are in protecting a citizen's right to privacy in this new electronic arena. What has been happening is that consumers using the Internet have wittingly and unwittingly given Internet companies and others that operate websites personal information about themselves that is then often sold to others for marketing and other purposes.

Each time a person logs on to the Internet and visits a website, information may be gathered in a variety of ways. Online purchases require a credit card number and mailing address, participating in a chat room reveals a person's e-mail address, browsing patterns may be tracked, and so on. Some websites place a "cookie" in the user's hard drive, which identifies the user the next time he or she visits the site. A cookie cannot identify a particular person unless it is attached to personally identifiable information (such as a name, address, Social Security number, etc.) that is collected through a means such as an on-line registration form, purchase agreement, or contest entry. This information may be sold to other companies, or intercepted by unintended people. In a recent Michigan case, a website operated by the Jobs Commission encouraged visitors to use their Social Security numbers as their passwords. Unfortunately, a computer expert in Pennsylvania cracked the security of the system and obtained a list of the Social Security numbers.

Even more alarming is the development of new technologies that can "backchannel" information when a person is online. Recently, the Privacy Forum, in the Privacy Forum Digest dated October 10, 1998 (Vol.7, issue 17) at www.vortex.com, reported on the new Netscape "What's Related" functionality of the Netscape web browser, which is capable of "backchanneling" information up to Netscape and its partners. The author writes that the infrastructure of the system has the capability to collect massive amounts of information about users' browsing patterns and habits, and that this information, in some cases, could be tied to specific users' names and other personal information. According to the article, any link site visited from a "What's Related" reply list is reported back to Netscape, and that up to an additional 1,000 sites visited after pushing the "What's Related" button may also be reported back to Netscape. Reportedly, Netscape, which does have a privacy policy, is not saving detailed information gathered through the "What's Related" functionalities at this time, and the functionalities can be turned off by those concerned with privacy issues. However, a user who may not know about the backchanneling ability may be unaware that he or she is having personal information gathered while being online.

The implications of the loss of personal privacy or control over one's personal information can range from being inconvenienced by an onslaught of telemarketers and junk mail to having one's identify stolen and financial credibility ruined.

Under mounting pressure from the FTC and consumers for industry regulation, about 100 companies and groups formed an alliance earlier this summer designed to protect privacy on the Internet. Members of the Online Privacy Alliance pledged to adhere to alliance policies that include informing people of what will be done with personal information collected online, giving people the chance to "opt out" of having personal information gathered, and refraining from collecting information on children under 13 at children's web sites without parental consent. Monitoring and enforcement are provided by third parties such as the Better Business Bureau and TRUSTe, who provides a trustmark as a seal for participating websites. Eight of the busiest Internet sites, acting together as the Privacy Partnership, ran more than 200 advertising messages on the Internet during the month of October urging Internet users to educate themselves on the issue of privacy and to read the privacy statements on websites before giving out any personal information on themselves.

Despite the recent industry attempt at self-regulation, the potential for abuse is so serious that demand for governmental intervention persists. Earlier this year, the Clinton administration issued a presidential memorandum that directed the heads of U.S. agencies to ensure that new technologies did not erode Privacy Act protections, to examine how new technologies could enhance privacy practices, and to conduct thorough reviews of existing privacy practices. Also, the Office of Management and Budget was directed to conduct a review and issue guidelines on how agencies could protect privacy information, especially when collaborating with state and local governments. As part of the administration's online privacy initiative, the FTC established a website (www.ftc.gov) to inform people how to better protect their personal information from being needlessly disclosed to others. In addition, the Omnibus Appropriations Act of 1998, Public Law 105-277, which was signed into law on October 21, contains within it the Children's Online Privacy Protection Act to prohibit operators of commercial websites or online services from collecting, using, or disclosing personal information from children without verifiable parental consent. Operators would also be required to provide notice on the website of what information is collected, how the information is used, and the disclosure practices.

Notwithstanding the beginning of tighter industry self-regulation and the Clinton administration's efforts to educate and protect consumers, there still is no nationwide baseline privacy standard. This lack of a uniform federal law has led some people to believe that individual states need to enact legislation to protect Internet users from the exploitation of personal information given online. Legislation is being offered that would prohibit Internet service providers operating within the state from disclosing personally identifiable information to a third party without permission.

## *THE CONTENT OF THE BILL:*

The bill would create the Internet Privacy Act to prohibit interactive computer services from disclosing personally identifiable information of subscribers to third parties without written consent. A subscriber could bring a civil suit for relief against a service for a violation of the bill. An "interactive computer service" would be defined as an information distribution system that provided access to the Internet through a modem to more than one person at a time. "Personally identifiable information" would be defined as data that enabled a specific person to be identified and would include, but not be limited to, the individual's name, Social Security number, driver's license number, personal identification card number, unlisted telephone number or address, electronic mail address, photograph, and digital or electronic image. "Unlisted" would mean a phone number or address that was not listed in a public phone book. A "subscriber" would be an individual who had provided personally identifiable information about himself or herself to a service.

Under the bill, unless authorized by state or federal law, an interactive computer service or its employees could not disclose personally identifiable information about a subscriber unless the subscriber provided the service with written consent to do so. "Informed written consent" would mean a written statement freely signed by a subscriber that identified his or her rights under the bill and that specifically authorized a service to disclose his or her personally identifiable information to third parties. In addition, a service or its employees could not knowingly falsify personally identifiable information about a subscriber or disclose information to a third party that the service knew was false. If a subscriber requested, a service would have to provide the subscriber with his or her personally identifiable information, permit the subscriber to verify the information, and permit the subscriber to correct errors contained in the information. Also upon request, the service would have to provide the subscriber, at no charge, with the identity of each

third party to whom the service had released his or her information.

## *FISCAL IMPLICATIONS:*

Fiscal information is not available.

## *ARGUMENTS:*

### *For:*

In bringing the world closer, the Internet has inadvertently created a new problem with invasion of personal privacy. Many websites deposit "cookies" to unknowing visitors that supply information to the web operator. This information may then be sold to third parties for marketing and other purposes. Often the information is collected in aggregate form, meaning that any one piece of information cannot be traced back to a particular individual. However, some cookies are attached to data collected when a user fills out an online registration form, subscribes to an online service, or places an order for merchandise. Even if a cookie is not used, users giving out their names, addresses, birth dates, credit card numbers, Social Security numbers, and other personal information may unknowingly be giving the information to more sources than they are aware of.

The result of personal information or browsing preferences that can be traced to a particular individual being sold to third parties may be as benign as unleashing a torrent of unsolicited mail order or online offers for services and merchandise, or may bring more serious threats such as the theft of credit card numbers or stealing an individual's identity via a Social Security number. There have been cases in which people participating in chat rooms have been stalked by someone who traced their street addresses through their e-mail addresses. In fact, several companies operate on the Internet solely to provide or sell personal information to others. Some of the information provided is gleaned from public records, such as land sales, court records, and bankruptcy filings, where other information is purchased from other online companies that have gathered information on users. From one online data reseller, a user can find out what another person keeps in his or her safety deposit box and even how much he or she has deposited in overseas accounts! The truly frightening fact in all of this is that this exchange of information is for the most part perfectly legal (apart from what would constitute fraudulent practices, such as illicit use of credit card numbers, and so on). Therefore, little incentive has existed to curb the spread of public information on the Internet or from information collected on the Internet from being disseminated to others.

Many believe that this invasion and erosion of personal privacy must be checked. Sadly, current laws have not kept up with the problems created by advancing technologies. Though the recent federal appropriations bill contained a new act to protect the rights of children under 13, little has been done to protect those over 13 years of age. House Bill 5356 would therefore be an important first step in providing some protection for Internet users.

Under the bill, interactive computer service providers, which would primarily comprise Internet service providers (ISPs) and commercial online services, could not sell or give personally identifiable information to a third party without the expressed consent of the individual. The collection or use of aggregate information would not be affected. Falsifying information or disclosing false information would also be prohibited. The bill goes further by including a provision that would give a subscriber to a service the right to verify personally identifiable information about himself or herself that the service had on file. Where subscribers have little recourse under current laws to curb the dissemination of their personal information, the bill would allow a subscriber to bring a civil suit against an ISP or online service that released information without permission. Perhaps if more states take the initiative to establish and enforce controls on Internet companies, it may prompt federal legislation that could establish a national baseline policy for Internet privacy rights and the dissemination of personal information. Until then, this bill is needed to afford Michigan residents some protection from the wanton sale of information that now occurs.

### *Against:*

The bill is problematic in several respects. First of all, several terms appear to be misdefined. For instance, "internet" with a lower case "I" would refer to an interconnected network of any kind, and so would attempt to regulate private systems. Further, the bill would only apply to Internet service providers and commercial online services, along with any other computer system that met the definition of "interactive computer service." Most, if not all, of these services already have privacy policies that deal with privacy issues. Besides, much of the personal information collected and resold on the Internet is done by commercial companies operating sites on the World

Wide Web. This segment of the Internet would not be regulated by the bill. It would be very difficult for an individual who felt that personal information had been disclosed to prove that a service provider, and not a commercial website, was the offending party.

In addition, since only an ISP that was incorporated or physically located within the state could be regulated under the bill, it is possible that attempts to regulate Internet access providers would be seen as violating the Commerce Clause of the U.S. Constitution. According to information supplied by the Electronic Frontier Foundation, in two recent federal district court cases [*American Library Association* v *Pataki*, Civ. Dkt. 97-0222 (S.D.N.Y. 1997) and *American Civil Liberties Union* v *Johnson*, Civ. Dkt. 98-474 (D.N.M. 1998), the courts held that "state restrictions on interstate online communications automatically trigger the Commerce Clause (even in cases where one of the parties is in the state in question), because the Internet is in and of itself an interstate (indeed, global) medium, and parties generally have no way to ascertain the physical location of other parties online."

Further, the bill only applies to those service providers and online services that connect a user to the Internet via a modem, which uses telephone lines. Therefore, Internet access supplied by other means, such as wireless, coaxial, digital telephonic, and ethernet technologies would not fall under the purview of the bill.

### *Against:*

The Internet, a global entity, does not lend itself easily to state regulation. Reportedly, there are at least 3,835 Internet Service Providers (ISPs) in North America, and at least 123 ISPs in the 517 area code alone. A better approach is to encourage self-regulation and federal regulation to establish a uniform privacy policy.

Self-regulation is well on its way. This summer, at least 100 companies that represent 85 percent of the websites visited online have joined the Online Privacy Alliance and Privacy Partnership. Alliance members pledge to adhere to privacy policies that include disclosing what kinds of information are collected and how they will be disseminated, and must provide an "opt-out" mechanism for users who do not want information collected from them. Privacy Partnership members have collaborated on attempts to educate consumers on how to protect their own privacy, and to encourage the use of those sites with posted privacy polices and opt-out options.

Further, the new Children's Online Privacy Protection Act of 1998 now prohibits websites and services that cater to children from collecting or disseminating information on children under 13 without verifiable parental consent. The FTC's website gives consumers important information on how protect their personal information. These initiatives should be given time to prove their effectiveness. After all, legislation is no substitute for common sense. Consumers need to take responsibility in being more careful about the types of information they disclose about themselves.

### *Response:*

The industry attempt at self-regulation came only under threat of federal legislation and pressure by the Federal Trade Commission. Since non-compliance results primarily in the loss of the TRUSTe privacy seal, and also since many consumers fail to look for such a seal before disclosing personal information, the initiative may lack sufficient teeth to ensure long-term, industry-wide compliance, especially when a profit can be made by selling personal information collected from Internet users to marketers. The bill won't affect every segment of the Internet, but it still represents an important first step in setting public policy for the protection of privacy rights on the Internet.

## *POSITIONS:*

The Department of Civil Rights has not taken a formal position on the bill. (10-30-98)

The Electronic Frontier Foundation, a nonprofit organization that advocates for civil liberties and responsible behavior in the electronic world, opposes the bill. (10-14-98)

Analyst: S. Stutzky

■This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.