Privacy Issues on the World Wide Web

Easily accessible information and data bases are giving rise to concerns about privacy on the Internet. Three panelists, Steve Morrissett of the Utah Attorney General's Office, Peggy Haney of American Express, and Maxine Sweet of Experian (formerly TRW) discussed the issues and implications for consumer education. The remarks of the speakers and discussion are summarized.

Elizabeth M. Dolan, University of New Hampshire[1]
Irene E. Leech, Virginia Tech[2]
Jikyeong Kang, University of Wisconsin-Madison[3]

Steve Morrissett, Utah Attorney General's Office, Criminal Division

Attorneys General are interested in the issue of privacy on the world wide web since there is fertile ground for opportunities which may not be legal. The web system is set up to be anonymous. Utah became involved in the issue of verifying identities on the world wide web. In 1995, the Utah legislature passed a digital signature law. This law created opportunities for banks and other institutions to act as the repositories of digital signatures, allowing individuals and businesses to send and receive confidential information over the web, as well as conduct binding contractual business transactions. Another issue is that Utah criminal law did not cover accessing another's computer, i.e., it was not a crime to break into another computer. When people are "on-line," it is like having an electronic open door: anyone can "walk in" who sees that the door is open. Passwords have not been very effective in keeping people out of computer systems. There are, in fact, people who are in business to try to get information out of other computer systems in order to find out how effective the safeguards are. Utah now has criminalized breaking into another computer.

The question of money laundering was raised. Right now, the Internet is not terribly effective for money laundering activities. But within a year or so, digital cash will be a reality which will change the picture. Persons or businesses will deposit money in a bank, type in pertinent information and send the money to another person/business/bank electronically. This can be done anonymously. Money, then, can be moved around (laundering) and the government is very concerned about this.

Another issue is that of encrypted messages. PGP programs (pretty good privacy) are free and allow the user to encrypt a message so that only the "proper" recipient will be able to decipher it. The U.S. government considers this a security risk and therefore encrypted messages cannot be sent outside the U.S. This prohibition is negatively impacting upon U.S. business in the competitive world marketplace.

"Remailers" take an encrypted message, strip the sender's name off the message and send it on to its destination. The recipient has no way of identifying who sent the message. One message can be sent through several "remailers" so the message cannot be traced. There is a balance between privacy and the government's need to know about illegal activities. The system was not designed to break into encrypted messages. However, the government is worried because it wants to be able to get into messages if need be for national security issues. This dilemma has yet to be resolved.

Peggy Haney, American Express

Privacy on the Internet is closely tied to the level of security provided by a website for transactions. American Express has been involved in privacy protection issues for nearly twenty-five years, and has provided leadership to the industry by advocating the creation of effective privacy policies. In 1974, American Express issued the first "opt-out" form allowing card holders to keep information about them from being used for marketing purposes. In 1978, American Express developed a privacy code of conduct for employees. This was revised in 1991 into a Privacy Principles format and to cover parts of the company which had not existed in 1978. The code was again revised in 1996 to reflect the reorganization of the company and new privacy issues. The company's position is that privacy protection is so much a part of their culture that the discussion is not whether to apply

privacy principles, but how.. A pamphlet is available explaining these privacy principles. For a copy, contact the Consumer Affairs Office, American Express Company, 801 Pennsylvania Ave., NW, Washington, D.C. 20004.

American Express has several committees working on privacy. The telemarketing committee was formed to ensure that American Express was in compliance with the new FTC telemarketing rules and that the company was not being intrusive in its marketing practices. There is a committee on internal data security to look at vulnerabilities so that confidential information is secure. The international committee deals with privacy issues which arise through a world wide market. These committees look at how the company uses consumer information and how secure that information is.

As new technologies are developed, new privacy issues arise. For example, SmartCards require a fresh look at how to apply the Principles to a new delivery system. The same is true for websites. Questions include how to provide disclosures and opt-out choices for consumers regarding how information may be used for marketing. Internet security is evolving rapidly.

American Express will not use a customer's e-mail address without the customer's knowledge. If a potential customer "browses" one of American Express's web-sites, American Express will not collect or use any information for solicitation purposes. The brokerage services may operate somewhat differently in this regard as brokers are in need of different types of information from their customers.

Right now, SSL security systems for Internet sites scramble information. This allows confidential information, such as credit card numbers, to be given over the Internet with the assurance that the information is reasonably secure. The retailer only gets part of the card number. The credit company receives the full number and retailer transaction information. A newer system called SET (secure electronic transactions) is becoming available. The SET system uses encryptions of confidential information. Consumers should look for either SSL or SET on their browsers before sending confidential information, such as credit card information, to a web-retailer.

The world wide web is an open system and is presenting a huge challenge to companies in maintaining their customers' privacy. Right now, the best approach for consumers is to web-shop with retailers that are known to be reputable. American Express has helped produce a brochure entitled "Cyber Shopping" about protecting yourself when buying on-line. Copies can be obtained through the Consumer Information Center (CIC) by sending 50¢ per copy to: CIC, Department 389C, Pueblo, CO 81009. CIC also has a website: http://www.pueblo.gsa.gov. The American Express web site address is: http://www.americanexpress.com.

Maxine Sweet, Experian (formerly TRW)

Experian has developed fair information values also so the company and its customers use data responsibly to ensure privacy. The issues are not new, but have been re-cast in light of the world wide web, and have become more broad based. Experian's Information Values include partnership, fairness, balance, security and communication.

A few years ago, only 3% of credit card users indicated that they would be comfortable using their credit cards on the Internet; today, many more people are turning to this retail experience. Because of the safeguards in place on browsers, credit card information may be more secure on the Internet than when used in the "regular" manner when clerks and wait persons take our cards out of our sight.

Currently, there are some companies which allow consumers to request a report on the Internet but the person will not receive the report that way - it will be mailed. Consumers want to get their own confidential information over the Internet so identity authentification is important. Thirty percent of questions to Experian are "why can't I get my credit report on the Internet?" The company is trying to come up with a reasonable policy.

There are two challenges to security of confidential information on the Internet. The first is transferring of data. Data are relatively easy to secure with data encryption programs and SSL (secure socket layer). The second challenge involves authenticating identities on the Internet. Are you who you say you are? One resolution may be to first require full identification, two credit card numbers, a driver's license number (which is not currently required), and a former address (how many fraud perpetrators would know where a victim used to live?). A report transmitted over the Internet would not include complete account numbers; this would ensure that the information could not be used. One stumbling block is the inability to verify when a report must be give for free. At this point, Experian is considering transmitting only paid credit reports in this manner.

Experian has a fraud unit with a toll-free number. They will assist anyone who has had a

problem with a credit identity being used fraudulently. The unit will even share information about fraud rings with other credit reporting agencies. Consumers need to understand what information a creditor needs to have to prove fraud. Consumers need to ask "what do you (creditor) need to verify that the charge is not mine, so that you can report it correctly to the credit bureau."

Currently, it is estimated that up to 40% of Experian's credit information disputes come from "credit clinics." Credit clinic operators tell their customers to dispute all negative information found on a credit report ("I'm not late" and "That's not mine"). Over-use of the procedure makes it difficult for credit bureaus and creditors to effectively handle legitimate problems.

Experian believes that consumers are interested in opportunities and choices on the Internet, a competitive marketplace, and fairness. Information should not be used to the consumer's disadvantage. Consumers do not want to be disadvantaged, embarrassed or be subject to increased anxiety when using the world wide web.

The Experian website address is http://www.experian.com. Consumer information is available online through the "Consumer Credit Pavilion," "Revolving Showcase" or "Ask Max."

Discussion

People need to know that some browsers have security programs while others do not. More information needs to be available about SSL and SET. On NetScape, if the tiny key in the bottom left corner is broken, then there is no security; if unbroken, then secure. But how many people know this?

The Federal Fair Credit Reporting Act was revised last year (became effective 10-1-96). Credit bureaus now must provide a free copy of a credit report not only to the person who has been turned down for credit within 60 days (up from 30 days), but also to the unemployed, those receiving welfare, and those who have been victims of a credit fraud.

One person asked what was to stop someone from setting up a web page short term, collecting as much credit information as possible through bogus sales and then disappearing. Steve Morrissett suggested that this also be done "offshore." The best approach to buying on line is to stick with reputable retailers. Common sense information needs to be disseminated about using the web for retail purposes. There are reasonably secure ways of sending confidential information and this needs to be more widely known.

If information is passing through multiple servers, even companies that are reputable could be a source of problems if credit card information is put on Internet. If information is encrypted, then information is probably secure. The merchant will only get part of the credit card information. The credit company receives the full card and retail information.

A member of the audience asked if those who create viruses are being prosecuted. According to Steve Morrissett, no, because these people are hard to track down.

The final question asked for an example of real fraud on the world wide web. The example given was Internet gambling. A person sends some dollar amount to another country (the Bahamas, for example), which enables them to gamble on-line with that money. Usually what happens is that the money just disappears without the person ever getting to gamble with it! The National Fraud Information Center may have a number of examples of Internet fraud on their web site.

Finally, the Better Business Bureau has been working on developing a "seal of approval" for web sites, similar to the Good Housekeeping Seal of Approval. It would simply verify that the site is what it says it is, i.e., the seal would be an endorsement of the site as a good web-citizen. Like its predecessor, there would be no claims regarding the quality of the products or services.

Endnotes

1. Associate Professor, Department of Family Studies.
2. Associate Professor, Department of Housing, Interior Design and Resource Management.
3. Assistant Professor, Department of Consumer Sciences.