

Safety in cyberspace

*What states are doing
about Internet privacy*

BY CINDY LACKEY

Seventy percent of U.S. Internet users are concerned about their privacy online, according to a March 2002 consumer survey by Jupiter Media Metrix, a company specializing in Internet analysis. Jupiter forecasts that \$24.5 billion in online sales will be lost by 2006 due to consumer privacy concerns — up from the estimated \$5.5 billion lost in 2001.

Consumer concerns about Internet privacy are not new. Survey research from the past five years consistently shows that Internet users worry about personal information privacy while they surf the Web. People are particularly concerned about the privacy of sensitive information such as Social Security numbers, credit card numbers and children's information.

Though e-commerce and e-government are growing steadily, analysts and government officials wonder how much more growth would be possible, were it not for persistent privacy concerns. In response, state government officials across the country are examining Internet privacy issues.

Research by The Council of State Governments (CSG) found that state policy actions on Internet privacy fall into six categories:

- (1) evaluating the need for policy action,
- (2) putting their own houses in order,
- (3) empowering consumers,
- (4) enforcing current criminal and consumer protection laws,



States are taking steps to secure the privacy of information they collect and store online.

- (5) creating specialized investigative and enforcement units, and
- (6) writing new laws.

Examples of these policy actions are highlighted in CSG's forthcoming *State Official's Guide to Internet Privacy*. The Guide provides an overview of Internet privacy and outlines the debates state officials likely will encounter when making policy decisions.

Ensuring privacy on state Web sites

Predominantly, states are addressing the Internet privacy concern for which they are directly responsible — ensuring the privacy of information collected and stored by state government. New state legislation and policies related to the Internet have focused on ensuring privacy of state government Web sites and data, according to CSG's 2002 national survey of state Internet privacy policies.

As repositories of citizens' personal information, state governments have a responsibility to be good stewards of these

resources, as well as an opportunity to lead the private sector by example. For e-government to flourish, states must build citizens' confidence in online transactions.

"On the upside, good privacy practices will encourage more citizens to use Web services, which will speed the transition to e-government," said Peter Swire, professor of law at Ohio State University and former Clinton administration privacy counselor. "On the downside, reports of bad privacy practices have spelled the end of a number of state government programs." Swire served on the CSG Internet Privacy Advisory Board, assisting CSG in developing the *State Official's Guide to Internet Privacy*.

To ensure the privacy of data collected and stored by state agencies, state officials are limiting the collection of and access to citizens' information, limiting citizens' information available on the Internet, adopting privacy policies, securing government data and systems, and designating chief privacy officers or other oversight mechanisms.

CSG launches new series

This fall, CSG will release the first three reports in a series of trends-oriented publications. The *State Official's Guide* series will cover urgent issues of critical importance to state governments. The *Guides* will provide practical tools for the assessment of an issue, examples of solutions and approaches taken by the states, discussion of possible sensitivities and concerns surrounding the issue. Each *Guide* will be developed in cooperation with a resource group of state officials, national policy experts and private-sector representatives.

Swire points to Washington as an example of a substantive privacy program.

Washington Gov. Gary Locke used an executive order to address the state's privacy practices broadly, as well as Internet privacy policies in particular. Issued on April 25, 2000, the order was intended to "ensure state agencies protect confidential personal information to the maximum extent possible while complying fully with the state's public disclosure and open government laws."

Among its requirements, the executive order prohibited posting citizens' personal information on Web sites and limited access to databases accessible via the Internet or intranet. The executive order also directed state agencies to prominently display on their Web sites privacy policies explaining the sites' practices for collecting and using personal information collected from site visitors. The state Department of Information Services issued a Model Privacy Notice that included required and suggested languages for agencies' privacy policies (see www.wa.gov/dis/architecture/FinalPrivacyModel.htm).

The Washington executive order looked beyond the Internet when protecting the privacy of citizens' personal information. The order required that Social Security numbers be removed from documents available to the public; personal information not be sold and lists of individuals not be released for commercial, profit-expect-

ing purposes; and state agencies designate contact persons to deal with privacy complaints and questions from the public.

Fighting deceptive practices and spam

Other than government-related Internet privacy issues, state legislation has most commonly targeted unsolicited bulk commercial e-mails, or "spam," based on responses to the CSG survey.

At least 25 states have passed laws regulating spam. Rather than ban spam, the laws target deceptive practices, such as using false return addresses, misleading subject lines or inoperative opt-out mechanisms. Most laws allow spam recipients and Internet service providers to sue spammers for damages. Spam laws in Washington and California, passed in 1998, recently withstood constitutional challenges.

The Washington law forbids commercial e-mail with misleading subject lines or with a disguised point of origin. Individuals who receive spam of this kind are eligible for damages of up to \$500, and the Internet service provider can sue for damages up to \$1,000. The state's Supreme Court upheld the law in July 2001, and the U.S. Supreme Court let that ruling stand by declining to review the case in October.

Internet resources

CSG's Internet Privacy Clearinghouse — www.csg.org

The site provides background information on privacy issues and links to online resources, including federal and state legislation and regulations.

National Electronic Commerce Coordinating Council — www.necc.org

NECCC, an alliance of national state government associations interested in information technology, offers guidelines and white papers specifically for state officials who are charged with advancing electronic government.

Spam Laws — www.spamlaws.com The site summarizes and links to full text versions of state spam laws.

California's anti-spam law requires "unsolicited e-mailed documents" that are transmitted via equipment in the state must be identified in the subject line as "ADV" for advertisement. If the e-mail contains sexual material, the subject line must include "ADV:ADLT." The message must provide an easy way for recipients to notify the sender to halt sending unsolicited messages. In April 2002, the California Supreme Court refused to hear an appeal by an online dating service that contended the state's spam-control law violated the commerce clause of the U.S. Constitution by imposing one state's spam restrictions on interstate advertisers. The decision let stand the California Court of Appeal ruling that the statute's intrusion on the federal commerce clause is minimal and is outweighed by California's interest in protecting its citizens from economic harm.

Empowering consumers

As part of their traditional consumer-education role, states are working to raise awareness of Internet privacy issues and inform citizens about protecting their privacy online. State outreach strategies include public service announcements, presentations, information and complaint hot lines, and consumer handbooks, according to the CSG survey.

An example is the South Dakota Internet Crimes Against Children Enforcement Unit's Web site, www.sdcbersafe.com, which educates consumers about protecting children online. The site has resources for kids, teens, parents and teachers, including links to filter software and to Disney Online's CyberNetiquette Comix, "an entertaining, interactive way for families to learn valuable lessons about online safety." The site even allows reports of crimes against children — whether they occur in the "real world" or in cyberspace — to be filed online.

As state officials act to resolve Internet privacy concerns, the challenge is to avoid restricting the unique advantages of the Internet. The *State Official's Guide to Internet Privacy* is a useful tool to inform state policy-makers. ★

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