

Privacy on the line

As they collect and use personal data on the Internet, states have a crucial role in raising awareness and fostering discussion about online privacy.

BY HEATHER BAKONDY

Heather Bakondy is policy and program coordinator for the National Association of State Telecommunications Directors, which is a CSG affiliate.



In many states today, people have the convenience of online vehicle registrations, driver's license renewals, hunting and fishing license applications and simplified tax filing. As states rush to adopt such electronic-commerce applications, policy-makers also need to pay attention to how they collect and use this proprietary, personally identifying information.

Online privacy is not a simple task. Public officials must protect constituents' rights in regard to proprietary information without impinging upon Freedom of Information safeguards that are unique to the public sector. Governments must strike the right balance between making public records available for proper use via the Internet without placing such information at risk for financial fraud, theft of reputation and theft of identity.

The Internet has relied on self-regulation. Recent reports of information brokering by online companies, however, have heated up the debate over Internet privacy. At the August Democratic convention in Los Angeles, U.S. Rep. Jay Inslee of Washington said, "The privacy of Americans is under siege."

Amazon.com announced Aug. 31 it considers its 23 million customers' personal information a business as-

set, which can be sold, licensed or shared.

Privacy has become the top concern of Internet users, and state governments' efforts to control the use of proprietary information posted online is coming under increased scrutiny. A 2000 report from the National Electronic Commerce Coordinating Council, a multiassociation consortium that focuses on information technology, found most politicians are not cognizant of the degree of public concern nor are they aware of privacy's increasing importance in this online era.

Privacy vs. commerce

While online retailers maintain that the collection of personal information allows for more efficient delivery of personalized services, "the overwhelming majority of American people are concerned about privacy," said Mark Uncapher, vice president of the Information Technology Association of America, an Arlington, Va.-based association of U.S. technology businesses. A 1999 *Business Week*/Harris poll found that 57 percent of online consumers now favor the passage of some type of law regulating the collection and use of personal information.

States are now offering many services online that require users to divulge sensitive information. State officials should bear in mind that the 55 percent of Internet subscribers who do not conduct online transactions have cited privacy and fraud concerns as the greatest deterrent, according to the *BusinessWeek* poll.

Caution urged

Harriet Pearson, IBM's director of privacy policy, said, "State legislators should address Internet privacy first in terms of their own state's e-government initiatives. State agencies must be responsive to citizens' needs and expectations regarding data, i.e.,

driver's license data. It is everyone's best interest for state lawmakers to know good housekeeping rules as they pertain to the Internet."

Pearson also recommended that states show restraint in regulation of the Internet at-large. IBM recently unveiled its Institute for Electronic Government, which includes Webcasts of discussions on Internet privacy and recommendations that are available as an educational resource to government officials and individuals (www.ieg.ibm.com).

State lawmakers are educating themselves on issues surrounding the Internet privacy debate. Pearson cited New York's Senate Majority Task Force on the Invasion of Privacy as an outstanding example. Not only did the task force take an in-depth look at privacy concerns, but it also released a complex report in respect to all privacy issues, including Internet privacy. Legislators and others should follow in New York's footsteps and "tread carefully before making decisions," Pearson said.

New York Senate Majority Leader Joseph Bruno, a 14-year Senate veteran, led the task force's investigation on the status of privacy protection. Bruno spearheaded the 1999 task force in response to "the explosion of technology and the increased citizen services that have accompanied it. As these services have increased, prices are being paid in terms of privacy," said his spokesperson Mark Hansen.

The task force took testimony from private-sector representatives with expertise in Internet and other technologies. The report yielded more than 50 recommendations on improving the privacy of personal proprietary information.

The report generated real change in New York. "As a result of the report, the Senate passed 20 pieces of legislation suggested by the task force, with five signed into law," Hansen said. He noted that while "some people joke that task force reports do nothing but sit around gathering dust, this report

worked to change state law to better privacy protection."

States take action

New York is not the only state to target privacy protection. In February, Washington legislators, supported by state Attorney General Christine Gregoire, introduced legislation to prohibit businesses from refusing service to customers unwilling to share personal information. The state Senate voted 41-6 in support of the bill; however, the House later killed the bill in committee.

A law took effect in Texas that as of July 1, the home page of all state Web sites and any new or changed key public entry points must post privacy policies. Each page must detail implementation of security and privacy safeguards such as Secure-Socket-Layer technology to encrypt personal information, including names, Social Security numbers,

transaction payment information and identification codes and passwords. These policies address the use of server logs and/or cookies for information collection. A cookie is a small text file containing unique information that allows Web sites to track such things as passwords, lists of pages visited, and the data when a specific page was last accessed. Often used in commercial Web

sites to identify the items selected for a specific shopping-cart application, cookies recognize repeat visitors and enable Web sites to store information on the user's computer for later reference.

States' reaction to privacy concerns has been considerable this year. According to the Internet Alliance, a Washington, D.C. association dedicated to promoting Internet services, state legislatures this year considered more than 110 privacy and children's privacy bills. Some experts caution, however, that policy-makers may be jumping the gun. "The Internet is a very vibrant place, but laws have effects we don't intend," said Sydney

Rubin, a spokeswoman for the Online Privacy Alliance. "It doesn't mean you never legislate, but you legislate with tremendous care, particularly when you're dealing with mediums as important to the economy as the Internet."

As seen in federal attempts, regulating privacy can be burdensome and complex for states and businesses. In May, Democratic U.S. Sens. Jay Rockefeller of West Virginia and Fritz Hollings of South Carolina introduced a bill that would require consumers to "opt in" before companies could seek personal-identification information. Rockefeller said, "The right information and the ability to withhold consent will allow consumers to choose a level of privacy that makes them comfortable."

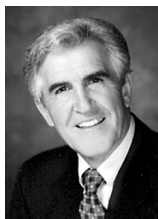
Also in May, the Federal Trade Commission issued a 159-page financial services privacy rule governing the sharing of Web sites' customer financial information with other companies. This action was in response to insufficient efforts by financial firms in protecting their customers' personally identifying information.

Minnesota Attorney General Mike Hatch also took notice of financial firms' laxity in protecting consumers' identifying information. Last year, Hatch sued U.S. Bancorp, charging that the firm shared identifying information with a telemarketing firm for a \$4 million fee. U.S. Bancorp settled the case and agreed to change its practices. California, New York, Washington and Vermont, along with 16 other states, began their own investigations into privacy abuses as a result of Hatch's lawsuit. Through the investigations of possible infractions, states can learn to best prevent privacy infringements in their own electronic-government systems.

Looking forward

As state leaders become aware of concerns over Internet privacy, a smart choice is to thoroughly examine the issue before legislating. In August, Florida Gov. Jeb Bush took such a cau-

continued on page 23



*New York
Senate
Majority
Leader Joseph
Bruno*

Privacy on the line

continued from page 15

tious step in appointing a Task Force on Privacy and Technology to be led by the state's chief technology officer, Roy Cales. This task force will examine best practices in working to protect proprietary information constituents submit to the state online.

In researching the privacy issue, policy-makers must consider constituents' values and interests in maintaining control of their personal information. The Direct Marketing Association maintains that online retailers can better target customer needs via the acquisition and manipulation of personal data. Of course, increasing collections

of personal data heightens the opportunities for fraudulent activity. On the other hand, limiting the amount or type of personal information collected can reduce the number of services available online while lowering the efficiency of e-government tools.

E-government models are just starting to develop and will continue to evolve. As they do, networks will increasingly be relied upon to enhance productivity and improve services to constituents. Policy-makers must weigh carefully the implications of information policy for privacy, confidentiality, security and efficiency as part of their state's e-government agendas. ★

Privacy principles

- *Access* — Individuals should have access to their own data to know what has been collected and to ensure its accuracy.

- *Choice* — Individuals should be given a choice whether or not to provide their personal information, subject to law.

- *Data Integrity* — Individuals should have reasonable assurance that their information was entered correctly and has not been corrupted.

- *Notice* — Individuals should be notified when their information is being collected and informed about how it will be used.

- *Transfer* — Individuals should be notified and given a choice if their personal information will be transferred to another organization than the one that originally collected it, or whether the information will be used for a difference purpose than that for which it was collected.

- *Security* — Individuals should have reasonable assurance that their information is secure and protected from outside attack or unauthorized alteration.

Source: "Privacy — Building the Public Trust," National Governors' Association, *Issue Brief*, June 20, 2000, www.nga.com.