

# 'Net balance: Online privacy

*If e-commerce and e-government are to reach their full potential, privacy concerns that shake consumer confidence must be resolved.*

**BY CINDY J. LACKEY**

**T**he Internet has something for everyone. From the convenience and privacy of their own homes, at any hour of the day, consumers can learn, shop, access government services and information, and communicate almost instantly worldwide. Through the Internet, businesses interact with individual customers, gathering information to understand the consumers' needs and, in turn, providing products, information and services to meet those needs. Governments can offer citizens and businesses 24-hour-a-day access to services and information.

As a result, e-commerce is growing. For example, despite the sluggish economy, 18.7 million households rang up \$5.7 billion in U.S. online sales in December 2001, up 14 percent from December 2000, according to Forrester Research, a technology research firm.

E-government also is maturing. In 2001, state governments earned an average score of nearly 70 for their progress in adopting digital technologies to improve service delivery, according to *The Digital State 2001*. The average score was just 44 in 1997, the first year of the annual report by the Progress & Freedom Foundation, a nonprofit organization that studies technology and public policy.

Though e-commerce and e-government are growing steadily, industry analysts and government officials wonder how much more would be possible, were it not for persistent consumer concerns about the privacy of "doing business" on the Internet — the world's most public marketplace. A

national survey conducted by Rockridge Associates in 1999 found that 58 percent of consumers do not consider any financial transaction online to be safe, and 77 percent think it is unsafe to provide a credit card number over the computer. If e-commerce and e-government reach their potential, consumers' concerns about privacy must be addressed.

## **Consumer concerns**

The Information Technology Industry Council, an association of information technology companies, identifies four categories of consumer concerns about Internet privacy: harm and fraud, sensitive information, nuisances and government.

Harm and fraud includes crimes such as identity theft, stolen credit-card numbers and fraud. Documented cases indicate that fraud and scams are thriving online. In testimony to Congress on May 23, 2001, the Federal Trade Commission reported the number of consumer complaints related to online fraud and deception jumped from fewer than 1,000 in 1997 to more than 25,000 in 2000.

In comparison, identity and credit-card thieves seem to operate mostly in the physical world of lost wallets and stolen mail, not cyberspace. The Pew Internet & American Life Project, a nonprofit initiative, claims that few cases of credit-card fraud or identity theft are related to the Internet. In an April 2001 report, the project reported that only 8 percent of those who reported stolen credit-card informa-

tion said that "the thief might have gotten the information because the consumer had provided it online." However, the same report said that the FBI reported in March 2001 that Russian and Ukrainian hackers had penetrated more than 40 U.S. computer systems to steal more than one million credit card numbers.

Sensitive information includes personal information that consumers want to keep private because it could be used to embarrass, harm or discriminate against individuals. The typical examples of "sensitive" information are medical and genetic information, financial information and children's information. For example, 85 percent of Internet users who seek health information online fear that insurance companies might alter their coverage after reviewing information they accessed online, according to a November 2000 report by the Pew Internet & American Life Project.

Nuisances and consumer-confidence issues include the most common consumer complaint: unsolicited e-mail, or "spam." This online equivalent of junk mail may not result in harm to consumers, but it may be annoying enough to limit some consumers' use of the Internet. The explosion in Web use provides "spammers" access to more e-mail addresses and offers a labyrinth of locations from which to distribute their mass mailing anonymously. The Gartner Group, a technology research and consulting firm, reported in March 2002 that there is now 16 times as much spam on the Internet as

there was just two years ago.

Another hot button for consumers is tracking of their Web browsing through the use of “cookies” — software programs that a Web site installs on a visitor’s computer. By tracking a consumer’s Web usage, companies can target advertisements and services to the consumer’s interests. However, only 27 percent of Internet users agree that tracking is helpful because it allows the sites to provide information tailored to specific consumers, according to a 2000 survey by the Pew Internet & American Life Project. Fifty-four percent of Internet users believe that Web sites’ tracking of users is harmful because it invades their privacy.

Other nuisances and concerns that undermine consumer confidence include deceptive uses of data collected by a Web site and monitoring employees’ online activities.

Government implications indicate citizens are wary that the explosion in electronic communications and cutting-edge surveillance technology will enable “Big Brother” to monitor citizens as never before. Stirring public interest and Congressional investigation in recent years was the FBI’s “Carnivore” system (renamed DCS1000 last year), which is used to monitor the e-mail of suspected criminals. Still, Americans seem comfortable with government surveillance of criminals — even before the Sept. 11 terrorist attacks. Fifty-four percent of Americans approved of the idea of FBI monitoring of suspects’ e-mail, according to a February 2001 survey by the Pew Internet American Life Project Americans.

Other privacy concerns are government access to stored electronic records, use of cookies to track visitors to government Web sites and misuse of government records available online.

### **Protecting privacy online**

The Internet offers both benefits and pitfalls to consumers, businesses and government, and each group can play a role in protecting privacy online.

Consumers serve as the front-line of defense in protecting their privacy while using the Internet. Consumers can choose strategies that balance their personal preferences for privacy with their desire for a

personalized Web experience. Low-tech, common-sense solutions include using discretion when giving out personally identifiable information (e.g., name, address, credit-card number) and reading the privacy policies posted on Web sites. Software solutions include setting your Internet browser to reject cookies and encrypting e-mail. Several online resources offer tips on protecting your privacy while using the Internet, including the Federal Trade Commission ([www.ftc.gov/bcp/conline/pubs/online/site/ese/index.html](http://www.ftc.gov/bcp/conline/pubs/online/site/ese/index.html)), the Privacy Rights Clearinghouse ([www.privacyrights.org/fs/fs18-cyb.htm](http://www.privacyrights.org/fs/fs18-cyb.htm)) and Consumer Privacy-Guide.org ([www.consumerprivacyguide.org/](http://www.consumerprivacyguide.org/)).

Businesses can adopt privacy policies and practices to address the privacy concerns that keep consumers offline. For example, two industry groups recently announced plans to respond to the consumer backlash against spam. The Direct Marketing Association will prohibit its members from sending e-mail to addresses on the DMA’s “do not contact list.” The nonprofit privacy group Truete will offer a service to stamp commercial e-mail with a “digital postmark” if the sender complies with defined privacy standards. Internet self regulation came under scrutiny when a 2000 survey by the Federal Trade Commission found that eight out of 10 of the most popular commercial Web sites in the United States had not implemented commonly accepted fair practices when collecting personal information from or about consumers online. The Progress & Freedom Foundation found signs of improvement when it compared the results of its 2002 and 2000 national surveys of commercial Internet sites. Among the most popular 100 domains, the proportion collecting personal information fell from 96 percent in 2000 to 84 percent in 2002, while the proportion offering visitors a choice over whether information can be shared with third parties rose from 77 percent to 93 percent.

Federal government regulation and standards address harm, fraud and treatment of sensitive information in the world of e-commerce. For example, the Children’s Online Privacy Protection Act regulates the collection, use and dissemination of personal identifying informa-

tion obtained online from children under 13. When implementing e-government, the federal government is guided by laws regarding access to public records, such as the Privacy Act and the Freedom of Information Act. In addition, federal agencies must comply with “Privacy Policies on Federal Web Sites,” which were outlined in a June 2, 1999, memorandum from the director of the Office of Management and Budget. The standards require agencies to post and adhere to privacy policies and to avoid using cookies without notice to visitors, among other things.

States address privacy concerns as part of their traditional public safety and consumer protection functions. Existing laws against deceptive practices, fraud, identity theft and credit-card-number theft can apply to online offenses, but some states are beginning to review the language of laws to make sure. State legislation and policies specifically related to the Internet have focused on spam and the privacy of state-government Web sites and data, rather than regulation of commercial sites, according to a 2002 survey by The Council of State Governments. States are limiting action to resolving the most common consumer complaint — spam — and to addressing the online-privacy consumer concern for which they are directly responsible — ensuring the privacy of information collected and stored by state government.

### **Striking a balance**

Consumers, businesses and government face a trade off when addressing consumer concerns about Internet privacy. When consumers reject cookies to prevent tracking of their online activities, they also diffuse the technology that may allow fast, personalized service. If governments made no public information available online to deter its use for illegal purposes, they would disregard an incomparable tool for providing citizens with open access to their government.

The challenge is to resolve Internet-privacy concerns without restricting the unique advantages of the Internet. ★

*Cindy J. Lackey is a Senior Policy Analyst at The Council of State Governments.*