NEW YORK STATE SENATOR

Martin J. Golden

Golden Introduces Online Privacy Bill To Protect New Yorkers Against Hackers, Misuse of Private Information

MARTIN J. GOLDEN September 22, 2014

State Senator Martin Golden (R, C, I) has introduced legislation to protect the online privacy of New Yorkers from hackers and to insure that owners of email accounts and web services keep personal information totally private, to require rapid notification of any breach of email accounts or credit cards, and to enforce penalties against the owners of email and web services when such breaches occur. The bill is called "The New York State Online Privacy Act."

The development of the legislation is spurred in part by recent news that Home Depot and Target security has been breached at levels involving the privacy of millions of customers—40 million in the case of Home deport and 70 million at Target. But other companies have also been hacked with millions affected, including U.P.S., Goodwill, P. F. Chang's, Sally Beauty, Michael's and Neiman Marcus. The Department of Homeland Security and the Secret Service have recently estimated that more than 1,000 businesses in the United States have been infected with malware that is programmed to siphon payment card details from cash registers in stores. They believed that many of these businesses did not even know they were sharing customers' credit card information.

“Now more than ever, after what have been almost weekly reports of breaches of the online privacy and security of our people, we need to create enforceable standards for privacy and confidentiality for our citizens when they are online,” Golden said. “This bill does that by providing that except under strictly defined situations, personally identifiable information cannot be released except with the permission of the user who provided that information, and it establishes a requirement that operators of websites and online services establish and show to users their privacy policies, and notify them in the case of a breach of security that compromises the integrity of the information. It also establishes appropriate penalties for violations.”

The bill applies to all commercial email, online, and web services but not to non-commercial websites or services that do not collect personally identifiable information concerning its users, or to the state or federal government, or financial institutions that adopt safeguards complying with Gramm-Leach-Bliley Act standards. State and federal government is already covered under separate laws, financial institutions are covered under he Gramm-Leach act, and certain health care information privacy is required under a number of federal laws.

Among its many comprehensive provisions, the Golden bill

Creates an Office of Privacy Protection to provide oversight, information, referral, and enforcement of the privacy laws created or updated in this bill. The commissioner of the new office will be confirmed by the Senate, and report directly to the Governor. The office will include a 9-member public-private Privacy Protection Advisory Committee to aid in policy

and oversight.

Requires a publicly-posted privacy policy for websites and online services that is accessible by being on the first webpage of a site or easily accessible by email.

Prohibits sharing personally identifiable information by a website or online service without express permission of the user, except in certain limited and enumerated cases (e.g., in response to a court order, or for legitimate business reasons, or with the permission of the individual). Personally identifiable information includes everything from an individual's name, home address, age, religion, occupation, telephone number, financial data, security or access codes, and any information that permits contact of the individual, such as a driver's license or state identification card, and products purchased or rented;

Makes social media confidential, by prohibiting penalties against an individual who refuses access by employers or universities to his or her social media,

Protects children, by extending the existing protections in the federal Children's Online Privacy Protection act to minors over 13 and less than 16 (COPPA already protects minors under 13). The act requires operators to post their online privacy policy, make reasonable efforts to notify parents of privacy practices and obtain verifiable parental consent, establish and maintain reasonable procedures to protect confidentiality, security, and integrity of the personal information collected from children under age 13, and other requirements.

Protects Consumers in the case of a Breach of information, by requiring notification to the office in the event of a security breach, with significant penalties for willful or negligent failure to comply with the new privacy provisions, and authorizes creation of a new breach alert system in the Office of Information Technology Services.

The provisions of the bill are modeled on successful law in other states and track principles of Fair Information Practices, a set of widely endorsed principles first described by the Federal Trade Commission in its 1998 report.

These include:

1. Notice/Awareness - Consumers should be given notice of an entity's information practices before any personal information is collected from them.

2. Choice/Consent Choice and consent in an online information-gathering sense means giving consumers options to control how their data is used.

3. Access/Participation Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

4. Integrity/Security Information collectors should ensure that the data they collect is accurate and secure.

5. Enforcement/Redress In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures.

This framework is addressed in this legislation.

###